博士論文

RSA Cryptanalyses with the LLL Reduction

（LLL 格子簡約を用いた RSA 暗号の攻撃）

高安敦

Abstract

RSA is one of the most famous cryptosystems and the security has been studied in numerous papers. One main approach for the research is due to Coppersmith's lattice based methods that enable us to solve modular/integer equations with small solutions in polynomial time. Indeed, several RSA vulnerabilities have been reported by using the methods. Thus far, a number of attacks on RSA and its variants with some special hints have been proposed, however, some of these attacks have obvious room to be improved. The facts come from the technical hardness to apply Coppersmith's methods to RSA cryptanalyses. More concretely,

- how to formulate attack scenarios appropriately and
- how to construct appropriate lattices to solve equations

are technically hard problems. In this paper, we propose several improved polynomial time attacks on RSA variants by resolving the above difficulties. Our first result is an improved algorithm for solving the small inverse problem that relates to the security evaluation of the small secret exponent (multi-prime) RSA. Our proposed algorithm offers improved attacks on multi-prime RSA with small prime differences. Our second results are improved partial key exposure attacks on CRT-RSA where the attacks utilize partial exposed bits of CRT-exponents. We study attacks with the most/least significant bits of d_p or/and d_q. For all the cases, we propose improved attacks. Our third results are improved partial key exposure attacks on RSA for general exposure scenarios. Our claimed scenarios contain several ones which have been studied as special cases. We construct attacks that contain all the currently known best attacks as special cases. Furthermore, we obtain improved attacks in several specific scenarios. Our last results are improved small secret exponent attacks and partial key exposure attacks on Takagi's RSA and the prime power RSA both of that have moduli $N = p^r q$. We propose simple lattice constructions to attack the variants and obtain improved attacks.

Keywords RSA, cryptanalysis, lattices, the LLL reduction, Coppersmith's methods

Acknowledgement

Best of all, I would like to express my sincere gratitude to Assistant Professor Noboru Kunihiro, who is my supervisor, and Professor Hirosuke Yamamoto for the continuous support. I joined their research laboratory since September 2012. At that time, I was just a beginner of academic research. I did not know how to read papers, obtain meaningful results, write papers, and present the results. Their continuous support enables us to publish twelve papers in the past five years. Moreover, Noboru Kunihiro never wasted my time. He tried to make my time by not forcing boring work on me. I could concentrate my research due to his effort. I should also thank other members of the laboratory; especially Yutaka Kawai, Junya Honda, Shota Yamada, Takashi Yamakawa, Kosei Endo, Shuichi Katsumata, and Yao Lu. They gave me nice comments in the seminar. Furthermore, I spent precious time with them including activities outside the laboratory. Unfortunately, I have to apologize to Chiaki Sakakibara who is the secretary of the laboratory. Before every official trips, my paperwork procedures delayed. It may take additional time for her. I would like to thank her perfect job.

Besides, I would like to thank Goichiro Hanaoka, who is a group leader of the Advanced Cryptosystems Research Group, Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology (AIST). He may be the first person (including even myself) to predict that my paper will be accepted in major conferences like IACR Conferences in the near future. He has always encouraged me and believed my ability. When we went to izakaya in Hakodate in July 2014, he invited me to join the study group Shin-Akarui-Ango-Benkyoukai. Since then, I joined the group for three years and have learned much better than expected. Needless to say, I want to thank other members of the study groups. They always gave me brilliant comments and suggestions.

I would like to express my special thanks to Katsuyuki Takashima who was the mentor during my internship to Mitsubishi Electric. It is not too much to say that all my recent publications owe to his patient guidance. When I went to the internship, I

already had several papers, however, I was not a good researcher at all. Although he was one of the best researchers in Japan, he always taught me everything from basic. He politely answers all my elementary questions. I learned a lot of things including how to write papers and an attitude of academic researchers. I want to thank members of Mitsubishi Electric; Mitsuru Matsui, Takato Hirano, Takeshi Sugawara, and Yutaka Kawai. I enjoyed the internship due to their courtesy.

All results presented in the thesis are supported by Research Fellowships of Japan Society for the Promotion of Science for Young Scientists. Finally, I would like to thank my families for their unconditional supports and loves in all stages of my life.

Contents

Chapter 1

Introduction

1.1 Background

1.1.1 Public Key Cryptosystem – Development and RSA

The information technology is indispensable for the modern society. In several situations, one has to consider the security of his digital data. Cryptography is the fundamental technique to resolve the problem such as secure communication and integrity of data. Here, assume that Alice wants to send her secret message M to Bob via an insecure channel. If they share a common secret k, they can achieve the goal by utilizing a symmetric encryption scheme. Alice encrypts the message M as $C := \mathsf{Enc}_k(M)$ by a symmetric encryption algorithm with a key k, then sends the ciphertext C to Bob. Due to the correctness of the symmetric encryption scheme, $M = \mathsf{Dec}_k(\mathsf{Enc}_k(M))$ holds. Hence, Bob gets the plaintext $M = \mathsf{Dec}_k(C)$ by a symmetric decryption algorithm with a key k. As we assumed, since they used an insecure channel for the communication, an eavesdropper Eve may obtain the ciphertext C. However, it does not matter. Due to the security of the symmetric encryption scheme, Eve, who does not know the common secret k, cannot recover the plaintext by the eavesdropped ciphertext c. As a result, Alice and Bob can successfully communicate via an insecure channel. However, a simple question arises; how do Alice and Bob share a common secret.

In 1976, Diffie and Hellman [DH76] resolved the key exchange problem in an elegant way. Let p be a prime number. Then, $\mathbb{Z}_p$ with the multiplication forms an abelian cyclic group G of order $p - 1$. Let $g \in G$ be a generator of G. Assume Alice and Bob want to share a common secret via an insecure channel along with public p and g. Alice picks random secret $a \in \mathbb{Z}_{p-1}$ and sends $g^a \pmod{p}$ to Bob. Bob picks random secret $b \in \mathbb{Z}_{p-1}$ and sends $g^b \pmod{p}$ to Alice. Then, Alice and Bob can share a common secret $k = g^{ab} \pmod{p}$. By eavesdropping the communication, what Eve knows is (g, g^a, g^b). Among the cryptographic community, it is widely believed that computing the secret g^{ab} from Eve's knowledge is computationally hard where the problem is called the Diffie-Hellman problem.

Diffie and Hellman's work developed a notion of public key cryptography. Alice and Bob share a common secret by utilizing the Diffie-Hellman key exchange protocol and communicate securely by utilizing symmetric key encryption schemes via an insecure channel. Then, let us consider a case when many n users $U_1, \ldots, U_n$ want to send their own secret message m_i to other members in the same manner. For the purpose, each user U_i should share a common secret $k_{i,j}$ with all the other users $U_1, \ldots, U_{i-1}, U_{i+1}, \ldots, U_n$. The task requires $\binom{n}{2}$ times run of the Diffie-Hellman key exchange protocol. Therefore, the approach results in heavy communication cost that depends on the number of users n.

In 1978, Rivest, Shamir, and Adleman [RSA78] proposed the first public key cryptosystem that avoids the key exchange problem; the so-called RSA cryptosystem, which we study in this paper. Let p and q be secret primes, $N = pq$, (e, d) be random elements in $\mathbb{Z}^*_{\Phi(N)}$ such that $ed = 1 \pmod{\Phi(N)}$ where $\Phi(N) = (p-1)(q-1)$ is Euler's totient function. In a public key cryptosystem, there are two forms of keys; a public key pk and a secret key sk. RSA has a public key $pk := (N, e)$ and a secret key $sk := (p, q, d)$. To communicate with Alice, Bob produces his public/secret key pair. Then, Bob publishes the public key $pk = (N, e)$ and store the secret key $sk = (p, q, d)$. Alice encrypts a plaintext $M \in \mathbb{Z}^*_N$ as $C = \mathsf{Enc}_{pk}(M) := M^e \pmod{N}$ by Bob's public key and sends the ciphertext C to Bob. Bob uses his secret key and recover the plaintext M by computing $M = \mathsf{Dec}_{sk}(C) := C^d \pmod{N}$. The decryption works correctly where the fact is verified from Fermat's little theorem; $M^{ed} \pmod{N} = M^{1+\ell\Phi(N)} \pmod{N} = M$ where ℓ is some integer. By eavesdropping the communication, Eve learns the ciphertext C and Bob's public key $pk = (N, e)$. However, the security of a public key cryptosystem ensures that Eve cannot decrypt the ciphertext even with the public key. Hence, Alice and Bob can communicate securely via an insecure channel without any key exchanges.

Designing the RSA cryptosystem is one of the most fantastic breakthrough in the context of cryptographic research thus far. Indeed, Rivest, Shamir, and Adleman received the valuable Turing Award in 2003. After the invention, several public key cryptosystems have been proposed (e.g., the ElGamal encryption scheme [Gam85], the knapsack cryptosystem [MH78], and more), however, RSA is still one of the most widely-used public key cryptosystems. Today, it is a common knowledge that RSA is not the first public key cryptosystem but the first "published" public key cryptosystem. The notion of public key cryptosystems was mentioned in James Ellis in 1969. In 1973, Clifford Cocks constructed a public key encryption scheme which is analogous to RSA. In the next year, Malcom Williams developed a key exchange protocol which is similar to Diffie-Hellman's one. Since they were UK secret agencies worked in Government Communications Headquarters, they did not publish the results due to the secrecy policies.

Since the popularity, several variants of the RSA cryptosystem with higher efficiency have been considered. The most well-known variant is the CRT-RSA as described by Quisquater and Couvreur [QC82] where the scheme has secret keys d_p and d_q in place of d where $ed_p = 1 \pmod{p-1}$ and $ed_q = 1 \pmod{q-1}$. CRT-RSA achieves about four times faster decryption than the standard RSA. Some variants have the composite integers N which are the product of more than two secret primes. The Multi-Prime RSA has a composite integer $N = p_1 \cdots p_k$. Other variants such that Takagi's RSA [Tak98] and the prime power RSA have a composite integer $N = p^r q$. If the same size of composite N is used, these variants achieve faster key generation and decryption than the standard RSA.

Thus far, several advanced forms of public key cryptosystems have been constructed based on more useful algebraic structures and developments of cryptographic techniques. The most typical two of them are bilinear pairing from elliptic curves and the lattice-based cryptography. Here, we introduce the most basic application of pairing; a one round tripartite key exchange protocol proposed by Joux [Jou00]. Let G_1, G_2, and G_T be cyclic groups of the same prime order p. A bilinear pairing $\hat{e}$ is a map such that $\hat{e} : G_1 \times G_2 \to G_T$. G_1 and G_2 are subgroups of points on an elliptic curve over a finite field where the group operations are denoted as addition. G_T is a subgroup of the multiplicative group of a finite field where the group operation is denoted as multiplication. Let P_1 and Q_1 be a generator of G_1 and G_2, respectively. In the context of cryptographic designs, non-degenerate, efficiently computable pairings are used. For a non-degenerate pairing $\hat{e}$, if $\hat{e}(P, Q)$ is an identity element in G_T, then either P or Q is an identity element in G_1 or G_2. The powerful feature of pairings is its bilinearity which is useful in designing cryptographic schemes; for $a, b \in \mathbb{Z}_p$, $\hat{e}(aP_1, bQ_1) = \hat{e}(bP_1, aQ_1) = \hat{e}(P_1, Q_1)^{ab}$ holds. Then, we show how Alice, Bob, and Charlie can share a common secret k via an insecure channel. Alice, Bob, and Charlie pick random $a, b, c \in \mathbb{Z}_{p-1}$, respectively. Alice broadcasts (aP_1, aQ_1) to Bob and Charlie, Bob broadcasts (bP_1, bQ_1) to Charlie and Alice, and

Charlie broadcasts (cP_1, cQ_1) to Alice and Bob. Since Alice knows her own secret a along with bP_1 and cQ_1 which Bob and Charlie broadcasted, she can compute $k = \hat{e}(bP_1, cQ_1)^a = \hat{e}(P_1, Q_1)^{abc}$. Similarly, Bob and Charlie can compute the same secret k as $k = \hat{e}(cP_1, aQ_1)^b = \hat{e}(P_1, Q_1)^{abc}$ and $k = \hat{e}(aP_1, bQ_1)^c = \hat{e}(P_1, Q_1)^{abc}$, respectively. Although an eavesdropper Eve can learn $(P_1, Q_1, aP_1, aQ_1, bP_1, bQ_1, cP_1, cQ_1)$, it is believed that computing $k = \hat{e}(P_1, Q_1)^{abc}$ seems infeasible.

As the example suggests, bilinear pairings and also lattices enable us to construct several advanced forms of public key cryptosystems that are infeasible to obtain without such powerful primitives. Fully homomorphic encryption [Gen09, vDGHV10, CMNT11, Bra12, CNT12, GHS12a, GHS12b, CCK$^+$13, GSW13, JR13, BGV14, BV14a, BV14b, CLT14, Nui14, CS15, NK15] have ciphertexts which one can operate addition and multiplication without knowing its secret key. More concretely, given $C_1 = \mathsf{Enc}_{pk}(m_1)$ and $C_2 = \mathsf{Enc}_{pk}(m_2)$ which are fully homomorphic ciphertexts of plaintexts m_1 and m_2, anyone can compute $\mathsf{Enc}_{pk}(m_1 + m_2)$ and $= \mathsf{Enc}_{pk}(m_1 \cdot m_2)$ which are fully homomorphic ciphertexts of plaintexts $m_1 + m_2$ and $m_1 \cdot m_2$. Identity-based encryption [Coc01, BF03, BB04, Wat05, BW06, Gen06, Wat09, ABB10, LW10, BB11, CHKP12, Lew12, CW13, AHY15, KY16, Yam16, ZCZ16] can use arbitrary strings as its public key. Attribute-baed encryption and predicate encryption [OT09, LOS$^+$10, OT10, AFV11, YAHK11, LW11, ACM12, OT12b, OT12a, KSW13, Xag13, Att14, BGG$^+$14, Tak14, YAHK14, AY15, CGW15, GVW15a, GVW15b, OT15] can control fine-grade access structure of its ciphertexts.

In 2013, one of the most expected cryptographic primitive was constructed by Garg, Gentry, and Halevi [GGH13a]. They proposed a graded encoding scheme which is an approximate multilinear map. Since a multilinear map is an extension of a bilinear map, a one round multipartite Diffie-Hellman key exchange is a straightforward application. After that, other constructions of graded encoding schemes [CLT13, LSS14, ACLL15, CLT15, GGH15] have been proposed. Based on the powerful map, numerous magical cryptosystems have been proposed [FHPS13, GGH$^+$13b, GGH$^+$13c, GGSW13, HSW13, BWZ14, Gar14, YYHK14, GLSW15, AFH$^+$16, GMM$^+$16].

1.1.2 Cryptanalysis – The Security of RSA

In Section 1.1.1, we introduce one side of cryptographic research, i.e., designing cryptographic schemes. There is the other side of the research, i.e., cryptanalysis, which is the main topic of this paper. The security of cryptographic schemes is verified by attacking the schemes. If there are efficient attack algorithms, the security of the schemes are broken. Conversely, if there does not seem to be efficient ones, the fact ensures the security.

Let us talk back about the Diffie-Hellman key exchange protocol. The security is broken if there is an efficient algorithm for solving the Diffie-Hellman problem; given (g, g^a, g^b) and the goal of the problem is computing g^{ab}. A simple approach is recovering a secret a from (g, g^a) (or equivalently recovering a secret b from (g, g^b)) where the problem is called a discrete logarithm problem. Shoup [Sho97] showed that any generic algorithms should perform $\Omega(\sqrt{p})$ group operations where p is the order of the group G. Hence, if one uses the group G whose order p is exponentionally large with respect to the security parameter, there exists no generic algorithms for computing discrete logarithms efficiently. We call the fact that "there are no efficient algorithms for solving the discrete logarithm problem" the discrete logarithm assumption, and so do other problems. Although there are no proofs which show the polynomial time equivalence between the Diffie-Hellman problem and the discrete logarithm problem, the former problem is also believed to be computationaly hard. As one evidence, Maurer and Wolf proved the polynomial time equivalence in some special groups [MW96]. Then, the Diffie-Hellman assumption has been used to ensure the security of cryptographic schemes. It is widely believed that similar assumption also holds for bilinear groups.

The Diffie-Hellman like problems are successful results. Unfortunately, there are several cryptographic schemes whose security have been broken. It is widely known that there are several critical attacks on knapsack cryptosystems [Sha82, LO85, CJL$^+$92]. Recently, a number of attacks on multilinear maps have been proposed [CGH$^+$15, CHL$^+$15, CFL$^+$16, CLLT16, HJ16, MSZ16]. As these negative examples suggest, cryptanalysts have to work extensively to guarantee the security of existing cryptographic schemes.

Then, the time has come to discuss the security of RSA. Since RSA is one of the most basic cryptosystems, the security has been discussed in numerous papers. The security of RSA relates to the factorization of large composite integers N which is a component of the pubic key. It is easy to see that the security of RSA is completely broken if N is factorized. When N is factorized, then its prime factors p and q are revealed. Recall the key generation $ed = 1 \pmod{(p-1)(q-1)}$. If the public e along with the prime factors p and q are known, the extended Euclidean algorithm enables one to recover the remaining secret d. Hence, all ciphertexts C can be decrypted.

Here, we want to emphasize the fact that breaking RSA is easier than the factorization of N, however, the reverse is not necessarily true. In a number of textbooks for information engineering which is not for experts of cryptgraphy, there are incorrect statements written, i.e., "breaking RSA is no easier than the factorization of N". Here, "breaking RSA" means that given a ciphertext C, then computing its plaintext M only with a public key (N, e). Most cryptographers expect that the statement is true, however, there are no proofs. Moreover, Boneh and Venkatesan [BV98] showed that there should be a gap between the hardness of breaking RSA and the factorization of N. Thus far, however, there are no attacks known that do not factorize N but break RSA. Indeed, there are some positive results that indicate that breaking RSA is almost as hard as the factorization of N. In the original paper of RSA [RSA78], the authors claimed the probabilistic polynomial time equivalence between computing the secret d from the public key (N, e) and the factorization of N due to the work by Miller [Mil75]. It means that there is a probabilistic polynomial time algorithm to factorize N when (N, e, d) is given. Furthermore, Miller's work suggests that there is a deterministic polynomial time equivalence between computing the secret d from the public key (N, e) and the factorization of N under the Extended Riemann's Hypothesis. However, it seems a strong assumption. Later, May [May04a], Coron and May [CM07] proved the deterministic polynomial time equivalence between computing the secret d from the public key (N, e) and the factorization of N. Although the results have the same restriction $ed \leq \Phi(N)^2$, it covers a standard parameter setting. Since there are no proofs for the polynomial time equivalence between breaking RSA and computing the secret d, these results are not sufficient. By taking a different approach, Aggarwal and Maurer [AM09] showed that a gap between breaking RSA and the factorization of N does not seem large. In the paper, they proved that if there exists a generic algorithm for breaking RSA, then the algorithm can factorize N. Since they studied the problem only in the generic group model, the result is not sufficient. However, as these results suggest, there are several conjectures that "breaking RSA is no easier than the factorization of N". Therefore, in the rest of this paper, we assume that the statement is true.

Since the factorization problem is one of basic number theoretic problems, it has been studied from ancient Greeks. However, no efficient algorithms are not known. Indeed, the current state-of-the-art factorization algorithms [Pom84, Len87, LJMP90] require subexponential time in the input length. It suggests that there does not seem to be any efficient algorithms for breaking RSA.

To summarize the above discussion, RSA seems secure since the factorization is computationally hard problem. However, thus far, several practical vulnerabilities of RSA have been reported. The factorization problem for $N = pq$ is computationally hard when p and q are randomly distributed. Since the sampling large primes cannot be performed very efficiently, there are several implementations that sometimes use the same primes or sample secret primes from statistically biased distributions. Lenstra et al. [LHA$^+$12] and Heninger et al. [HDWH12] independently showed that about 0.2% of public N's for SSL/TLS protocols can be factorized efficiently since they share the same secret prime factors. Similarly, Bernstein et al. [BCC$^+$13] efficiently factorized 184 out of more than two million N's for Taiwan's government-issued digital smart cards since they share the same secret prime factors or the primes are sampled from statistically biased distributions. Not only the distribution of secret primes p, q but also that of d may disclose the factorization of N. If d is sampled as small integers, the decryption/signature generation becomes faster. However, Wiener [Wie90] first showed that if too small d's such that $d < N^{0.25}$ are used, then N can be factorized in polynomial time. After that, Boneh and Durfee [BD00] further improved the bound to $d < N^{0.292}$. Moreover, even if RSA is implemented correctly, some portions of secret information can be extracted via physical attacks against cryptographic devices where such attacks are called side channel attacks. Kocher [Koc96] and Kocher, Jaffe, and Jun [KJJ99] showed that power analysis can extract some secret information about d. Genkin, Shamir, and Tromer [GST14] proposed an acoustic attack, which utilized acoustic information during cryptographic operations, where the attack can extract whole RSA secret keys from the GnuPG software. Boneh, DeMillo, and Lipton [BDL97] showed that if the fault is induced during the CRT-RSA signature generation, the output faulty signature discloses the factorization of N. Several follow-up papers have been published to attack more secure systems [CJK$^+$09, CNT10, BNNT11, BBD$^+$13, FGL$^+$13]. Halderman et al. [HSH$^+$09] applied coldboot attack against laptop then some secret information about (p, q, d) along with (d_p, d_q) can be extracted. Several papers [HS09, HMM10, PPS12, KSI13, KH14, Kun15] followed Halerman et al.'s work and proposed key recovery attacks against RSA where the attacks utilize secret information which are extracted from coldboot attacks.

Since the secret information extracted from practical side channel attacks are not the exact secret keys but some partial information of the secret keys in general, cryptanalyses of RSA with its partial information have been studied in numerous papers. Furthermore, such cryptanalyses are also interesting topic in the theoretical sense since they assure the hardness for breaking RSA. Indeed, such attacks have been analyzed before the development of side channel attacks. The most basic problem for the research direction is the factorization problem with some portions of secret primes. Rivest and Shamir [RS85] proposed the polynomial time factorization algorithm for $N = pq$ with 3/5 of the most significant bits of p. Then Coppersmith [Cop96a] proposed an improved algorithm that works with half of the most significant bits of p. Herrmann and May [HM08] extends the attack with known bits which are not in consecutive blocks. Maurer [Mau95] constructed a factorization algorithm with the strong oracle that can answer arbitrary questions for Yes/No. May and Ritzenhofen [MR09] introduced implicit hints for the prime factor and proposed implicit factoring algorithms where the work has been followed by [SM09a, SM10, FMR10, SM11, TK14a, LPZ$^+$15]. Not only the partial information of the secret primes, attacks on RSA with the partial information of d have also been studied [BDF98, BM03, EJMdW05, Aon09, SSM10, JL12, TK14d]. Other attacks on RSA are summarized in [Cop97, Bon99, NS01, May03, May10].

1.1.3 Coppersmith's Methods – Tools for Attacking RSA

In 1996, Coppersmith [Cop96b, Cop96a] introduced elegant techniques to solve univariate modular equations with small solutions or bivariate integer equations with small solutions in polynomial time by using the LLL lattice basis reduction algorithm [LLL82]. Although there are no rigorous proofs, several evidences [AASW12, Kun12, CHHS16] for the optimality of the methods have been claimed. In short, to solve modular/integer equations, the methods first construct lattices that contain algebraic structures of the polynomials. Since the short lattice vectors in the lattices contain secret information of the small solutions, apply the LLL reduction and recover the short vectors. In the original papers [Cop96b, Cop96a], Coppersmith mentioned the algorithms for solving univariate modular equations and bivariate integer equations, however, the methods can be extended to equations with more variables under reasonable assumptions. Although the original methods are hard to apply to equations with more variables, simplified reformulations have been proposed. Howgrave-Graham [How97] proposed a simpler reformulation of the modular equations solving method whereas Coron [Cor04, Cor07] proposed simpler reformulations of the integer equations solving method. Then the methods are applied to cryptanalyses, especially for RSA, in numerous papers. Indeed, several results for RSA cryptanalyses which are introduced in Section 1.1.2 utilized the methods. Until recently, the cryptanalytic results based on Coppersmith's methods have theoretical flavor, however, Bernstein et al. [BCC$^+$13] first applied the methods to the realistic cryptanalysis.

However, it is hard task to construct optimal attacks on RSA by using Coppersmith's methods. There are two main difficulties for constructing nice attacks. The first difficulty is how to formulate attack scenarios as modular/integer equations. For the same attack scenario, we can formulate it as several ways by using modular equations or integer equations. In general, we do not know optimal formulations before we construct concrete attack algorithms. The second difficulty, which is the main bottleneck of algorithm constructions via Coppersmith's method, is how to construct lattices to solve modular/integer equations. The qualities of attack algorithms depend on underlying lattices. In other words, if we can construct appropriate lattices which contain full algebraic structures of the polynomials, we can construct the best attack. However, an optimal lattice construction methodology is not known. Hence, we should construct each algorithm in an ad hoc manner.

Jochemsz and May [JM06] proposed one solution for resolving the above difficulties. They proposed a general strategy for lattice constructions to solve both modular equations and integer equations. The method is applicable to any equations and offers to some extent nice algorithms. Indeed, there are no integer equations solving algorithms that are better than ones based on the Jochemsz-May strategy.

However, the strategy cannot resolve the above difficulties completely. Lattice constructions for the modular method are simpler than those for the integer method in general. Thus far, in the context of RSA cryptanalyses based on Coppersmith's methods, most attacks are based on the modular method due to its simplicity. However, once the integer method is applied, better attacks may be obtained. Although attacks that solve modular equations based on the Jochemsz-May strategy are also constructed by solving integer equations and reverse does not hold in general, there are several attacks that have been analyzed only with the modular method. For example, Ernst et al.'s partial key exposure attacks on RSA [EJMdW05] utilized the integer method and no attacks with the same quality have been constructed based on the modular method.

Moreover, the bottleneck of the Jochemsz-May strategy is that there are several modular equations solving algorithms that are better than ones based on the strategy. Due to its generality, the strategy does not capture specific algebraic structures of underlying polynomials. If one exploits useful algebraic structures, then better algorithms can be constructed. For example, in the context of Boneh and Durfee's small secret exponent attack on RSA [BD00], small $d < N^{0.284}$ discloses the factorization of N based on the Jochemsz-May strategy. However, Boneh and Durfee showed that small $d < N^{0.292}$ discloses the factorization of N by exploiting more useful algebraic structures.

1.2 Our Contributions

In this paper, we carefully analyze formulation of attack scenarios and lattice constructions. Then, we obtain several improved results in the context of the security evaluation of RSA. More concretely, the spirits of our improvements owe to the following two approaches:

- solving integer equations based on the Jochemsz-May strategy,
- solving modular equations based on better lattice constructions than the Jochemsz-May strategy by exploiting useful algebraic structures.

Chapter 3: We study solving a specific modular equation called the small inverse problem; given two integers (N, e) then solving a bivariate modular equation $x(N + y) \equiv 1 \pmod{e}$. The small inverse problem was introduced by Boneh and Durfee [BD00] in the context of the small secret exponent attack on RSA; the attack on RSA for small d. Thus far, more general formulation of the small inverse problem has been analyzed by Weger [dW02], Sarkar, Maitra, and Sarkar [SMS08], Kunihiro, Shinohara, and Izu [KSI14]. Concretely, Boneh and Durfee only studied the case when the absolute value of the solution of y is bounded above by $N^{1/2}$, however, the follow-up papers studied arbitrary sizes.

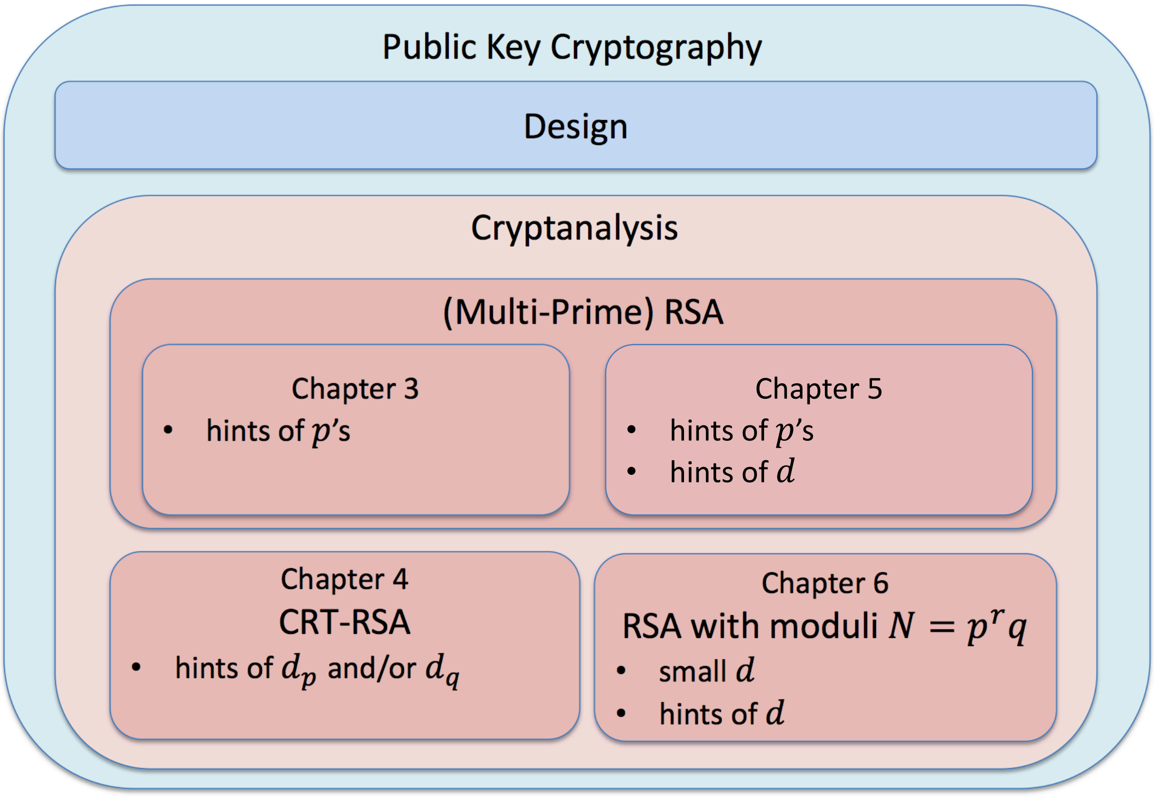
In this paper, we first show that the results of Sarkar et al. and Kunihiro et al. are not valid. Then, we propose an improved algorithm to solve the general version of the small inverse problem. The improved result owes to our better lattice construction. As a result, by using the algorithm, we propose an improved small secret exponent attack on the Multi-Prime RSA, which has a public modulus $N = p_1 \cdots p_k$, with small prime differences; $p_1 < \cdots < p_k$ and $p_k - p_1 < N^{\gamma}$ for $0 < \gamma \leq 1/k$.
(The results appeared in the international conference *ICISC 2014* [TK14c] and the international journal IEICE Transactions [TK17a].)
Chapter 4: We study the partial key exposure attacks on CRT-RSA; attacks on CRT-RSA when some portions of the most/least significant bits of CRT-exponents d_p or/and d_q are exposed to attackers. Blömer and May [BM03] proposed attacks with the most/least significant bits of d_p or d_q where $d_p, d_q \approx N^{1/2}$. Given the most significant bits of d_p, the attack works for $e < N^{1/4}$ whereas given the least significant bits of d_p, the attack works for extremely small $e = poly(\log N)$. Sarkar and Maitra [SM09b] proposed attacks with the most significant bits of d_p and d_q. As opposed to Blömer and May's attacks, although Sarkar and Maitra used more partial

information than Blömer and May, their attack does not work for $d_p, d_q \approx N^{1/2}$. Lu, Zhang, and Lin [LZL14] proposed improved attacks of Blömer and May with the least significant bits of d_p or d_q. Lu et al.'s attack works for $e < N^{3/8}$. We note that Blömer and May's attacks and Lu et al.'s attacks used Coppersmith's method to solve modular equations whereas Sarkar and Maitra's attack used Coppersmith's method to solve integer equations.

In this paper, we use Coppersmith's method to solve integer equations and improve Blömer and May's attacks and Lu et al.'s attacks. As opposed to previous results, the interesting feature of our results is that attack conditions do not depend on the position of exposed bits. Then, we propose the first partial key exposure attack on CRT-RSA for $e < N^{3/8}$ with the exposed most significant bits. We claim that our attack is better than Lu et al.'s attack with the exposed least significant bits; our attack works with less exposed bits than Lu et al. We also improve Sarkar and Maitra's attack with detailed analyses where our improved attack works for $e < N$ and $d_p, d_q \approx N^{1/2}$.
(The results appeared in the international conference *ACNS 2015* [TK15] and *ISC 2016* [TK16b].)

Chapter 5: Thus far, *partial key exposure attacks on RSA* have been intensively studied using lattice based Coppersmith's methods. In the context, attackers are given partial information of a *secret exponent* and *prime factors* of *(Multi-Prime) RSA* where the partial information is exposed in various ways. Although these attack scenarios are worth studying, there are several known attacks whose constructions have similar flavor. In this paper, we try to formulate general attack scenarios to capture several existing ones and propose attacks for the scenarios. Our attacks contain all the state-of-the-art partial key exposure attacks, e.g., due to Ernst et al. (Eurocrypt'05) and Takayasu-Kunihiro (SAC'14, ICISC'14), as special cases. As a result, our attacks offer better results than previous best attacks in some special cases, e.g., Sarkar-Maitra's partial key exposure attacks on RSA with the most significant bits of a prime factor (ICISC'08) and Hinek's partial key exposure attacks on Multi-Prime RSA (J. Math. Cryptology '08). We claim that our contribution is not only generalizations or improvements of the existing results. Since our attacks capture general exposure scenarios, the results can be used as a tool kit; the security of some future variants of RSA can be examined without any knowledge of Coppersmith's methods.

(The results will appear in the international conference *CT-RSA 2017* [TK17b].)



Chapter 6: We study the security of Takagi's RSA [Tak98] and the prime power RSA. Both variants have the moduli $N = p^r q$ where r is a fixed constant and p, q are the same bit-size. The public/secret exponent, i.e., e and d, of Takagi's RSA satisfies $ed = 1 \pmod{(p-1)(q-1)}$ whereas that of the prime power RSA satisfies $ed = 1 \pmod{p^{r-1}(p-1)(q-1)}$. For $r = 1$, these variants are the same as the original RSA. Thus far, the small secret exponent attack; the attack for small d, and the partial key exposure attacks; attacks when some portions of the most/least significant bits of d are exposed to attackers, on these variants have been studied in several papers. Itoh, Kunihiro, and Kurosawa [IKK09] proposed the small secret exponent attack on Takagi's RSA. Huang et al. [HHX$^+$14] proposed the partial key exposure attacks on Takagi's RSA. Both attacks on the prime power RSA have studied in several papers [Tak98, May04a, Sar14, LZPL15, Sar16]. However, Itoh et al.'s attack is the only result that is the same as the best attack on the standard RSA for $r = 1$. Furthermore, the spirit of lattice constructions for these attacks are hard to follow due to the complicated moduli $N = p^r q$ and key generation.

In this paper, we propose generic transformations that convert the lattices to attack the standard RSA to lattices to attack Takagi's RSA and the prime power RSA. Hence, our lattice constructions are relatively easy to understand. Moreover, our proposed transformations enable us to construct improved attacks on the variants. Indeed, we propose an improved small secret exponent attack on the prime power RSA and improved partial key exposure attacks on both variants. Although not all our attacks are the same as the best attacks on the standard RSA for $r = 1$, however, we claim that our results are to some extent optimal from our simple lattice constructions. (The results appeared in the international conference *PKC 2016* [TK16a].)

Chapter 2

Preliminaries

In the beginning of this section, we introduce the RSA cryptosystem. In the remaining of this section, we introduce tools to solve modular equations and integer equations; lattices and the LLL algorithm, the overview of Coppersmith's method, and the Jochemsz-May strategy.

2.1 RSA

In this section, we introduce the RSA cryptosystem and its CRT variants.

In 1978, Rivest, Shamir, and Adleman [RSA78] proposed RSA cryptosystems. In this section, we introduce the RSA encryption scheme. Although there is the RSA signature scheme, we omit the definition in this paper.

The original RSA encryption scheme consists of the following three algorithms (Gen, Enc, Dec):

- $\mathsf{Gen}(\lambda)$: On input the security parameter λ, samples two distinct primes p and q with the same bit-size and computes

  $$N = pq.$$

  Next, samples e and d where

  $$ed = 1 \pmod{(p-1)(q-1)}.$$

  Then, $\mathsf{Gen}(\lambda)$ outputs the public key PK and the secret key SK where

  $$\mathsf{PK} := (N, e) \quad \text{and} \quad \mathsf{SK} := (p, q, d).$$

  The message space is defined as $\mathcal{M} := \mathbb{Z}_N^*$.

- $\mathsf{Enc}(\mathsf{PK}, M)$: On input the message $M \in \mathcal{M}$ and the public key (N, e), outputs the ciphertext C where
$$C := M^e \pmod{N}.$$
- $\mathsf{Dec}(\mathsf{PK}, \mathsf{SK}, C)$: On input the chiphertext C and public key N and the secret key d, outputs the message M by computing
$$M = C^d \pmod{N}.$$

Notice that the decryption algorithm outputs the correct message M from Fermat's little theorem. If the public RSA modulus N is factorized, then whole the decryption key including d can be computed efficiently. Hence, the factorization of N should be computationally hard.

For the fast decryption, the Chinese Remainder Theorem is often used. We call the scheme, the CRT-RSA encryption scheme. The CRT-RSA encryption scheme consists of the following three algorithms (Gen, Enc, Dec):

- $\mathsf{Gen}(\lambda)$: On input the security parameter λ, samples two distinct primes p and q with the same bit-size and computes
$$N = pq \quad \text{and} \quad q_{Inv} := q^{-1} \pmod{p}.$$
Next, samples e and d, where
$$ed = 1 \pmod{(p-1)(q-1)},$$
then computes d_p and d_q, where
$$d_p := d \pmod{p-1} \quad \text{and} \quad d_q := d \pmod{q-1}.$$
Then, $\mathsf{Gen}(\lambda)$ outputs the public key PK and the secret key SK, where
$$\mathsf{PK} := (N, e) \quad \text{and} \quad \mathsf{SK} := (p, q, d, d_p, d_q, q_{Inv}).$$
The message space is defined as $\mathcal{M} := \mathbb{Z}_N^*$.
- $\mathsf{Enc}(\mathsf{PK}, M)$: On input the message $M \in \mathcal{M}$ and the public key (N, e), outputs the ciphertext C, where
$$C := M^e \pmod{N}.$$
- $\mathsf{Dec}(\mathsf{PK}, \mathsf{SK}, C)$: On input the chiphertext C and public key N and the secret key $(p, q, d_p, d_q, q_{Inv})$, computes M_p and M_q as
$$M_p := C^{d_p} \pmod{p} \quad \text{and} \quad M_q := C^{d_q} \pmod{q}.$$

Next, computes M' as

$$M' := q_{Inv} \cdot (M_p - M_q) \pmod{p},$$

then outputs M by computing

$$M = M_q + M' \cdot q.$$

The main computational cost of the decryption is the modular exponentiation. The operation in the standard RSA is performed $\pmod{N}$ whereas that in the CRT-RSA is performed $\pmod{p}$ and $\pmod{q}$. Hence, the decryption becomes about four times faster. In Chapter 4, we define d_p and d_q as

$$ed_p := 1 \pmod{p-1} \quad \text{and} \quad ed_q := 1 \pmod{q-1},$$

where the definitions are essentially the same.

2.2 Lattices

In this section, we define an integer lattice in Section 2.2.1 and explain a basic property of the LLL lattice basis reduction algorithm in Section 2.2.2.

2.2.1 Definition

Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{Z}^{n'}$ be linearly independent n'-dimensional vectors. All vectors are row representations. The lattice $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ spanned by the basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is defined as

$$L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{j=1}^{n} c_j \boldsymbol{b}_j : c_j \in \mathbb{Z} \ \text{ for all } j = 1, 2, \ldots, n \right\}.$$

We also use matrix representations $\boldsymbol{B} \in \mathbb{Z}^{n \times n'}$for the bases where each row corresponds to a basis vector $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$. Then, a lattice spanned by the basis matrix $\boldsymbol{B}$ is defined as:

$$L(\boldsymbol{B}) = \{\boldsymbol{cB} : \boldsymbol{c} \in \mathbb{Z}^n\}.$$

We call n a rank of the lattice and n' a dimension of the lattice. We call the lattice full-rank when $n = n'$.

For the same lattice $L(\boldsymbol{B})$, the representation of its basis is not unique. Let $\boldsymbol{U} \in \mathbb{Z}^{n \times n}$ be an arbitrary unimodular matrix, i.e., an integer matrix with $|\det(\boldsymbol{U})| = 1$.

Then, $\boldsymbol{UB}$ is also a basis for $L(\boldsymbol{B})$. We can verify the fact that any lattice points $\boldsymbol{cB}$ in $L(\boldsymbol{B})$ are equal to lattice points $\boldsymbol{c'UB}$ in $L(\boldsymbol{UB})$ where $\boldsymbol{c'} = \boldsymbol{cU}^{-1}$.

Let $\mathcal{P}(\boldsymbol{B})$ be a fundamental parallelpiped of the lattice $L(\boldsymbol{B})$ defined as:

$$\mathcal{P}(\boldsymbol{B}) = \{\boldsymbol{cB} : 0 \leq c_j < 1 \text{ for all } j = 1, 2, \ldots, n\}.$$

Then we define a determinant of the lattice $\det(L(\boldsymbol{B}))$ as n-dimensional volume of the fundamental parallelpiped. The value is computed as:

$$\det(L(\boldsymbol{B})) = \sqrt{\det(\boldsymbol{BB}^T)},$$

where $\boldsymbol{B}^T$ is a traspose of $\boldsymbol{B}$. By definition, the determinant of a full-rank lattice is computed as $\det(L(\boldsymbol{B})) = |\det(\boldsymbol{B})|$. Notice that the determinant is invariant with respect to the representation of a lattice basis.

In cryptographic research, lattices are used in various ways such as cryptographic designs [AD97, GGH97, HPS98, GPV08, Pei09, Reg09, MP12], security proofs [Sho02, FOPS04, KOS10], and cryptanalyses. See [NS01] for more information. In recent years, lattices are considered as one of the main cryptographic tools in cryptographic research. In the context of cryptographic designs, lattice-based schemes are believed as post-quantum ones and the security is guaranteed by the powerful worst-case average-case reduction. Furthermore, thus far, numerous advanced cryptosystems have been constructed such as the fully homomorphic encryption [Gen09, Bra12, GSW13, BGV14, BV14a, BV14b], the functional encryption [ABB10, AFV11, ACM12, CHKP12, Xag13, BGG$^+$14, GV15, GVW15a, GVW15b, AFL16, Yam16, ZCZ16], and the cryptographic Multilinear map [GGH13a, LSS14, GGH15].

2.2.2 LLL Reduction

One of the main cryptographic applications of lattices is the cryptanalysis. In general, cryptanalytic problems are reduced to finding short vectors in integer lattices. Hence, a number of algorithms to find the exact shortest lattice vectors have been proposed, e.g., sieve algorithms [AKS01, NV08, MV10b, ADRS15, Laa15, BDGL16], enumeration [Kan83, FP85, Hel85, HS07, GNR10, MW15, Wal15], random sampling reduction [Sch03, FK15], the voronoi cell computation [MV10a], and more. However, since finding the exact shortest vectors is NP-hard problem under the randomized reduction [Ajt98], these algorithms run in at least exponential time in the lattice dimension.

In 1982, Lenstra, Lenstra, and Lovász [LLL82] proposed a polynomial time algorithm to find short lattice vectors, called the LLL algorithm. Although the LLL algorithm can find only $2^{O(n)}$ approximate shortest lattice vectors in the worst case, it is sufficient for our purpose.

Propostion 1 (LLL algorithm [LLL82, May03])**.** *Given a lattice basis matrix $\boldsymbol{B} \in \mathbb{Z}^{n \times n'}$, the LLL algorithm finds linearly independent vectors $\boldsymbol{b}'_1$ and $\boldsymbol{b}'_2$ in a lattice $L(\boldsymbol{B})$ where Euclidean norms of the vectors are bounded above by*

$$\|\boldsymbol{b}'_1\| \leq 2^{(n-1)/4}(\det(L(\boldsymbol{B})))^{1/n} \quad \textit{and} \quad \|\boldsymbol{b}'_2\| \leq 2^{n/2}(\det(L(\boldsymbol{B})))^{1/(n-1)}.$$

The running time is polynomial time in n, n', and the maximum input length of $\boldsymbol{B}$.

Thus far, faster variants of the LLL reduction [Sch88, KS01, NS05, Sch06, NS09, NSV11, SMSV14, NS16] have been proposed. Furthermore, there exist several blockwise generalizations of the LLL algorithm where they find $2^{O(n \log\log n/\log n)}$ approximate shortest lattice vectors in polynomial time, e.g., the BKZ reduction [Sch87, SE94, CN11, HPS11, AWHT16] and the slide reduction [GN08, Ngu10], and more [GHKN06, MW16]. However, in this paper, we use the LLL reduction that is sufficient for Coppersmith's methods.

2.3 Coppersmith's Methods

In this section, we introduce Coppersmith's methods for solving modular/integer equations with small solutions [Cop96b, Cop96a]. Instead of the original Coppersmith method, we introduce Howgrave-Graham's reformulation to solve modular equations [How97] in Section 2.3.1 and Coron's reformulation to solve integer equations [Cor04] in Section 2.3.2. Although Coron's method [Cor04] is less efficient than the original Coppersmith method [Cop96a] and Coron's other method [Cor07], it is simpler to analyze than the other methods.

For a k-variate polynomial $h(x_1, \ldots, x_k) = \sum h_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$, we define norms of a polynomial as

$$\|h(x_1, \ldots, x_k)\| = \sqrt{\sum h^2_{i_1,\ldots,i_k}} \quad \text{and} \quad \|h(x_1, \ldots, x_k)\|_\infty = \max_{i_1,\ldots,i_k} |h_{i_1,\ldots,i_k}|.$$

2.3.1 Modular Equations Solving Method

At first, we show a modular method since an integer method makes use of the modular method. Coppersmith's method can find solutions $(\tilde{x}_1, \tilde{x}_2)$ of a bivariate modular equation $h(x_1, x_2) = 0 \mod e$ when $|\tilde{x}_1| < X_1, |\tilde{x}_2| < X_2$, and X_1X_2 is reasonably smaller than e. Let m be a positive integer. We construct n polynomials $h_1(x_1, x_2), \ldots, h_n(x_1, x_2)$ that have the root $(\tilde{x}_1, \tilde{x}_2)$ modulo e^m. Then, we construct a matrix $\boldsymbol{B}$ whose rows consist of coefficients of $h_1(x_1X_1, x_2X_2), \ldots, h_n(x_1X_1, x_2X_2)$. Applying the LLL algorithm to $\boldsymbol{B}$ and we obtain two short vectors $\boldsymbol{b}'_1$ and $\boldsymbol{b}'_2$, and their corresponding polynomials $h'(x_1, x_2)$ and $h'_2(x_1, x_2)$. If norms of these polynomials are small, they have the root $(\tilde{x}_1, \tilde{x}_2)$ over the integers. The fact comes from the following lemma.

Lemma 1 (Howgrave-Graham's Lemma [How97])**.** *Let $h(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ be a polynomial over the integers that consists of at most n monomials. Let $X_1, \ldots, X_k$, and R be positive integers. If the polynomial $h(x_1, \ldots, x_k)$ satisfies the following two conditions:*
1. $h(\tilde{x}_1, \ldots, \tilde{x}_k) = 0 \mod R$, where $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_k| < X_k$,
2. $\|h(x_1X_1, \ldots, x_kX_k)\| < R/\sqrt{n}$.
Then, $h(\tilde{x}_1, \ldots, \tilde{x}_k) = 0$ holds over the integers.

Therefore, if $h'(x_1, x_2)$ and $h'_2(x_1, x_2)$ satisfy Howgrave-Graham's lemma, we can compute Gröbner bases or a resultant of them and easily recover $(\tilde{x}_1, \tilde{x}_2)$.

If the basis matrix is triangular, the volume of the lattice $\mathrm{vol}(L(\boldsymbol{B}))$ can be computed as a product of all diagonals. Therefore, when we add an extra polynomial, the polynomial is helpful when the absolute value of the diagonal is less than W^m. Although May [May10] first noted the definition, Takayasu and Kunihiro [TK14d] considered more general definition of helpful polynomials.

Definition 1 (Helpful Polynomials [TK14d])**.** *To solve equations with a modulus W, consider a basis matrix $\boldsymbol{B}$. We add a new shift-polynomial and construct a new basis matrix $\boldsymbol{B}^+$. We call the polynomial a helpful polynomial, provided that*

$$\frac{\det(\boldsymbol{B}^+)}{\det(\boldsymbol{B})} \leq W^m.$$

Conversely, if the inequality does not hold, we call the polynomial an unhelpful polynomial.

To maximize the solvable root bounds, a simple approach is to use as many helpful polynomials as possible and as few unhelpful polynomials as possible as long as basis matrices are triangular.

We should note that the methods need heuristic argument. There are no assurance if new polynomials obtained by outputs of the LLL algorithm are algebraically independent. In this paper, we assume that these polynomials are always algebraically independent and resultants of polynomials will not vanish since there have been few negative reports that contradict the assumption.

2.3.2 Integer Equations Solving Method

Next, we show an integer method. Coppersmith's method can find solutions $(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)$ of a trivariate equation $h(x_1, x_2, x_3) = 0$ over the integers when $|\tilde{x}_1| < X_1, |\tilde{x}_2| < X_2, |\tilde{x}_3| < X_3$, and $X_1X_2X_3$ is reasonably smaller than $\|h(x_1X_1, x_2X_2, x_3X_3)\|_\infty$. Although we omit details of the method, we set a reasonable integer R and remaining procedures are almost the same as modular case by solving a modular equation $h(x_1, x_2, x_3) = 0 \mod R$. If we use the LLL algorithm and obtain small polynomials $h'_1(x_1, x_2, x_3)$ and $h'_2(x_1, x_2, x_3)$ that satisfy Howgrave-Graham's Lemma, they have the same root as $h(x_1, x_2, x_3)$ over the integers. Furthermore, the following Hinek-Stinson's Lemma showed that they are algebraically independent of $h(x_1, x_2, x_3)$.

Lemma 2 (Hinek-Stinson's Lemma [HS06]). *Let $f(x_1, \ldots, x_k)$ and $g(x_1, \ldots, x_k)$ be two non-zero polynomials over $\mathbb{Z}$ of maximum degree δ separately in each variable such that $g(x_1, \ldots, x_k)$ is a multiple of $f(x_1, \ldots, x_k)$ in $\mathbb{Z}[x_1, \ldots, x_k]$. Assume that $f(0, \ldots, 0) \neq 0$ and $g(x_1, \ldots, x_k)$ is divisible by a non-zero integer r such that $\gcd(f(0, \ldots, 0), r) = 1$. Then $g(x_1, \ldots, x_k)$ is divisible by $r \cdot f(x_1, \ldots, x_k)$ and*

$$\|g(x_1, \ldots, x_k)\| \geq 2^{-(\delta+1)^k+1} \cdot |r| \cdot \|f(x_1, \ldots, x_k)\|_\infty.$$

More concretely, if norms of $h'_1(x_1, x_2, x_3)$ and $h'_2(x_1, x_2, x_3)$ are small enough to contradict the inequality of Hinek-Stinson's Lemma, they are algebraically independent of $h(x_1, x_2, x_3)$. See [Cor04] for the detail.

Since the integer method is hard to understand, here, we summarize concrete lattice constructions to solve integer equations based on the Jochemsz-May strategy [JM06]. To the best of our knowledge, there are no algorithms to solve integer equations that are better than the algorithms based on the Jochemsz-May strategy. Let l_j denote the largest exponent of x_j in the polynomial $h(x_1, \ldots, x_k) = \sum h_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k}$. We set an (possibly large) integer W such that $W \leq \|h(x_1, \ldots, x_k)\|_\infty$. Next, we set an integer $R := WX_1^{l_1(m-1)+t} \prod_{u=2}^{k} X_j^{l_u(m-1)}$ with some positive integers m and $t = O(m)$ such that $\gcd(R, h_{0,\ldots,0}) = 1$. We compute $c = h_{0,\ldots,0}^{-1} \mod R$ and

$h'(x_1,\dots,x_k) := c\cdot h(x_1,\dots,x_k) \mod R$. We define shift-polynomials g and g' as

$$\begin{aligned}
&g: x_1^{i_1}\cdots x_k^{i_k}\cdot h(x_1,\dots,x_k)\cdot X_1^{l_1(m-1)+t-i_1}\prod_{u=2}^{k} X_j^{l_u(m-1)-i_j} \quad \text{for } x_1^{i_1}\cdots x_k^{i_k}\in S,\\
&g': x_1^{i_1}\cdots x_k^{i_k}\cdot R \quad \text{for } x_1^{i_1}\cdots x_k^{i_k}\in M\backslash S,
\end{aligned}$$

for sets of monomials

$$\begin{aligned}
S :=& \bigcup_{0\le j\le t}\{x_1^{i_1+j}\cdots x_k^{i_k} | x_1^{i_1}\cdots x_k^{i_k} \text{ is a monomial of } h(x_1,\dots,x_k)^{m-1}\},\\
M :=& \{\text{monomials of } x_1^{i_1}\cdots x_k^{i_k}\cdot h(x_1,\dots,x_k) \text{ for } x_1^{i_1}\cdots x_k^{i_k}\in S\}.
\end{aligned}$$

All these shift-polynomials g and g' modulo R have the roots $(\tilde{x}_1,\dots,\tilde{x}_k)$ that are the same as $h(x_1,\dots,x_k)$. We construct a lattice with coefficients of $g(x_1X_1,\dots,x_kX_k)$ and $g'(x_1X_1,\dots,x_kX_k)$ as the bases. The shift-polynomials generate a triangular basis matrix. Ignoring low order terms of m, LLL outputs short vectors that satisfy Howgrave-Graham's lemma when

$$\prod_{j=1}^{k} X_j^{s_j} < W^{|S|} \text{ for } s_j = \sum_{x_1^{i_1}\cdots x_k^{i_k}\in M\backslash S} i_j.$$

When the condition holds, we can find all small roots. See [JM06] for the detail.

Chapter 3

General Bounds for the Small Inverse Problem

3.1 Introduction

3.1.1 Background

The Small Inverse Problem. In [BD00], Boneh and Durfee introduced the *small inverse problem* (SIP). Given two distinct large integers N and e, the goal of the SIP is finding $\tilde{x}$ and $\tilde{y}$ such that $\tilde{x}$ is an inverse of $N + \tilde{y} \pmod{e}$ where $\tilde{x}$ and $\tilde{y}$ are small, i.e., absolute values of $\tilde{x}$ and $\tilde{y}$ are bounded above by $X := N^{\delta}$ and $Y := N^{\beta}$, respectively. The SIP can be formulated as the following modular equation,

$$x(N + y) \equiv 1 \pmod{e}$$

whose solution is $(x, y) = (\tilde{x}, \tilde{y})$. In this paper, we call the problem the (δ, β)-SIP.

One of the typical cryptographic applications of the SIP is the small secret exponent attack on RSA. Recall RSA key generation

$$ed \equiv 1 \pmod{\Phi(N)},$$

where $\Phi(N) = (p - 1)(q - 1) = N - (p + q) + 1$. We can rewrite the equation as

$$ed + \ell(N - (p + q) + 1) = 1$$

with some integer $\ell < N^{\delta}$. If we can solve the $(\delta, 1/2)$-SIP, i.e., $x(N+y) \equiv 1 \pmod{e}$, whose solution is $(x, y) = (\ell, -(p+q)+1)$, we can factor the RSA modulus N. Notice that $|-(p + q) + 1|$ is bounded above by $N^{1/2}$ within a constant factor since p and

q are the same bit-size. When the public exponent e is full size, the size of the secret exponent d is $\approx \ell < N^{\delta}$. Boneh and Durfee [BD00] proposed lattice-based polynomial time algorithms to solve the $(\delta, 1/2)$-SIP. At first, they proposed an algorithm that works when

$$\delta < \frac{7 - 2\sqrt{7}}{6} = 0.28474 \cdots . \tag{3.1}$$

This result improved the previous bound $\delta < 1/4 = 0.25$ proposed by Wiener [Wie90]. In the same work, Boneh and Durfee further improved the bound to

$$\delta < 1 - \frac{1}{\sqrt{2}} = 0.29289 \cdots . \tag{3.2}$$

To obtain the stronger bound (3.2), they extracted sublattices from the previous lattices that provided the weaker bound (3.1). However, the analysis for computing the determinant of the sublattice is involved since the basis matrix is not triangular.

Boneh and Durfee [BD00] claimed that their bound may not be optimal. They estimated that the bound should be improved to $\delta < 1/2$. Although several papers [BM01, HM10, KSI14] have followed the work, no results that improved the Boneh-Durfee stronger bound (3.2) have been reported and Aono et al. [AASW12] showed some evidence of the optimality of the attack. Blömer and May [BM01] considered different lattice constructions to solve the $(\delta, 1/2)$-SIP. Their algorithm works when

$$\delta < \frac{\sqrt{6} - 1}{5} = 0.28989 \cdots . \tag{3.3}$$

Although the bound (3.3) is inferior to the Boneh-Durfee stronger bound (3.2), it is superior to the weaker bound (3.1). Moreover, dimensions of the Blömer-May lattices are smaller than those of the Boneh-Durfee lattices. However, the analysis for computing the determinant of the lattice is still involved since the basis matrix is not triangular.

Herrmann and May [HM10] revisited the Boneh-Durfee algorithms [BD00]. They used a technique called unravelled linearization [HM09] and analyzed the determinant of the lattice to obtain the stronger bound (3.2). They used the linearization $z = -1 + xy$ and transformed the basis matrices that were not triangular to be triangular. The proof is very simple compared with Boneh and Durfee's original proof [BD00]. Kunihiro, Shinohara, and Izu [KSI14] followed the work and provided a simpler proof for the Blömer-May algorithm [BM01] by using unravelled linearization. Hence, unravelled linearization is a key technique to maximize solvable root bounds of the SIP with simple analyses.

General Bounds for the SIP. The SIP is an important problem in the context of RSA cryptanalyses and has been analyzed in several papers. Then, several variants of the problem have been considered, small secret exponent attacks on variants of RSA [DN00, IKK08], partial key exposure attacks [BM03, EJMdW05, Aon09, SSM10, TK14d], multiple small secret exponent attacks [Aon13, TK14d], and more. To analyze the problem in detail, mathematical generalizations of the SIP [Kun11, Kun12] have also been considered. One of the well considered generalizations is the (δ, β)-SIP for an arbitrary $0 < \beta < 1$, not only $\beta = 1/2$. To study the problem, generalizations of lattices for the $(\delta, 1/2)$-SIP [BD00, BM01] have been analyzed.

Weger [dW02] studied small secret exponent attacks on RSA for a small difference of prime factors, e.g., $|p - q| < N^{\gamma}$ with $\gamma \leq 1/2$. In this case, they revealed that the RSA modulus can be factorized when $(\delta, 2\gamma - 1/2)$-SIP is solved. They extended the Boneh-Durfee lattice constructions and proposed algorithms to solve the (δ, β)-SIP for an arbitrary β. Their algorithms solve the (δ, β)-SIP when

$$\delta < 1 - \sqrt{\beta} \quad \text{for } \frac{1}{4} \leq \beta < 1, \tag{3.4}$$

$$\delta < 1 - \frac{1}{3}\left(2\sqrt{\beta(\beta + 3)} - \beta\right). \tag{3.5}$$

The first bound (3.4) can be obtained by lattice constructions to obtain the Boneh-Durfee stronger bound (3.2) whereas the second bound (3.5) can be obtained by lattice constructions to obtain the Boneh-Durfee weaker bound (3.1). Weger [dW02] also extended Wiener's algorithm [Wie90] for the attack. The algorithm works when

$$\delta < \frac{3}{4} - \beta. \tag{3.6}$$

Although the bound (3.4) is the best among the three bounds, the algorithm works only when $1/4 \leq \beta < 1$. The bound (3.5) is the better when $0 < \beta < 1/8$ whereas the bound (3.6) is the better when $1/8 \leq \beta < 1/4$.

Sarkar et al. [SMS08] studied small secret exponent attacks on RSA for the case when attackers know the most significant bits of a prime factor p. They solved the (δ, β)-SIP for an arbitrary β for the attack. In addition to Weger's results [dW02], Sarkar et al. extended the Blömer-May lattice constructions for the bound (3.3). Sarkar et al.'s algorithm solves the (δ, β)-SIP when

$$\delta < \frac{2}{5}\left(\sqrt{4\beta^2 - \beta + 1} - 3\beta + 1\right). \tag{3.7}$$

The bound is superior to Weger's bound (3.5) and (3.6) when $3/35 \leq \beta < 1/4$.

Kunihiro, Shinohara, and Izu [KSI14] considered a broader class of lattices which is not straightforward generalizations of existing lattices for the $(\delta, 1/2)$-SIP [BD00, BM01]. To solve the (δ, β)-SIP for an arbitrary β, Kunihiro et al. analyzed hybrid lattice constructions that included the Boneh-Durfee lattices for the stronger bound (3.2) and the Blömer-May lattices for the bound (3.3). To be precise, Kunihiro et al. considered a broader class of lattices, and the previous two lattices were special cases of the class. Therefore, there may be chances to improve the previous result by making use of the structures of two lattices, simultaneously. However, their result becomes the same as Weger's bound (3.4) for $1/4 \le \beta < 1$ and Sarkar et al.'s bound (3.7) for $0 < \beta < 1/4$.

Small Secret Exponent Attacks on Multi-Prime RSA with Small Prime Differences. Multi-Prime RSA is a variant of RSA whose public modulus $N = \prod_{j=1}^{k} p_j$ is a product of k distinct primes $p_1, p_2, \ldots, p_k$. The bit length of all prime factors are the same. Key generations of Multi-Prime RSA are the same as that of standard RSA,

$$ed = 1 \pmod{\Phi(N)},$$

where $\Phi(N) = \prod_{j=1}^{k}(p_j - 1)$.

Multi-Prime RSA becomes efficient for its low cost decryption for a large k since the main computation costs are modular exponentiations with $\log N/k$ bits moduli when Chinese Remaindering is used. Moreover, most algebraic attacks become less efficient for a larger k such as small secret exponent attacks [Wie90, BD00] and partial key exposure attacks [BM03, EJMdW05, TK14d]. As the standard RSA (for $k = 2$), Multi-Prime RSA becomes insecure when extremely small secret exponents $d < N^{\delta}$ are used. Ciet et al. [CKLQ02] extended Wiener's [Wie90] and Boneh and Durfee's attacks [BD00]. Extensions of Wiener's attacks work when $\delta < 1/2k$. To extend Boneh and Durfee's attacks, they solved the $(\delta, 1 - 1/k)$-SIP. The algorithms work when $\delta < 1 - \sqrt{1 - 1/k}$. Both bounds become the same as the previous results [Wie90, BD00] for $k = 2$.

Zhang and Takagi [ZT13] analyzed small secret exponent attacks on Multi-Prime RSA with small prime differences[*1]. Assume $p_1 > p_2 > \cdots > p_k$ without loss of generality. Zhang and Takagi analyzed the case when $|p_1 - p_k| < N^{\gamma}$ with $0 < \gamma \le 1/k$ and revealed that Multi-Prime RSA becomes insecure when we can solve the $(\delta, \gamma + 1 - 2/k)$-SIP. After that the same authors [ZT14] gave an improved analysis.

[*1] See also Bahig et al.'s work [BBN12]. They extended Weger's attacks that are based on Wiener's work [Wie90]. The attacks work when $\delta < 1/k - \gamma/2$.

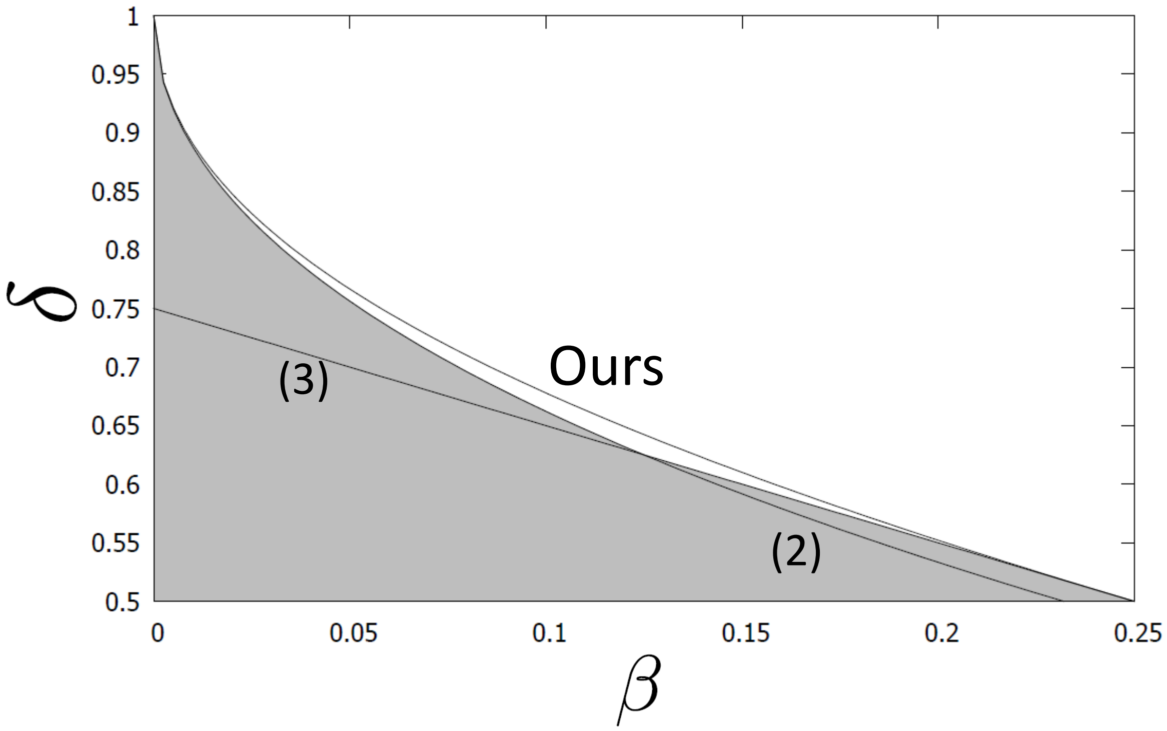


Fig. 3.1. The comparison of the recoverable sizes of δ for $0 \leq \beta \leq 1/4$. Our algorithm works in the left below of the solid line.

Multi-Prime RSA becomes insecure when we can solve the $(\delta, 2\gamma + 1 - 3/k)$-SIP. When $\gamma = 1/k$, the results [ZT13, ZT14] becomes the same as that of Ciet et al.'s results [CKLQ02] that solves the $(\delta, 1 - 1/k)$-SIP. In addition, the improved result for the standard RSA setting, i.e., for $k = 2$, becomes the same as Weger's attack [dW02] that solves the $(\delta, 2\gamma - 1/2)$-SIP.

3.1.2 Our Contributions

In this paper, we study the (δ, β)-SIP for an arbitrary β. At first, we summarize previous lattice constructions [BD00, BM01, dW02, SMS08, KSI14] to obtain the bounds (3.4) to (3.7). We reveal that a generalization of the Blömer-May lattices to obtain the bound (3.7) is not valid for $\beta < 1/4$. Therefore, although Sarkar et al. [SMS08] and Kunihiro et al. [KSI14] claimed that the bound (3.7) is the best when $3/35 < \beta < 1/4$, the results are incorrect. Among previous results, Weger's bound (3.5) and (3.6) is the best for $0 < \beta \leq 1/8$ and $1/8 < \beta < 1/4$, respectively.

Next, we propose an improved algorithm to solve the (δ, β)-SIP for arbitrary β.

Table 3.1. Numerical data of solvable δ for the (δ, β)-SIP.

β	Ours	(3.6) of [dW02]	(3.5) of [dW02]
$1/4 = 0.25$	0.5	0.5	0.482408121
0.225	0.5255002	0.525	0.507109165
0.2	0.552146808	0.55	0.533333333
0.175	0.580217435	0.575	0.561398283
0.15	0.610102051	0.6	0.591742431
$1/8 = 0.125$	0.642374781	0.625	0.625
0.1	0.67793654	0.65	0.662149042
0.075	0.718337521	0.675	0.704843788
0.05	0.766666667	0.7	0.756325011
0.025	0.831074521	0.725	0.825
0	1	0.75	1

The spirit of our approach is the same as Kunihito et al. [KSI14]. We consider a broader class of lattices that include Weger's three lattices to obtain the bounds (3.4)-(3.6) [dW02] for special cases. Therefore, there may be chances to improve the previous results by making use of the structures of previous lattices, simultaneously. Indeed, when $0 < \beta < 1/4$, our algorithm works when

$$\delta < 1 - \frac{2}{3}\left(\sqrt{\beta(3+4\beta)} - \beta\right) \tag{3.8}$$

and the bound is superior to the previous bounds. This means that our lattice constructions make better use of algebraic structures of polynomials than previous analyses to solve the (δ, β)-SIP [dW02]. As several previous works [HM10, KSI14, ZT14], we analyze the determinant of lattices using unravelled linearization. Therefore, the proof is rather simple.

Figure 3.1 compares recoverable sizes of δ between our algorithm and previous ones [dW02, SMS08] to solve the (δ, β)-SIP for $0 \leq \beta \leq 1/4$. Table 3.1 shows the numerical data. When $\beta = 1/4$ and $\beta = 0$, our bound becomes the same as Weger's result $\delta < 0.5$ and $\delta < 1$, respectively. However, our algorithm is better than the two results for $0 < \beta < 1/4$.

As an application of our algorithm, we analyze small secret exponent attacks on Multi-Prime RSA with small prime differences. It is clear that we can improve previous results since our algorithm to solve the (δ, β)-SIP is better than the algorithm which was used in [ZT14].

3.1.3 Roadmap

In Section 3.2, we define the (δ, β)-SIP and recall previous lattice constructions to solve the (δ, β)-SIP. In Section 3.3, we propose our lattice constructions to solve the (δ, β)-SIP for an arbitrary β. In Section 3.4, we analyze small secret exponent attacks on Multi-Prime RSA with small prime differences.

3.2 Previous Lattice Constructions to Solve the (δ, β)-SIP

In Section 3.2.1, we formally define the (δ, β)-SIP and the common approach for the lattice constructions. In Section 3.2.2, we explain the previous lattice constructions [BD00, BM01, dW02, SMS08, HM10, KSI14]. The understanding of the latter section enables readers to understand the spirit of our improvement.

3.2.1 Definition and Approach

In this section, we formally define the (δ, β)-SIP as follows.

Definition 2 (The (δ, β)-SIP)**.** *Given two distinct integers N and e with the same bit-size and real numbers $\delta, \beta \in (0, 1)$, the goal of the the (δ, β)-SIP is finding integers $\tilde{x}$ and $\tilde{y}$ that satisfy $|\tilde{x}| < N^{\delta}$, $|\tilde{y}| < N^{\beta}$, and*

$$\tilde{x}(N + \tilde{y}) \equiv 1 \pmod{e}.$$

In this paper, we also use $X := N^{\delta}$ and $Y := N^{\beta}$ that denote upper bounds of the absolute values of the solutions. Although we only consider the case when two integers N and e are the same bit-size, it is easy to extend the following algorithms to more general cases.

To solve the modular equation

$$f(x, y) = -1 + x(N + y) = 0 \pmod{e},$$

Boneh and Durfee [BD00] used two forms of shift-polynomials,

$$g^{x}_{[i,u]}(x, y) := x^{i-u} f^{u}(x, y) e^{m-u} \quad \text{and} \quad g^{y}_{[u,j]}(x, y) := y^{j} f^{u}(x, y) e^{m-u}.$$

Each polynomial $g^{x}_{[i,u]}(x, y)$ and $g^{y}_{[u,j]}(x, y)$ is called x-shifts and y-shifts, respectively. When all indices i, u, and j are non-negative integers, both polynomials modulo e^{m} have the same root $(\tilde{x}, \tilde{y})$ as $f(x, y)$, i.e., $g^{x}_{[i,u]}(\tilde{x}, \tilde{y}) = 0 \pmod{e^{m}}$ and $g^{y}_{[u,j]}(\tilde{x}, \tilde{y}) = 0$

(mod e^m). Let $\mathcal{I}_x$ and $\mathcal{I}_y$ denote sets of indices and $\boldsymbol{B}$ be the basis matrices that consist of coefficients of shift-polynomials $g^x_{[i,u]}(x,y)$ with indices in $\mathcal{I}_x$ and $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{I}_y$. The selection of shift-polynomials $\mathcal{I}_x$ and $\mathcal{I}_y$ is essential to maximize the solvable root bounds X and Y.

3.2.2 Previous Lattice Constructions

In the rest of this section, we summarize previous lattice constructions [BD00, BM01, dW02, SMS08, HM10, KSI14] to solve the (δ,β)-SIP.

Weaker Boneh-Durfee Lattices. We introduce the Boneh-Durfee lattices [BD00] to obtain the weaker bound (3.1); $\delta < (7-2\sqrt{7})/6$, and its generalization by Weger [dW02] to obtain the bound (3.5); $\delta < \frac{1}{3}(\beta+3-2\sqrt{\beta(\beta+3)})$. Boneh and Durfee defined sets of indices as:

$$\begin{aligned}\mathcal{I}_x^{wBD} &:= \{(i,u)|i=0,1,\ldots,m; u=0,1,\ldots,i\},\\ \mathcal{I}_y^{wBD} &:= \{(u,j)|u=0,1,\ldots,m; j=1,2,\ldots,\lfloor\eta m\rfloor\},\end{aligned}$$

with a parameter $\eta \geq 0$. They constructed basis matrices $\boldsymbol{B}$ whose row vectors consist of coefficients of $g^x_{[i,u]}(x,y)$ with indices in $\mathcal{I}_x^{wBD}$ and $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{I}_y^{wBD}$. The matrices become triangular with diagonals

- $X^iY^ue^{m-u}$ for $g^x_{[i,u]}(x,y)$ and
- $X^uY^{u+j}e^{m-u}$ for $g^y_{[u,j]}(x,y)$.

Ignoring low order terms of m, the dimension and the determinant of the lattices are computed as

$$n = \left(\frac{1}{2}+\eta\right)m^2$$

and

$$\det(\boldsymbol{B}) = X^{(\frac{1}{3}+\frac{\eta}{2})m^3}Y^{(\frac{1}{6}+\frac{\eta(1+\eta)}{2})m^3}e^{(\frac{1}{3}+\frac{\eta}{2})m^3},$$

respectively. The conditions for the (δ,β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^m$, become

$$\delta\left(\frac{1}{3}+\frac{\eta}{2}\right)+\beta\left(\frac{1}{6}+\frac{\eta(1+\eta)}{2}\right)+\left(\frac{1}{3}+\frac{\eta}{2}\right) < \frac{1}{2}+\eta$$

which yields the bound

$$\delta < \frac{1-\beta+3(1-\beta)\eta-3\beta\eta^2}{2+3\eta}.$$

To maximize the right hand side of the inequality, we set the parameter

$$\eta = \frac{-2\beta + \sqrt{\beta(\beta+3)}}{3\beta}$$

and the condition becomes the inequality (3.5);

$$\delta < \frac{1}{3}\left(\beta + 3 - 2\sqrt{\beta(\beta+3)}\right).$$

Stronger Boneh-Durfee Lattices. To improve the bound, Boneh and Durfee [BD00] extracted sublattices from the previous weaker Boneh-Durfee lattices and constructed an algorithm that solves the $(\delta, 1/2)$-SIP when the condition (3.2); $\delta < 1 - 1/\sqrt{2}$, holds. Weger [dW02] generalized the lattice constructions and constructed an algorithm that solves the (δ, β)-SIP when the condition (3.4); $\delta < 1 - \sqrt{\beta}$, holds.

Boneh and Durfee redefined sets of indices as:

$$\mathcal{I}_x^{sBD} := \{(i,u) | i = 0, 1, \ldots, m; u = 0, 1, \ldots, i\},$$
$$\mathcal{I}_y^{sBD} := \{(u,j) | u = 0, 1, \ldots, m; j = 1, 2, \ldots, \lfloor \tau u \rfloor\},$$

with a parameter $0 \leq \tau \leq 1$. They selected shift-polynomials $g^x_{[i,u]}(x,y)$ with indices in $\mathcal{I}_x^{sBD}$ and $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{I}_y^{sBD}$. Although the basis matrices generated by the polynomial selections are not triangular, Herrmann and May [HM10] showed that the matrices can be transformed into triangular with a linearization

$$z = -1 + xy.$$

As the Boneh-Durfee weaker lattice, polynomials in $\mathcal{I}_x^{sBD}$ generate a triangular matrix with diagonals $X^i Y^u e^{m-u}$. When the linearization $z = -1 + xy$ is applied to the polynomials, the matrix is still triangular with diagonals $X^{i-u} Z^u e^{m-u}$. Although the matrix with extra polynomials in $\mathcal{I}_y^{sBD}$ becomes non-triangular, the linearization preserves the matrix to be triangular with diagonals $Y^j Z^u e^{m-u}$. In short, existences of monomials $X^{i-u} Z^u$ for $i = 0, 1, \ldots, m; u = 0, 1, \ldots, i$ (that are equivalent to $X^i Y^u$ for the same set of indices) enable the transformation. To summarize the discussion, the basis matrices become triangular with diagonals

- $X^{i-u} Z^u e^{m-u}$ for $g^x_{[i,u]}(x,y)$ and
- $Y^j Z^u e^{m-u}$ for $g^y_{[u,j]}(x,y)$.

Notice that the analysis requires a restriction $\tau \leq 1$. See [HM10] for the detailed analysis.

Ignoring low order terms of m, the dimension and the determinant of the lattices are computed as

$$n = \left(\frac{1}{2} + \frac{\tau}{2}\right) m^2$$

and

$$\det(\boldsymbol{B}) = X^{\frac{1}{6}m^3} Y^{\frac{\tau^2}{6}m^3} Z^{(\frac{1}{6}+\frac{\tau}{3})m^3} e^{(\frac{1}{3}+\frac{\tau}{6})m^3},$$

respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^m$, becomes

$$\delta \cdot \frac{1}{6} + \beta \cdot \frac{\tau^2}{6} + (\delta + \beta)\left(\frac{1}{6} + \frac{\tau}{3}\right) + \left(\frac{1}{3} + \frac{\tau}{6}\right) < \frac{1}{2} + \frac{\tau}{2}$$

which yields the bound

$$\delta < \frac{1 - \beta + 2(1-\beta)\tau - \beta\tau^2}{2 + 2\tau}.$$

To maximize the right hand side of the inequality, we set the parameter

$$\tau = \sqrt{\frac{1}{\beta}} - 1$$

and the condition becomes the ineqality (3.4);

$$\delta < 1 - \sqrt{\beta}.$$

Although the bound is the best, the algorithm does not work for an arbitrary $0 < \beta < 1$. Since the restriction $0 \le \tau = \sqrt{1/\beta} - 1 \le 1$, the algorithm works only when $1/4 \le \beta \le 1$.

Wiener Lattices. Weger [dW02] also considered the generalization of Wiener's algorithm [Wie90] and obtained the bound (3.6).[*2] The bound can be obtained by the special case of the stronger Boneh-Durfee lattice. We fix the parameter $\tau = 1$ and obtain the condition (3.6);

$$\delta < \frac{3}{4} - \beta.$$

By the definition, the Wiener lattice is the special case of the stronger Boneh-Durfee lattices.

Blömer-May Lattices. Blömer and May [BM01] extracted other sublattices from the weaker Boneh-Durfee lattices and constructed an algorithm that solves the

[*2] In Boneh and Durfee's work [BD00], they obtain the Wiener's bound $\delta < 1/4$ for the $(\delta, 1/2)$-SIP [Wie90]. The bound can be obtained by the special case of the Boneh-Durfee lattice with the fixed parameter $\eta = 0$ or $\tau = 0$.

$(\delta, 1/2)$-SIP when the condition (3.3); $\delta < (\sqrt{6}-1)/5$, holds. Sarkar et al. [SMS08] generalized the lattice constructions and constructed an algorithm that solves the (δ, β)-SIP when the condition (3.7); $\delta < \frac{2}{5}\left(\sqrt{4\beta^2-\beta+1}-3\beta+1\right)$, holds.

Blömer and May defined sets of indices as:

$$\mathcal{I}_x^{BM} := \left\{ (i,u) \middle| \begin{array}{c} i = \lfloor (1-\mu)m \rfloor, \lfloor (1-\mu)m \rfloor + 1, \ldots, m; \\ u = 0, 1, \ldots, i \end{array} \right\},$$
$$\mathcal{I}_y^{BM} := \left\{ (u,j) \middle| \begin{array}{c} u = \lfloor (1-\mu)m \rfloor, \lfloor (1-\mu)m \rfloor + 1, \ldots, m; \\ j = 1, 2, \ldots, \lfloor u - (1-\mu)m \rfloor \end{array} \right\},$$

with a parameter $0 \le \mu < 1$. As the Boneh-Durfee lattices, the basis matrices generated by the polynomial selections are not triangular. Following the work of Herrmann and May [HM10], Kunihiro et al. [KSI14] used the same linearization

$$z = -1 + xy$$

and transformed the basis matrices to be triangular. Applying the linearization appropriately and the basis matrices become triangular with diagonals

- $X^{i-u}Z^u e^{m-u}$ for $g^x_{[i,u]}(x,y)$ and
- $Z^u Y^j e^{m-u}$ for $g^y_{[u,j]}(x,y)$.

See [KSI14] for the detailed analysis. Ignoring low order terms of m, the dimension and the determinant of the lattices are computed as

$$n = \mu m^2$$

and

$$\det(B) = X^{\frac{3\mu-3\mu^2+\mu^3}{6}m^3} Y^{\frac{\mu^3}{6}m^3} Z^{\frac{\mu}{2}m^3} e^{\frac{\mu}{2}m^3},$$

respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^m$, become

$$\delta \cdot \frac{3\mu - 3\mu^2 + \mu^3}{6} + \beta \cdot \frac{\mu^3}{6} + (\delta + \beta) \cdot \frac{\mu}{2} + \frac{\mu}{2} < \mu$$

which yields the bound

$$\delta < \frac{3 - 3\beta - \beta\mu^2}{6 - 3\mu + \mu^2}.$$

To maximize the right hand side of the inequality, we set the parameter

$$\mu = \frac{1 + \beta - \sqrt{4\beta^2 - \beta + 1}}{\beta}$$

and the condition becomes the ineqality (3.7);

$$\delta < \frac{2}{5}\left(\sqrt{4\beta^2 - \beta + 1} - 3\beta + 1\right).$$

Although Sarkar et al. [SMS08] claimed that the bound is the best when $3/35 \leq \beta < 1/4$ for the (δ, β)-SIP, it is incorrect. Since the restriction of the parameter $0 \leq \mu = \left(1 + \beta - \sqrt{4\beta^2 - \beta + 1}\right)/\beta < 1$, the algorithm works only when $1/4 < \beta \leq 1$. In this range, the bound (3.7) is weaker than the generalization of the Boneh-Durfee stronger bound (3.4).

Kunihiro-Shinohara-Izu Lattices. Kunihiro et al. [KSI14] considered a broader class of lattices for the (δ, β)-SIP. They defined sets of indices as:

$$\mathcal{I}_x^{KSI} := \left\{ (i,u) \,\middle|\, \begin{array}{c} i = \lfloor (1-\mu)m \rfloor, \lfloor (1-\mu)m \rfloor + 1, \ldots, m; \\ u = 0, 1, \ldots, i \end{array} \right\},$$

$$\mathcal{I}_y^{KSI} := \left\{ (u,j) \,\middle|\, \begin{array}{c} u = \lfloor (1-\mu)m \rfloor, \lfloor (1-\mu)m \rfloor + 1, \ldots, m; \\ j = 1, 2, \ldots, \lfloor \tau(u - (1-\mu)m) \rfloor \end{array} \right\},$$

with two parameters $0 \leq \tau \leq 1$ and $0 \leq \mu < 1$. The sets are hybrid sets consisting of the stronger Boneh-Durfee lattices and the Blömer-May lattices. More concretely, the previous two lattices are the special cases of the Kunihiro-Shinohara-Izu lattices; when $\tau = 1$, the sets $\mathcal{I}_x^{KSI}$ and $\mathcal{I}_y^{KSI}$ become the same as the sets $\mathcal{I}_x^{sBD}$ and $\mathcal{I}_y^{sBD}$ whereas when $\mu = 1$, the sets $\mathcal{I}_x^{KSI}$ and $\mathcal{I}_y^{KSI}$ become the same as the sets$\mathcal{I}_x^{BM}$ and $\mathcal{I}_y^{BM}$.

As the stronger Boneh-Durfee lattices and the Blömer-May lattices, the basis matrices generated by the polynomial selections are not triangular. Kunihiro et al. [KSI14] used the same linearization

$$z = -1 + xy$$

and transformed the basis matrices to be triangular. Applying the linearization appropriately and the basis matrices become triangular with diagonals

- $X^{i-u}Z^u e^{m-u}$ for $g^x_{[i,u]}(x,y)$ and
- $Z^u Y^j e^{m-u}$ for $g^y_{[u,j]}(x,y)$.

See [KSI14] for the detailed analysis. Ignoring low order terms of m, the dimension and the determinant of the lattices are computed as

$$n = \frac{(2\mu - \mu^2) + \mu^2\tau}{2} m^2$$

and

$$\det(\boldsymbol{B}) = X^{\frac{3\mu-3\mu^2+\mu^3}{6}m^3} Y^{\frac{\mu^3\tau^2}{6}m^3} Z^{\frac{(3\mu-3\mu^2+\mu^3)+(3\mu^2-\mu^3)\tau}{6}m^3} e^{\frac{(3\mu-\mu^3)+\mu^3\tau}{6}m^3},$$

respectively. The conditions for the (δ, β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^m$, become

$$\delta \cdot \frac{3\mu - 3\mu^2 + \mu^3}{6} + \beta \cdot \frac{\mu^3\tau^2}{6} + (\delta + \beta) \cdot \frac{(3\mu - 3\mu^2 + \mu^3) + (3\mu^2 - \mu^3)\tau}{6} \\ + \frac{(3\mu - \mu^3) + \mu^3\tau}{6} < \frac{(2\mu - \mu^2) + \mu^2\tau}{2}$$

which yields the bound

$$\delta < \frac{(1-\beta)((3 - 3\mu + \mu^2) + (3\mu - \mu^2)\tau) - \beta\mu^2\tau^2}{2(3 - 3\mu + \mu^2) + (3\mu - \mu^2)\tau}.$$

When $1/4 \leq \beta < 1$, we set the parameter $\mu = 1, \tau = \sqrt{1/\beta} - 1$, and obtain the bound $\delta < 1 - \sqrt{\beta}$ that is the same as the stronger Boneh-Durfee lattices. When $0 < \beta < 1/4$, we set the parameter $\mu = 1, \tau = 1$, and obtain the bound $\delta < 3/4 - \beta$ that is the same as Wiener's Lattice.[*3]

3.3 New Lattice Constructions to Solve the (δ, β)-SIP

In this section, we propose an improved algorithm to solve the (δ, β)-SIP. Inspired by the work of [KSI14], we consider a broader class of lattices that contains the weaker and stronger Boneh-Durfee lattices, and the Wiener lattices as special cases. The three lattices provide the best results among previous results [dW02, SMS08, KSI14]. When $1/4 \leq \beta < 1$, our hybrid lattices become the same as the stronger Boneh-Durfee lattices and yield the bound (3.4). When $0 < \beta < 1/4$, our lattices make use of the properties of the three lattices, i.e., the weaker and stronger Boneh-Durfee lattices, and the Wiener lattices, simultaneously and obtain the following improved result.

Theorem 1. *There is a polynomial time algorithm to solve the (δ, β)-SIP when the following conditions hold:*

$$\delta < 1 - \sqrt{\beta} \quad \textit{for} \;\; 1/4 \leq \beta < 1,$$
$$\delta < 1 - \frac{2}{3}\left(\sqrt{(3 + 4\beta)\beta} - \beta\right) \quad \textit{for} \;\; 0 < \beta < \frac{1}{4}.$$

[*3] Although Kunihiro et al. [KSI14] claimed the lattices yield the bound (3.7) when $0 < \beta < 1/4$, the result is not correct as we noted above.

3.3.1 The Lattice Construction

To solve the SIP, we define sets of indices

$$\mathcal{I}_x := \{(i,u) | i = 0,1,\ldots,m; u = 0,1,\ldots,i\},$$
$$\mathcal{I}_y := \{(u,j) | u = 0,1,\ldots,m; j = 1,2,\ldots,\lfloor \eta m + \tau u \rfloor\},$$

with two parameters $\eta \geq 0$ and $0 \leq \tau \leq 1$. The sets are hybrid sets with the weaker and stronger Boneh-Durfee lattices, and the Wiener lattices. More concretely, the previous three lattices are the special cases of our lattices; when $\tau = 0$, the sets $\mathcal{I}_x$ and $\mathcal{I}_y$ become the same as the sets $\mathcal{I}_x^{wBD}$ and $\mathcal{I}_y^{wBD}$ whereas when $\eta = 0$, the sets $\mathcal{I}_x$ and $\mathcal{I}_y$ become the same as the sets $\mathcal{I}_x^{sBD}$ and $\mathcal{I}_y^{sBD}$. Since the Wiener lattice is the special case of the stronger Boneh-Durfee lattices, the Wiener lattice is the special case of our lattices.

Our selections of polynomials generate basis matrices $\boldsymbol{B}$ that are not triangular. However, as Herrmann and May's analysis, we use the same linearization

$$z = -1 + xy$$

and the matrices can be transformed into triangular with diagonals

- $X^{i-u} Z^u e^{m-u}$ for $g^x_{[i,u]}(x,y)$ and
- $Z^u Y^j e^{m-u}$ for $g^y_{[u,j]}(x,y)$.

The analysis is almost trivial from the previous analyses. At first, as the case of the weaker Boneh-Durfee lattice, polynomials in $\mathcal{I}_x$ and $\mathcal{I}_y$ for $j = 1,2,\ldots,\lfloor \eta m \rfloor$ generate a triangular matrix with diagonals $X^i Y^u e^{m-u}$ for $\mathcal{I}_x$ and $X^u Y^{u+j} e^{m-u}$ for $\mathcal{I}_y$ and $j = 1,2,\ldots,\lfloor \eta m \rfloor$. When the linearization $z = -1 + xy$ is applied to the polynomials, the matrix is still triangular with diagonals $X^{i-u} Z^u e^{m-u}$ for $g^x_{[i,u]}(x,y)$ and $Z^u Y^j e^{m-u}$ for $g^y_{[u,j]}(x,y)$. Hence, what we have to show is that the matrix is still triangular when we use extra polynomials in $\mathcal{I}_y$ for $u = 0,1,\ldots,m; j = \lfloor \eta m \rfloor + 1, \lfloor \eta m \rfloor + 2, \ldots, \lfloor \eta m + \tau u \rfloor$. Notice that there are monomials $X^i Y^u$ for $i = 0,1,\ldots,m; u = \lfloor \eta m \rfloor, \lfloor \eta m \rfloor + 1, \ldots, \lfloor \eta m \rfloor + i$ that correspond to diagonals for $\mathcal{I}_x$ and for $\mathcal{I}_y$ and $j = 1,2,\ldots,\lfloor \eta m \rfloor$. The extra polynomials $g^y_{[u,j]}(x,y)$ for $u = 0,1,\ldots,m; j = \lfloor \eta m \rfloor + 1, \lfloor \eta m \rfloor + 2, \ldots, \lfloor \eta m + \tau u \rfloor$ are (almost) equivalent to $y^{\lfloor \eta m \rfloor}$ times $g^y_{[u,j]}(x,y)$ with indices in $\mathcal{I}_y^{sBD}$. Therefore, as the Boneh-Durfee stronger lattice, the existences of the monomials $X^i Y^u$ for $i = 0,1,\ldots,m; u = \lfloor \eta m \rfloor, \lfloor \eta m \rfloor + 1, \ldots, \lfloor \eta m \rfloor + i$ preserve the matrix with the extra polynomials to be triangular by using the linearization $z = -1 + xy$. The diagonals for the extra polynomials are $Z^u Y^j e^{m-u}$.

The dimension and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e}$ are computed by

$$\begin{aligned}
n &= \sum_{i=0}^{m}\sum_{u=0}^{i} 1 + \sum_{u=0}^{m}\sum_{j=1}^{\lfloor \eta m+\tau u\rfloor} 1 = \left(\frac{1}{2}+\eta+\frac{\tau}{2}\right) m^2 + o(m^2),\\
s_X + s_Z &= \sum_{i=0}^{m}\sum_{u=0}^{i} i + \sum_{u=0}^{m}\sum_{j=1}^{\lfloor \eta m+\tau u\rfloor} u = \left(\frac{1}{3}+\frac{\eta}{2}+\frac{\tau}{3}\right) m^3 + o(m^3),\\
s_Y + s_Z &= \sum_{i=0}^{m}\sum_{u=0}^{i} u + \sum_{u=0}^{m}\sum_{j=1}^{\lfloor \eta m+\tau u\rfloor} (u+j)\\
&= \left(\frac{1}{6}+\frac{\eta}{2}+\frac{\tau}{3}+\frac{\eta^2}{2}+\frac{\tau\eta}{2}+\frac{\tau^2}{6}\right) m^3 + o(m^3),\\
s_e &= \sum_{i=0}^{m}\sum_{u=0}^{i} (m-u) + \sum_{u=0}^{m}\sum_{j=1}^{\lfloor \eta m+\tau u\rfloor} (t-u) = \left(\frac{1}{3}+\frac{\eta}{2}+\frac{\tau}{6}\right) m^3 + o(m^3).
\end{aligned}$$

Ignoring low order terms of m, the conditions for the (δ, β)-SIP to be solved, i.e., $(\det(\boldsymbol{B}))^{1/n} < e^m$, become

$$\delta < \frac{1-\beta+3(1-\beta)\eta+2(1-\beta)\tau-3\beta\eta^2-3\beta\tau\eta-\beta\tau^2}{2+3\eta+2\tau}.$$

When $1/4 \leq \beta < 1$, to maximize the right hand side of the inequality, we set the parameter $\eta = 0$ and $\tau = \sqrt{1/\beta} - 1$, and obtain the bound

$$\delta < 1 - \sqrt{\beta}$$

that is the same as the bound (3.4).

When $0 < \beta < 1/4$, we set the parameter

$$\eta = \frac{-4\beta + \sqrt{\beta(3+4\beta)}}{3\beta} \quad \text{and} \quad \tau = 1,$$

and obtain the bound

$$\delta < 1 - \frac{2}{3}\left(\sqrt{(3+4\beta)\beta} - \beta\right).$$

This bound is the best among all known results [dW02, SMS08, KSI14] when $0 < \beta < 1/4$.

3.3.2 An Observation of the Lattice

Although the lattice construction is obtained by a simple combination of the previous three lattices, i.e., the weaker and the stronger Boneh-Durfee lattice and the Wiener lattice, the construction should be appropriate. To show the fact, we introduce *helpful polynomials*. The notion was introduced by May [May10], and Takayasu and Kunihiro [TK14a] made use of the notion and proposed improved lattice constructions. In lattice constructions to solve modular equations, we call polynomials helpful if the absolute values of the diagonals are smaller than the modulus in triangular basis matrices. Helpful polynomials enable us to solve modular equations for larger solutions since the polynomials reduce the norm of vectors output by the LLL algorithm. Takayasu and Kunihiro suggested that as many helpful polynomials as possible should be selected in lattice constructions as long as the basis matrices are triangular.

To solve the (δ, β)-SIP for $1/4 \leq \beta < 1$ and $\delta < 1 - \sqrt{\beta}$, the above lattice (that is equivalent to the stronger Boneh-Durfee lattice) contains as many helpful polynomials as possible. That means all $g^y_{[u,j]}(x, y)$ in the lattice basis are helpful polynomials and other $g^y_{[u,j]}(x, y)$ are not helpful since the diagonals $Z^u Y^j e^{m-u}$ for the polynomials $g^y_{[u,j]}(x, y)$ with indices in $u = 0, 1, \ldots, m; j \leq \left(\sqrt{1/\beta} - 1\right) u$ are always equivalent to or smaller than the modulus e^m and and those for the polynomial with indices in $j > \left(\sqrt{1/\beta} - 1\right) u$ are larger than e^m:

$$\begin{aligned} Z^u Y^j e^{m-u} \leq e^m \Leftrightarrow & \left(1 - \sqrt{\beta} + \beta\right) u + \beta j \leq u \\ \Leftrightarrow & j \leq \left(\sqrt{1/\beta} - 1\right) u. \end{aligned}$$

Although not all $g^x_{[i,u]}(x, y)$ in lattice basis are helpful, they contribute the basis matrices to be triangular.

As we explained, the lattice construction is valid only when $\sqrt{1/\beta} - 1 \leq 1$, i.e., $\beta \geq 1/4$, since the unravelled linearization does not work well otherwise. Then we consider to solve the (δ, β)-SIP for $0 < \beta < 1/4$ and $\delta < 1 - \frac{2}{3}\left(\sqrt{(3 + 4\beta)\beta} - \beta\right)$. In this case, not all $g^y_{[u,j]}(x, y)$ in the lattice basis are helpful and not all helpful $g^y_{[u,j]}(x, y)$ are in the lattice basis. However, our lattice construction is the best possible. For the series of $g^y_{[u,j]}(x, y)$ for $u = 0, 1, \ldots, m; j = \eta m + u$ with some η, the corresponding diagonals in the lattice basis are

$$\begin{aligned} Z^u Y^{\eta m + u} e^{m-u} &= N^{(\beta + \delta) u + \beta(\eta m + u) + m - u} \\ &\leq N^{-\frac{2}{3}\left(\sqrt{(3+4\beta)\beta} - 4\beta\right) u + (1 + \eta\beta) m}. \end{aligned}$$

Since $\beta < 1/4$, $\sqrt{(3+4\beta)\beta} - 4\beta > 0$ holds and the diagonals become smaller for larger u. Hence, if possible, we want to select only $g^y_{[u,j]}(x,y)$ for larger u in the lattice basis, however, unravelled linearization does not work well without $g^y_{[u,j]}(x,y)$ for smaller u. Therefore, the best possible lattice construction is collecting as many helpful series of $g^y_{[u,j]}(x,y)$ for $u = 0,1,\ldots,m; j = \eta m + u$ as possible. The helpful series of $g^y_{[u,j]}(x,y)$ for $u = 0,1,\ldots,m; j = \eta m + u$ means the geometric mean of all the diagonals is smaller than the modulus e^m. The geometric mean is calculated as

$$\begin{aligned}\left(\prod_{u=0}^{m} Z^u Y^{\eta m+u} e^{m-u}\right)^{1/(m+1)} &\leq N^{-\frac{1}{3}\left(\sqrt{(3+4\beta)\beta}-4\beta\right)m+(1+\eta\beta)m} \\ &= N^{\left(1-\frac{1}{3}\left(\sqrt{(3+4\beta)\beta}-(4+3\eta)\beta\right)\right)m}.\end{aligned}$$

Hence, the series of $g^y_{[u,j]}(x,y)$ becomes helpful when the geometric mean is smaller than $e^m \approx N^m$, that is,

$$\sqrt{(3+4\beta)\beta} - (4+3\eta)\beta \geq 0 \quad \Leftrightarrow \quad \eta \leq \frac{-4\beta + \sqrt{\beta(3+4\beta)}}{3\beta}.$$

The analysis suggests that our lattice contains all helpful series of $g^y_{[u,j]}(x,y)$ for $u = 0,1,\ldots,m; j = \eta m + u$.

3.4 On the Security of Multi-Prime RSA

In this section, we study the security of Multi-Prime RSA for small differences of the prime factors.

3.4.1 Background and Our Improvement

We write the Multi-Prime RSA modulus as

$$N = p_1 p_2 \cdots p_k$$

and assume the following two conditions $p_1 > p_2 > \cdots > p_k$ without loss of generality, and $|p_1 - p_k| < N^\gamma$. Define

$$p'_j = \frac{N}{p_j}$$

and

$$\Delta_k = \sum_{j=1}^{k} p'_j - k\left(\prod_{j=1}^{k} p'_j\right)^{1/k}.$$

By definition,

$$p'_1 < p'_2 < \cdots < p'_k$$

and

$$k \left(\prod_{j=1}^{k} p'_j \right)^{1/k} = kN^{(k-1)/k}$$

holds.

In [ZT13, ZT14], Zhang and Takagi analyzed the security. They revealed that Multi-Prime RSA becomes insecure if we can solve the (δ, β)-SIP.

Lemma 3 (Proposition 1 and Theorem 2 of [ZT13])**.** *Let $N = p_1 p_2 \cdots p_k$ such that $p_1 > p_2 > \cdots > p_k$ be a Multi-Prime RSA modulus. All prime factors of N are the same bit-size and $p_1 - p_k < N^{\gamma}$, $0 < \gamma < 1/k$. Let e be a full size public exponent whose corresponding secret exponent d is smaller than N^{δ}. When $\Delta_k = \sum_{j=1}^{k} p'_j - k \left(\prod_{j=1}^{k} p'_j \right)^{1/k}$ is smaller than N^{β}, if we can solve the (δ, β)-SIP, we can factor the Multi-Prime RSA modulus N.*

For the attack, bounding the size of Δ_k is crucial. Although Zhang and Takagi [ZT14] obtained a similar bound, i.e., $0 < \Delta_k < \mathit{poly}(k) \cdot N^{2\gamma+1-3/k}$ from Proposition 1 of [ZT14], we show a slightly better bound as follows.

Lemma 4. *Let $N = p_1 p_2 \cdots p_k$ be composite integers and Δ_k be defined as in Lemma 3, then*

$$0 < \Delta_k < 2(k-1) \cdot N^{2\gamma+1-3/k}.$$

Zhang and Takagi [ZT14] used Newton's Generalized Binomial Theorem to bound the size of Δ_k. See [ZT14] for detailed information. Since small $k = 3, 4, 5$ are used in standard settings of Multi-Prime RSA, the term $\mathit{poly}(k)$ can be assumed to be much smaller than N. Therefore, Zhang and Takagi did not analyze the term in detail.

We give an alternative proof for Lemma 4 that does not use Newton's Generalized Binomial Theorem. Moreover, our proof shows $\mathit{poly}(k) = 2(k-1)$. Hence, our result justifies the assumption, e.g., the term $\mathit{poly}(k)$ is much smaller than N. The proof will appear in Section 3.4.2.

Since we proposed an improved algorithm for the (δ, β)-SIP, i.e., Theorem 1, we can improve the cryptanalysis of Multi-Prime RSA. Combining Lemma 3, Lemma 4, and Theorem 1, we obtain the following result.

Theorem 2. *Let the Multi-Prime RSA modulus N, public (resp. secret) exponent e*

(resp. d) as in Lemma 3. We can factor the Multi-Prime RSA modulus N when

$$\delta < 1 - \sqrt{1 + 2\gamma - 3/k} \qquad \textit{for} \ \frac{3}{2}\left(\frac{1}{k} - \frac{1}{4}\right) \le \gamma < \frac{1}{k},$$
$$\delta < 1 - \frac{2}{3}\left(\sqrt{(7 + 8\gamma - 12/k)(1 + 2\gamma - 3/k)} - 1 - 2\gamma + 3/k\right)$$
$$\textit{for} \ \ 0 < \gamma < \frac{3}{2}\left(\frac{1}{k} - \frac{1}{4}\right).$$

3.4.2 Proof of Lemma 4

To prove Lemma 4, we use the following Lemma 5 and Lemma 6. In all following equations, if all indices j for p_j in summations are larger than k, let j be $j-k$.

Lemma 5. *Let $N = p_1 p_2 \cdots p_k$ be composite integers and Δ_k be defined as in Lemma 3, then*

$$\Delta_k = \frac{1}{2}\sum_{u=0}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} \mathcal{P}_{u,j}^{1/k} p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k}\left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2,$$

where

$$\mathcal{P}_{u,j} = \begin{cases} 1 & \textit{for} \ \ u = 0, \\ p'_{j+1}p'_{j+2}\cdots p'_{j+u} & \textit{for} \ \ u = 1, 2, \ldots, k-2. \end{cases}$$

The proof of Lemma 5 is written at the end of this section.

Lemma 6. *Let $N = p_1 p_2 \cdots p_k$ be composite integers, then*

$$\left|p_i'^{1/k} - p_j'^{1/k}\right| \le \frac{2^{(k+1)/k}}{k} \cdot N^{\gamma - 1/k^2},$$

for all $i, j = 1, 2, \ldots, k, i \neq j$.

Proof. By definition,

$$\left|p_i'^{1/k} - p_j'^{1/k}\right| = \left|\frac{1}{p_i^{1/k}} - \frac{1}{p_j^{1/k}}\right| \cdot N^{1/k} = \left|\frac{p_j^{1/k} - p_i^{1/k}}{p_i^{1/k} p_j^{1/k}}\right| \cdot N^{1/k}.$$

By definition, since $p_1 > p_2 > \cdots > p_k$,

$$< \frac{p_1^{1/k} - p_k^{1/k}}{p_k^{2/k}} \cdot N^{1/k} = \frac{p_1 - p_k}{p_k^{2/k}\sum_{l=0}^{k-1} p_1^{(k-l-1)/k} p_k^{l/k}} \cdot N^{1/k}$$

$$< \frac{p_1 - p_k}{p_k^{2/k} \sum_{l=0}^{k-1} p_k^{(k-1)/k}} \cdot N^{1/k} = \frac{p_1 - p_k}{kp_k^{(k+1)/k}} \cdot N^{1/k}.$$

By definition, all prime factors $p_1, p_2, \cdots, p_k$ are the same bit size. Hence, $p_k > \frac{1}{2}N^{1/k}$ holds, then

$$< \frac{N^\gamma}{k\left(\frac{1}{2}N^{1/k}\right)^{(k+1)/k}} \cdot N^{1/k} = \frac{2^{(k+1)/k}}{k} \cdot N^{\gamma - 1/k^2}$$

as required. □

Combining Lemma 5 and Lemma 6, we can prove Lemma 4 as follows.

Proof of Lemma 4. From Lemma 5,

$$\Delta_k = \frac{1}{2}\sum_{u=0}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} \mathcal{P}_{u,j}^{1/k} p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2.$$

By splitting the summation into two parts with respect to $u = 0$ and $u = 1, 2, \ldots, k$,

$$\begin{aligned} =&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2} p_j'^{(k-l-2)/k} p_{j+1}'^{l/k} \left(p_j'^{1/k} - p_{j+1}'^{1/k}\right)^2 \\ &+ \frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2} \left(p_{j+1}'p_{j+2}'\cdots p_{j+u}'\right)^{1/k} \cdot p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k}\right)^2. \end{aligned} \tag{3.9}$$

By definition, since $p_1' < p_2' < \cdots < p_k'$, we bound the first summation of equation (3.9) as

$$\begin{aligned} &\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2} p_j'^{(k-l-2)/k} p_{j+1}'^{l/k} \left(p_j'^{1/k} - p_{j+1}'^{1/k}\right)^2 \\ <&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2} p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k}\right)^2 \\ =&\frac{1}{2}k(k-1)p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k}\right)^2. \end{aligned}$$

As the proof of Lemma 6, since $p_k > \frac{1}{2}N^{1/k}$, $p_k' = N/p_k < 2N^{(k-1)/k}$ holds, then

$$\begin{aligned} &< \frac{1}{2}k(k-1)\left(2N^{(k-1)/k}\right)^{(k-2)/k} \cdot \left(p_k'^{1/k} - p_1'^{1/k}\right)^2 \\ &= \frac{1}{2^{2/k}}k(k-1)N^{(k-1)(k-2)/k^2} \cdot \left(p_k'^{1/k} - p_1'^{1/k}\right)^2. \end{aligned}$$

By Lemma 6,

$$
\begin{aligned}
&< \frac{1}{2^{2/k}} k(k-1) N^{(k-1)(k-2)/k^2} \cdot \left(\frac{2^{(k+1)/k}}{k} N^{\gamma - 1/k^2} \right)^2 \\
&= \frac{4(k-1)}{k} N^{2\gamma+1-3/k}.
\end{aligned}
$$

Next, we bound the second summation of equation (3.9). By definition, since $p'_1 < p'_2 < \cdots < p'_k$,

$$
\begin{aligned}
&\frac{1}{2} \sum_{u=1}^{k-2} \sum_{j=1}^{k} \sum_{l=0}^{k-u-2} \left(p'_{j+1} p'_{j+2} \cdots p'_{j+u}\right)^{1/k} \cdot p_j'^{(k-u-l-2)/k} p_{j+u+1}'^{l/k} \left(p_j'^{1/k} - p_{j+u+1}'^{1/k} \right)^2 \\
<&\frac{1}{2} \sum_{u=1}^{k-2} \sum_{j=1}^{k} \sum_{l=0}^{k-u-2} p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k} \right)^2 \\
=&\frac{(k-2)(k-1)k}{4} \cdot p_k'^{(k-2)/k} \left(p_k'^{1/k} - p_1'^{1/k} \right)^2.
\end{aligned}
$$

Since $p'_k < 2N^{(k-1)/k}$,

$$
\begin{aligned}
&< \frac{(k-2)(k-1)k}{4} \cdot \left(2N^{(k-1)/k} \right)^{(k-2)/k} \cdot \left(p_k'^{1/k} - p_1'^{1/k} \right)^2 \\
&= \frac{(k-2)(k-1)k}{2^{(k+2)/k}} \cdot N^{(k-1)(k-2)/k^2} \cdot \left(p_k'^{1/k} - p_1'^{1/k} \right)^2.
\end{aligned}
$$

By Lemma 6,

$$
\begin{aligned}
&< \frac{(k-2)(k-1)k}{2^{(k+2)/k}} \cdot N^{(k-1)(k-2)/k^2} \cdot \left(\frac{2^{(k+1)/k}}{k} N^{\gamma - 1/k^2} \right)^2 \\
&= \frac{2(k-2)(k-1)}{k} N^{2\gamma+1-3/k}.
\end{aligned}
$$

Therefore, Δ_k is bounded above by

$$
\begin{aligned}
\Delta_k &< \frac{4(k-1)}{k} N^{2\gamma+1-3/k} + \frac{2(k-2)(k-1)}{k} N^{2\gamma+1-3/k} \\
&= 2(k-1) N^{2\gamma+1-3/k}
\end{aligned}
$$

as required. □

In the rest of this section, we prove Lemma 5.

Proof of Lemma 5. We show the following equation

$$
\sum_{j=1}^{k} p'_j = \frac{1}{2} \sum_{j=1}^{k} \sum_{l=0}^{k-2} \left(p_j'^{1/k} - p_{j+1}'^{1/k} \right)^2 p_j'^{(k-l-2)/k} p_{j+1}'^{l/k}
$$

$$+\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot$$
$$p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2$$
$$+k\left(\prod_{j=1}^{k}p'_j\right)^{1/k}$$

that is equivalent to the equation of Lemma 5.

For all $u=2,3,\cdots,k$,

$$\begin{aligned}&\left(p_i'^{1/k}-p_j'^{1/k}\right)^2\sum_{l=0}^{u-2}p_i'^{(u-l-2)/k}p_j'^{l/k}\\ =&\left(p_i'^{1/k}-p_j'^{1/k}\right)\left(p_i'^{(u-1)/k}-p_j'^{(u-1)/k}\right)\\ =&p_i'^{u/k}+p_j'^{u/k}-p_i'^{1/k}p_j'^{(u-1)/k}-p_i'^{(u-1)/k}p_j'^{1/k}.\end{aligned}$$

Hence,

$$\begin{aligned}&p_i'^{u/k}+p_j'^{u/k}\\ =&\left(p_i'^{1/k}-p_j'^{1/k}\right)^2\sum_{l=0}^{u-2}p_i'^{(u-l-2)/k}p_j'^{l/k}+p_i'^{1/k}p_j'^{(u-1)/k}+p_i'^{(u-1)/k}p_j'^{1/k}.\end{aligned}\tag{3.10}$$

Next, by the equation (3.10),

$$\begin{aligned}&\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\left(p_j'^{(k-u)/k}+p_{j+u+1}'^{(k-u)/k}\right)\\ =&\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot[\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2\sum_{l=0}^{k-u-2}p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\\ &+p_j'^{1/k}p_{j+u+1}'^{(k-u-1)/k}+p_j'^{(k-u-1)/k}p_{j+u+1}'^{1/k}]\\ =&\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\\ &+\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}p_{j+u+1}'^{(k-u-1)/k}+p_j'^{(k-u-1)/k}p_{j+u+1}'^{1/k}\right).\end{aligned}$$

From the standard calculation, we slide the indices of the second term as

$$=\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}$$

$$\begin{aligned}
&+\sum_{j=1}^{k}\left[\left(p'_jp'_{j+1}\cdots p'_{j+u}\right)^{1/k}\cdot p'^{(k-u-1)/k}_{j+u+1}+\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u+1}\right)^{1/k}p'^{(k-u-1)/k}_{j}\right]\\
=&\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot\left(p'^{1/k}_j-p'^{1/k}_{j+u+1}\right)^2p'^{(k-u-l-2)/k}_jp'^{l/k}_{j+u+1}\\
&+\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u+1}\right)^{1/k}\left(p'^{(k-u-1)/k}_j+p'^{(k-u-1)/k}_{j+u+2}\right).
\end{aligned}\tag{3.11}$$

Again, by the equation (3.10) for $u=k$,

$$\begin{aligned}
\sum_{j=1}^{k}p'_j=&\frac{1}{2}\sum_{j=1}^{k}\left(p'_j+p'_{j+1}\right)\\
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p'^{1/k}_j-p'^{1/k}_{j+1}\right)^2p'^{(k-l-2)/k}_jp'^{l/k}_{j+1}\\
&+\frac{1}{2}\sum_{j=1}^{k}\left(p'^{1/k}_jp'^{(k-1)/k}_{j+1}+p'^{(k-1)/k}_jp'^{1/k}_{j+1}\right).
\end{aligned}$$

From the standard calculation, we slide the indices of the second term as

$$\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p'^{1/k}_j-p'^{1/k}_{j+1}\right)^2p'^{(k-l-2)/k}_jp'^{l/k}_{j+1}\\
&+\frac{1}{2}\sum_{j=1}^{k}\left(p'^{1/k}_{j+1}p'^{(k-1)/k}_{j+2}+p'^{(k-1)/k}_jp'^{1/k}_{j+1}\right)\\
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p'^{1/k}_j-p'^{1/k}_{j+1}\right)^2p'^{(k-l-2)/k}_jp'^{l/k}_{j+1}+\frac{1}{2}\sum_{j=1}^{k}p'^{1/k}_{j+1}\left(p'^{(k-1)/k}_j+p'^{(k-1)/k}_{j+2}\right).
\end{aligned}$$

For the second term, we recursively apply the transformation of the equation (3.11) for $u=1,2,\ldots,k-1$ and obtain

$$\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p'^{1/k}_j-p'^{1/k}_{j+1}\right)^2p'^{(k-l-2)/k}_jp'^{l/k}_{j+1}\\
&+\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot p'^{(k-u-l-2)/k}_jp'^{l/k}_{j+u+1}\left(p'^{1/k}_j-p'^{1/k}_{j+u+1}\right)^2\\
&+\sum_{j=1}^{k}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+k-2}\right)^{1/k}p'^{1/k}_jp'^{1/k}_{j+k-1}.
\end{aligned}$$

From the fact that

$$\left(p'_{j+1}p'_{j+2}\cdots p'_{j+k-2}\right)^{1/k} p_j'^{1/k} p_{j+k-1}'^{1/k} = \left(\prod_{j=1}^{k} p'_j\right)^{1/k}$$

for all $j = 1, 2, \ldots, k$,

$$\begin{aligned}
=&\frac{1}{2}\sum_{j=1}^{k}\sum_{l=0}^{k-2}\left(p_j'^{1/k}-p_{j+1}'^{1/k}\right)^2 p_j'^{(k-l-2)/k}p_{j+1}'^{l/k}\\
&+\frac{1}{2}\sum_{u=1}^{k-2}\sum_{j=1}^{k}\sum_{l=0}^{k-u-2}\left(p'_{j+1}p'_{j+2}\cdots p'_{j+u}\right)^{1/k}\cdot p_j'^{(k-u-l-2)/k}p_{j+u+1}'^{l/k}\left(p_j'^{1/k}-p_{j+u+1}'^{1/k}\right)^2\\
&+k\left(\prod_{j=1}^{k} p'_j\right)^{1/k}
\end{aligned}$$

as required. □

3.5 Concluding Remarks

In this chapter, we studied the (δ, β)-SIP for an arbitrary β that relates to the security of Multi-Prime RSA. Unlike the results of the $(\delta, 1/2)$-SIP [BD00, BM01, HM10], the results for the general (δ, β)-SIP are not widely known. Indeed, some previous results reconstruct the algorithm to solve the problem, which had already been proved, and did not refer to the previous works. Therefore, one of the contributions of this paper is to summarize the previous results [BD00, BM01, dW02, HM10, KSI14, SMS08]. Moreover, we revealed that the bound (3.7) proposed by previous works [KSI14, SMS08] is not valid.

The main contribution of the paper was to provide the improved lattice construction for the (δ, β)-SIP. Our lattice covers a broader class and previous results [BD00, dW02] that provide the best bounds among previous works are special cases of our lattice. The lattice makes better use of the algebraic structures of modular polynomials and we improved the previous bound.

Based on the improvement, we also showed the improved analysis for the security of Multi-Prime RSA. Our result showed that Multi-Prime RSA is vulnerable than expected when differences of prime factors are small.

Chapter 4

Partial Key Exposure Attacks on CRT-RSA

4.1 Introduction

4.1.1 Background

CRT-RSA. RSA [RSA78] is one of the most famous cryptosystems and is widely used. Let $N = pq$ be a public RSA modulus where prime factors p and q are the same bit-size. A public exponent e and a secret exponent d satisfy $ed = 1 \pmod{(p-1)(q-1)}$. For encryption/verifying and decryption/signing, one should calculate heavy modular exponentiations. To speed up the calculation, one simple solution is using a smaller public/secret exponent. However, the public RSA modulus can be factorized in polynomial time when too small secret exponent is used. At first, Wiener [Wie90] proposed a polynomial time attack on the small secret exponent RSA that works when $d < N^{0.25}$. Later, Boneh and Durfee [BD00] revisited the attack and improved the bound to $d < N^{0.284}$ using Coppersmith's method [Cop96b]. Moreover, they further improved the bound to $d < N^{0.292}$ in the same work.

To thwart the attack and achieve faster calculations for decryption/signing, Chinese Remainder Theorem (CRT) is often used as described by Quisquater and Couvreur [QC82]. Instead of the original secret exponent d, one uses CRT-exponents d_p and d_q which satisfy

$$ed_p = 1 \pmod{(p-1)} \qquad \text{and} \qquad ed_q = 1 \pmod{(q-1)}.$$

However, when too small CRT-exponents are used, analogous attacks to [BD00] have been proposed [May02, GHM05, BM06, JM07, HM10]. Hence, in this chapter, we only focus on a case when $d_p, d_q \approx N^{1/2}$.

Partial Key Exposure Attacks on RSA. It is widely known that factorization and RSA problems become easy when certain amount of secret information is known to attackers. Coppersmith [Cop96a] showed that the half most significant bits of a prime factor suffices to factorize N. There have also been several results which use not explicit bits of prime factors but implicit hints [MR09, SM09b, FMR10, SM11, TK14a, LPZ+15, NIK15].

RSA becomes vulnerable also with partial bits of a secret exponent d. Boneh, Durfee, and Frankel [BDF98] showed that the most/least significant bits (MSBs/LSBs) of a secret exponent d enable us to factorize a public RSA modulus N. Later, several papers revisited the attack [BM03, EJMdW05, Aon09, SSM10, JL12, TK14d], and Ernst et al. [EJMdW05] first revealed that RSA is vulnerable even for a full size public/secret exponent against the attack.

Partial Key Exposure Attacks on CRT-RSA. As with the standard RSA, several attacks that use partial information of d_p and d_q, i.e., partial key exposure attacks on CRT-RSA, have also been studied [BM03, SM09b, LZL14]. Blömer and May [BM03] studied an attack scenario when the MSBs/LSBs of either d_p *or* d_q are known to attackers. We call an attack for the scenario a *single* partial key exposure attack. Blömer-May's attacks work when the public exponent is small; $e < N^{1/4}$ with the MSBs of d_p whereas $e = poly(\log N)$ with the LSBs of d_p. On the other hand, the attacks can recover unknown LSBs/MSBs of a CRT-exponent which are less than $N^{1/4}$ for extremely small e. Lu, Zhang, and Lin [LZL14] revisited Blömer-May's attack. When the MSBs of a CRT-exponent are known, Lu et al.'s attack is inferior to Blömer-May's attack unless the CRT-exponent is significantly smaller than $N^{1/2}$. Since we only study the security of CRT-RSA for $d_p, d_q \approx N^{1/2}$, we do not care Lu et al.'s attack with the MSBs. When the LSBs of a CRT-exponent are known, they proposed two attacks where the first attack works for $e < N^{1/4}$ whereas the second attack works for $e < N^{3/8}$. On the other hand, the first attack can recover larger unknown MSBs than the second attack for small e. For extremely small e, Lu et al.'s first attack can recover unknown MSBs of a CRT-exponent which are less than $N^{1/4}$ as Blömer-May's attack. Therefore, Lu et al.'s attack with the LSBs is always better than or equal to Blömer-May's attack.

Sarkar and Maitra [SM09b] extended partial key exposure scenarios. Unlike the above previous works [BM03, LZL14], Sarkar and Maitra studied an attack scenario when the most significant bits of both d_p *and* d_q are known to attackers. Hence, they utilized more partial information than Blömer-May and Lu et al. We call an attack

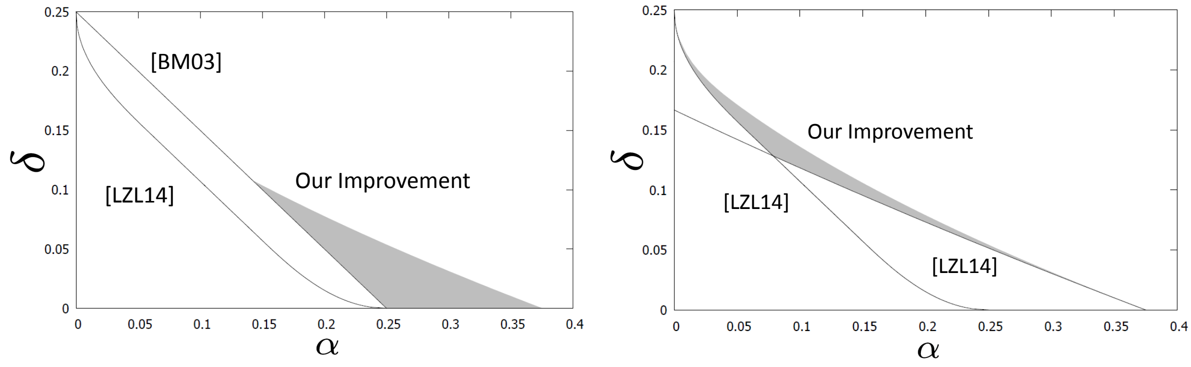


Fig. 4.1. Recoverable conditions for partial key exposure attacks on CRT-RSA when the most significant bits of either d_p or d_q are known to attackers.

for the scenario a *double* partial key exposure attack. To be precise, they also used the MSBs of a prime factor p to construct their attack. For the moment, we ignore the additional hints. Unfortunately, Sarkar and Maitra's attack is not successful. It means that they used more partial information, however, the attack is weaker than other attacks [BM03, LZL14]. In particular, Sarkar and Maitra's attack does not work when $d_p, d_q \approx N^{1/2}$. The attack works only for smaller d_p and d_q.

4.1.2 Our Contributions

In this Chapter, we study single/double partial key exposure attacks on CRT-RSA with the MSBs/LSBs. For all the attack scenarios, we propose improved attacks.

At first, we show that Lu et al.'s single attack with the LSBs does not achieve their claimed bound, hence, we correct the analysis. The corrected attack works for $e < N^{3/8}$ as Lu et al. claimed, however, it requires more partial information than they claimed. Next, we slightly modify Lu et al.'s lattice constructions and obtain an improved attack. The improved attack works for $e < N^{3/8}$ as Lu et al.'s attack, however, it requires less partial information than their attack. We claim that the improvement only stems from a slight modification, hence, it is not very technical.

Technical contributions of this chapter starts from the next improvement. Our observation of the previous attacks [BM03, SM09b, LZL14] including the above corrected attack is that the best attack conditions depend on positions of known bits. For the single scenario, the best attack works for $e < N^{1/4}$ with the MSBs of a CRT-exponent whereas $e < N^{3/8}$ with the LSBs. For the double scenario, there are no attacks with the LSBs. An interesting feature of our improved attacks is that their

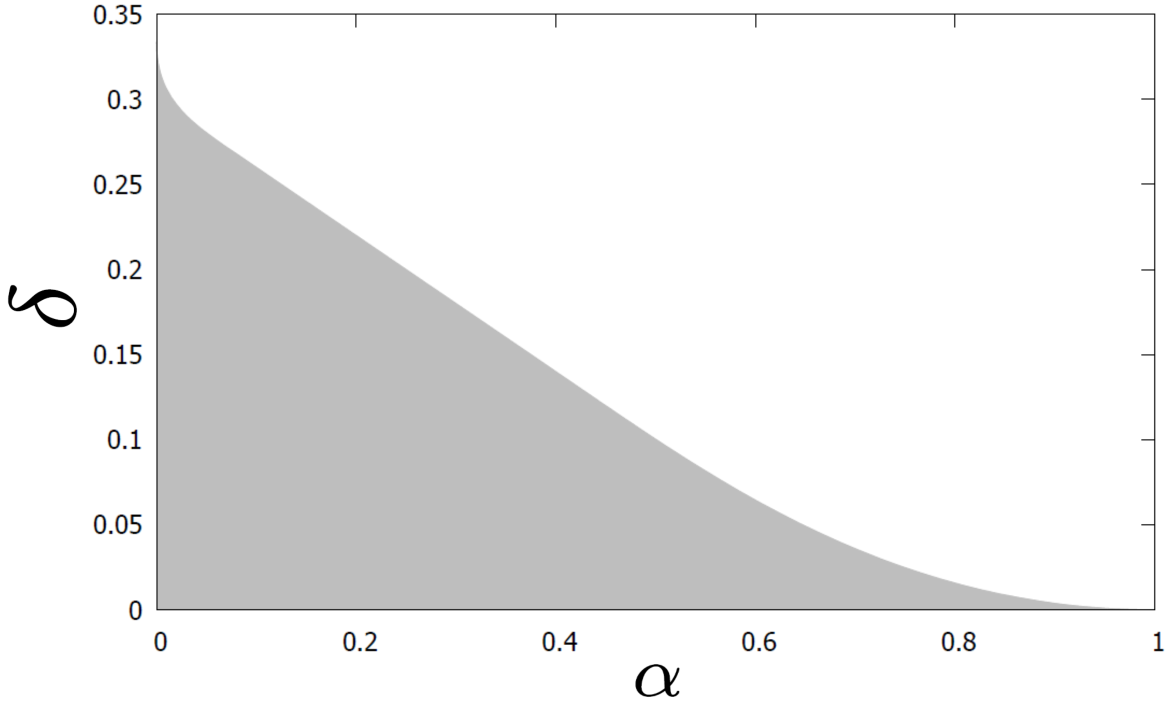


Fig. 4.2. Recoverable conditions for partial key exposure attacks on CRT-RSA when the most/least significant bits of both d_p and d_q are known to attackers.

attack conditions are independent of positions of known bits. Concretely, we propose a single attack with the MSBs where the attack condition is the same as corrected Lu et al.'s attack. Hence, we obtain the first single partial key exposure attack that works for $e < N^{3/8}$. In addition, we propose an improved double attack with the MSBs and the first double attack with the LSBs where their attack conditions are the same. Our double attacks are much better than any single attacks. Our double attacks work for $e < N$ and recover unknown LSBs/MSBs which are less than $N^{1/3}$ for extremely small e.

Notice that Lu et al. proposed two single attacks where the first attack is better than the second attack for small e. The above our single attack with the LSBs only improves Lu et al.'s second attack. It means that the above attack is weaker than Lu et al.'s first attack for small e. However, we further improve a single attack with the LSBs. The attack works for $e < N^{3/8}$ as the previous attacks, however, the attack requires less partial information than the other attack in the range. To summarize, we completely improve Lu et al.'s single attack with the LSBs.

The left of Figure 4.1 compares attack conditions between our attack and Blömer-

May's attack. The right of Figure 4.1 compares attack conditions between our attack and Lu et al.'s attack. Figure 4.2 denotes an attack condition of our proposed attack. Horizontal axis α denotes a size of public exponent; $\alpha = \log_N e$. Vertical axis δ denotes a logarithm of unknown bits with a base N. We obtain improvements in gray areas.

4.1.3 Technical Overview

All the previous partial key exposure attacks on CRT-RSA utilized Coppersmith's methods. The methods have two forms; the first method solves modular equations with small roots whereas the second method solves integer equations with small solutions. To improve attacks is equivalent to constructing algorithms that recover larger solutions. The recoverable sizes depend on two factors; a Newton polytope and a size of a modulus. Note that the integer equation solving method sets a modulus whose size depends on a norm of a polynomial. The simpler Newton polytope of a polynomial is, and the larger the size of the modulus is, the larger solutions can be recovered. To the best of our knowledge, there are no exact criteria to decide which methods, i.e., the modular equation solving method or the integer equation solving method, are the better for each attack scenario in the context of RSA cryptanalysis. Therefore, we should decide which methods to be used appropriately. The appropriate decisions enable us to obtain improved attacks at the first stage.

To maximize solvable solutions for both methods, we should design appropriate lattices. For the purpose, Jochemsz and May [JM06] proposed general strategies for the construction. If we follow the strategy, we can obtain to some extent nice algorithms. Indeed, we do not know how to obtain integer equation solving algorithms that outperform ones based on the Jochemsz-May strategy. However, there are modular equation solving algorithms that outperform ones based on the strategy. For example, the strategy enables us to obtain Boneh-Durfee's weaker attack that works for $d < N^{0.284}$. However, the stronger attack, which works for $d < N^{0.292}$ cannot be captured by the strategy. Therefore, appropriate lattice designs enable us to obtain attacks that outperform ones based on the Jochemsz-May strategy. The appropriate designs enable us to obtain an improved attack at the second stage.

Blömer and May and Lu et al. used the modular equation solving method whereas Sarkar and Maitra used the integer equation solving method. As we suggested, (corrected) Lu et al.'s attack with the LSBs works for larger e than Blömer-May's attack with the MSBs. We show that although the original paper used the modular equation solving method, (corrected) Lu et al.'s attack is also available by using the integer equation solving method. We then show that both integer equations to attack on CRT-RSA with the MSBs and LSBs have the same Newton polytope and are the same norm. This observation is similar to Ernst et al.'s one in the context of partial key exposure attacks on RSA [EJMdW05]. The fact enables us to obtain better attack with the MSBs where the attack works in the same condition as Lu et al, i.e., for larger e. Similarly, we propose double attack with the LSBs that work under the same condition as that with the MSBs.

These attacks are based on the Jochemsz-May strategy. As we noted, we cannot construct integer equation solving algorithms that outperform ones based on the strategy. Among the above attacks which we proposed, corrected Lu et al.'s attack is the only one which is available by solving modular equations. Hence, we analyze the lattices to obtain the attack. Our careful analysis reveals that the lattice bases contain some polynomials that do not contribute to maximize solvable solutions. Then, we omit the useless polynomials from the lattice bases and obtain a better attack. The approach is analogous to one that how Takayasu and Kunihiro [TK14d] improved Ernst et al.'s attack in the context of partial key exposure attacks on RSA. Our proposed attack is the first partial key exposure attack on CRT-RSA that do not rely on the Jochemsz-May strategy.

4.1.4 Roadmap

In Section 4.2, we define the attack scenario for partial key exposure attacks on CRT-RSA and summarize previous results [BM03, SM09b, LZL14]. In Section 4.3, we propose our attacks when the most/least significant bits of either d_p or d_q are known. In Section 4.4, we propose our attacks when the most/least significant bits of both d_p and d_q are known. In Section 4.5,

4.2 Definitions and Previous Works

In Section 4.2.1, we define single/double partial key exposure scenarios. In Section 4.2.2, we summarize previous results proposed in [BM03, SM09b, LZL14].

4.2.1 Definitions of Partial Key Exposure Attacks on CRT-RSA

Let α and β denote the sizes of encryption/CRT exponents, i.e., $e = N^\alpha$ and $d_p, d_q \approx N^\beta$. We study single/double partial key exposure attacks on CRT-RSA; attackers are given the MSBs/LSBs of d_p or/and d_q. Without loss of generality, we assume that attackers know some bits of d_p for the single case. We formulate exposed bits. We write CRT-exponents as

$$d_p = d_{p_0} M + d_{p_1} \qquad \text{and} \qquad d_q = d_{q_0} M + d_{q_1}$$

with some positive integer M. When attackers are given the MSBs of d_p, d_q, they know d_{p_0} and d_{q_0} with some positive integer $M = N^{\delta}$. Attackers do not know the LSBs such that $d_{p_1}, d_{q_1} < N^{\delta}$. Similarly, when attackers are given the LSBs of d_p, d_q, they know d_{p_0}, d_{q_0} with some positive integer $M = N^{\beta-\delta}$. Attackers do not know the MSBs such that $d_{p_1}, d_{q_1} < N^{\delta}$.

4.2.2 Previous Results

We summarize the previous results for single/double partial key exposure attacks on CRT-RSA with the MSBs/LSBs of CRT-exponents.

Theorem 3 (Single MSBs [BM03]). *Let* $0 < \alpha \le 1/4$. *For a single MSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{1}{4} - \alpha,$$

then public RSA modulus N can be factorized in polynomial time.

The attack of Theorem 3 is the best when α is small and β is large.

Theorem 4 (Single LSBs [BM03]). *Let* $e = poly(\log N)$. *For a single LSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \beta - \frac{1}{4},$$

then public RSA modulus N can be factorized in polynomial time.

The attack of Theorem 4 is the first result for the exposed LSBs, however, it works only for extremely small α.

Theorem 5 (Double MSBs Adapted from [SM09b]). *Let* $1/2 - \beta < \alpha < 5/4 - 5\beta/2$. *For a double MSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{(18 - 36\beta - 12\alpha)\tau^2 + (20 - 40\beta - 16\alpha)\tau + 5 - 10\beta - 4\alpha}{24\tau^3 + 30\tau^2 + 16\tau + 4}$$

holds for some $\tau \ge 0$, *then public RSA modulus N can be factorized in polynomial time.*

Theorem attack is the only known result for the double partial key exposure attacks on CRT-RSA, however, it is weaker than even single attacks since the attack of Theorem 5 does not work for $\beta \approx 1/2$.

Theorem 6 (Single MSBs/LSBs [LZL14])**.** *Let $1/2 < \alpha + \beta < 3/4$. For a single MSBs/LSBs partial key exposure attacks on CRT-RSA, when*

$$\left(\alpha+\beta-\frac{1}{2}\right)\left(\frac{3}{2}-\delta-2\sqrt{\alpha+\beta-\delta-\frac{1}{2}}\right)<\frac{1}{8} \quad \textit{for} \;\; 1-\frac{\sqrt{2}}{4}\le\alpha+\beta<\frac{3}{4},$$

$$\alpha+\beta+\delta<\frac{1}{\sqrt{2}},$$

$$\delta\left(2-\alpha-\beta-2\sqrt{\delta-\alpha-\beta+\frac{1}{2}}\right)<\frac{1}{8} \quad \textit{for} \;\; \frac{1}{2}<\alpha+\beta\le\frac{3\sqrt{2}}{4}-\frac{1}{2},$$

then public RSA modulus N can be factorized in polynomial time.

The attack is the best single attack with the LSBs for small α. Although the attack with the MSBs is stronger than Blömer-May's attack of Theorem 4 for small β, it is weaker for $\beta \approx 1/2$. Note that the second condition is valid when $1/2 < \alpha+\beta \le 1/\sqrt{2}$ and better than the other conditions when $3\sqrt{2}/4 - 1/2 < \alpha+\beta < 1-\sqrt{2}/4$.

Theorem 7 (Single LSBs Adapted from [LZL14])**.** *Let $1/2 < \alpha + \beta \le 7/8$. For a single LSBs partial key exposure attacks on CRT-RSA, when*

$$\delta<\frac{5-2\sqrt{1+6(\alpha+\beta)}}{6},$$

then public RSA modulus N can be factorized in polynomial time.

The attack is the best for large α and the first result which works for $1/4 < \alpha \le 3/8$. Note that the condition of Theorem 7 is slightly worse than that was written in [LZL14]. In Section 4.3.1, we show that Lu et al.'s analysis in [LZL14] is not valid. Then we compute the valid condition of Theorem 7 in the section.

4.3 Single Partial Key Exposure Attacks on CRT-RSA by Solving Integer Equations

In this section, we study the single MSBs/LSBs partial key exposure attacks on CRT-RSA and show the following result.

Theorem 8 (Single MSBs/LSBs). *Let $1/2 < \alpha+\beta \leq 7/8$. For the single MSBs/LSBs partial key exposure attacks on CRT-RSA, when*

$$-5 + 8(\alpha+\beta) + 8\delta - 12\delta^2 - 2(1-4\delta)\sqrt{1-4\delta} < 0,$$

then public RSA modulus N can be factorized in polynomial time.

When the MSBs are given, the attack is the first result that works for $1/4 < \alpha \leq 3/8$. When the LSBs are given, the attack works for $\alpha \leq 3/8$ as Lu et al.'s attack of Theorem 7. However, our attack is better than Lu et al.'s attack for large α.

In Section 4.3.1, we correct Lu et al.'s attack with the LSBs. Concretely, we compute the attack condition of Theorem 7 by solving modular equations with the same lattices which are used in [LZL14]. Then, we slightly modify the lattices and propose an improved attack of Theorem 8. Although the attack construction is only applicable for the exposed LSBs, we solve integer equations and propose an attack of Theorem 8 with the exposed MSBs. In Section 4.3.2, we solve integer equations by following the Jochemsz-May basic strategy and propose attacks that work the same condition as the second condition of Theorem 6. Furthermore, in Section 4.3.3, we solve integer equations by following the Jochemsz-May extended strategy and propose attack of Theorem 8.

4.3.1 A Correction and an Improvement of Lu et al.'s Attack

Recall the CRT-RSA key generation:

$$e(d_{p_0}M + d_{p_1}) = 1 \pmod{(p-1)}$$

which can be rewritten as

$$e(d_{p_0}M + d_{p_1}) = 1 + \ell(p-1)$$

with some integer ℓ. Since

$$\ell = \frac{ed_p - 1}{p-1} < \frac{ed_p}{\sqrt{N}/2},$$

the absolute value of ℓ is bounded above by $N^{\alpha+\beta-1/2}$ within a constant factor. For the single LSBs partial key exposure attacks on CRT-RSA, Lu et al. [LZL14] considered a modular polynomial

$$f_{LZL}(x,y) := 1 - ed_{p_1} + x(y-1) \pmod{eM}$$

whose root is $(x, y) = (\ell, p)$. They also used an additional variable $z = q$ and the Durfee-Nguyen technique [DN00]; $yz = N$, which Bleichenbacher and May [BM06] first used to attack CRT-RSA. Absolute values of the root are bounded above by $X := N^{\alpha+\beta-1/2}, Y := N^{1/2}, Z := N^{1/2}$ within constant factors.

To solve a modular equation $f_{LZL}(x, y) = 0$, they constructed a lattice whose basis consists of the following shift-polynomials:

$$g^{LZL1}_{[i,j]}(x, y, z) = x^j z^s f_{LZL}(x, y)^i (eM)^{m-i},$$
$$g^{LZL2}_{[i,j]}(x, y, z) = y^j z^s f_{LZL}(x, y)^i (eM)^{m-i},$$

where $s = \eta m$. These polynomials modulo $(eM)^m$ have the same root as the original modular polynomial, i.e., $g^{LZL1}_{[i,j]}(\ell, p, q) = 0 \pmod{(eM)^m}$ and $g^{LZL2}_{[i,j]}(\ell, p, q) = 0 \pmod{(eM)^m}$. Then they collected shift-polynomials

$$g^{LZL1}_{[i,j]}(x, y, z) \quad \text{for } i = 0, 1, \ldots, m; j = 0, 1, \ldots, m - i,$$
$$g^{LZL2}_{[i,j]}(x, y, z) \quad \text{for } i = 0, 1, \ldots, m; j = 1, 2, \ldots, t,$$

where $t = \tau m$ in lattice bases. To reduce a determinant of the lattice, they multiply the inverse of N modulo $(eM)^m$. This operation eliminates the powers of N in diagonals.

In [LZL14], Lu et al. computed a dimension of the lattice

$$n = \sum_{i=0}^{m}\sum_{j=0}^{m-i} 1 + \sum_{i=0}^{m}\sum_{j=1}^{t} 1 = \left(\frac{1}{2} + \tau\right) m^2 + o(m^2),$$

and a determinant of the lattice $\det(L(\boldsymbol{B})) = (eM)^{s_{eM}} X^{s_X} Y^{s_Y} Z^{s_Z}$, where

$$\begin{aligned}
s_{eM} &= \sum_{i=0}^{m}\sum_{j=0}^{m-i}(m-i) + \sum_{i=0}^{m}\sum_{j=1}^{t}(m-i) = \left(\frac{1}{3} + \frac{\tau}{2}\right) m^3 + o(m^3),\\
s_X &= \sum_{i=0}^{m}\sum_{j=0}^{m-i}(i+j) + \sum_{i=0}^{m}\sum_{j=1}^{t} i = \left(\frac{1}{3} + \frac{\tau}{2}\right) m^3 + o(m^3),\\
s_Y &= \sum_{i=s}^{m}\sum_{j=0}^{m-i}(i-s) + \sum_{i=0}^{m}\sum_{j=\max\{1,s-i\}}^{t}(i+j-s)\\
&= \left(\frac{(1+\tau-\eta)^3}{6} - \frac{(\tau-\eta)^3}{6}\right) m^3 + o(m^3),\\
s_Z &= \sum_{i=0}^{s}\sum_{j=0}^{m-i}(s-i) + \sum_{i=0}^{s}\sum_{j=1}^{s-i}(s-i-j) = \frac{\eta^2}{2} m^3 + o(m^3).
\end{aligned}$$

We should note that this computation has restrictions

$$\eta \leq 1 \ \text{ and } \ \eta \leq \tau.$$

The lattice yileds a condition $X^{s_X} Y^{s_Y} Z^{s_Z} < (eM)^{mn - s_{eM}}$. Ignoring low order terms of m, the condition becomes

$$\begin{aligned}&\left(\alpha + \beta - \frac{1}{2}\right)\left(\frac{1}{3} + \frac{\tau}{2}\right) + \frac{1}{2}\left(\frac{(1+\tau-\eta)^3}{6} - \frac{(\tau-\eta)^3}{6} + \frac{\eta^2}{2}\right)\\ &< (\alpha + \beta - \delta)\left(\frac{1}{2} + \tau - \frac{1}{3} - \frac{\tau}{2}\right).\end{aligned}$$

Optimizing parameters

$$\eta = \frac{1-2\delta}{2} \ \text{ and } \ \tau = \frac{1-4\delta}{2},$$

they obtained the condition

$$24\delta^2 - 20\delta + 7 - 8(\alpha+\beta) > 0$$

which yields the bound

$$\delta < \frac{5 - \sqrt{48(\alpha+\beta) - 17}}{12}.$$

This bound is slightly better than that of Theorem 7. However, the bound is not correct since the restriction $\eta \leq \tau$ does not hold. Under the restriction, valid optimized parameters are

$$\eta = \tau = \frac{1-2\delta}{2}.$$

These parameters hold the restrictions $\eta \leq 1$ and $\eta \leq \tau$. With the parameters, we can obtain the valid condition

$$12\delta^2 - 20\delta + 7 - 8(\alpha+\beta) > 0$$

which yields the bound of Theorem 7;

$$\delta < \frac{5 - 2\sqrt{6(\alpha+\beta)+1}}{6}.$$

4.3.2 Attacks Based on the Jochemsz-May Basic Strategy

At first, we start from the attack which is based on the Jochemsz-May basic strategy. The result is interesting since the lattice construction yields the second condition of Theorem 6.

For the single MSBs partial key exposure attack on CRT-RSA, looking at CRT-RSA key generation,

$$e(d_{p_0}M + d_{p_1}) = 1 + \ell(p-1)$$

with some integer ℓ whose absolute value is bounded above by $N^{\alpha+\beta-1/2}$ within a constant factor. We consider a polynomial over the integers

$$f_{sMSBs}(x, y, z_1) := c_{sMSBs} + ex + y(z_1 - 1)$$

whose root is $(x, y, z_1) = (-d_{p_1}, \ell, p)$ where $c_{sMSBs} = 1 - ed_{p_0}M$. If we can find two polynomials which have the same roots over the integers as f_{sMSBs}, we can recover the roots. We also use an additional variable $z_2 = q$ and the Durfee-Nguyen technique [DN00]; $z_1 z_2 = N$, which Bleichenbacher and May [BM06] and Lu et al. [LZL14] used to attack CRT-RSA. Absolute values of the solution are bounded above by $X := N^{\delta}, Y := N^{\alpha+\beta-1/2}, Z_1 := 2N^{1/2}$ within constant factors. For the notational convenience, we also use $Z_2 := N/Z_1$. Notice that Z_2 is not the upper bound of q. Furthermore, Z_2 is not an integer.

We set an integer

$$W_{sMSBs} := N^{\alpha+\beta}$$

since $\|f_{sMSBs}(x, y, z_1)\|_\infty \geq |c_{sMSBs}| \approx N^{\alpha+\beta}$. Next, we set an integer

$$\begin{aligned} R_{s1} &:= W_{sMSBs}(XY)^{m-1} Z_1^{m-1} Z_2^{k} \\ &= W_{sMSBs}(XY)^{m-1} Z_1^{m-k-1} N^{k} \end{aligned}$$

with some integer m and $k = \eta m$ with a restriction

$$0 \leq \eta \leq 1$$

such that $\gcd(c_{sMSBs}, R_{s1}) = 1$. We compute $a_{sMSBs1} = c_{sMSBs}^{-1} \pmod{R_{s1}}$ and

$$f'_{sMSBs1}(x, y, z_1) := a_{sMSBs1} \cdot f_{sMSBs}(x, y, z_1) \pmod{R_{s1}}.$$

Clearly, $f'_{sMSBs1}(x, y, z_1) \pmod{R_{s1}}$ has the same root as $f_{sMSBs}(x, y, z_1)$.

Then we define a set of shift-polynomials g_{sMSBs1}, g_{sMSBs2} and g'_{sMSBs1}, g'_{sMSBs2} as

$$\begin{aligned}
g_{sMSBs1} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot f'_{sMSBs1}(x,y,z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1+k-i_{z_1}} Z_2^k \\
&\quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s1}, \\
g_{sMSBs2} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot f'_{sMSBs1}(x,y,z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1} Z_2^{i_{z_1}} \\
&\quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s2}, \\
g'_{sMSBs1} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot R_{s1} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s1} \backslash (S_{s1} \cup S_{s2}), \\
g'_{sMSBs2} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot R_{s1} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s2} \backslash (S_{s1} \cup S_{s2}),
\end{aligned}$$

for

$$\begin{aligned}
S_1 &:= \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}} | x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'_{sMSBs1}(x,y,z_1)^{m-1} \text{ and } i_{z_1} \geq k \right\}, \\
S_2 &:= \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}} | x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'_{sMSBs1}(x,y,z_1)^{m-1} \text{ and } i_{z_1} < k \right\}, \\
M_1 &:= \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}} \middle| \begin{array}{c} \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'_{sMSBs1}(x,y,z_1) \\ \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s1} \cup S_{s2} \text{ and } i_{z_1} \geq k \end{array} \right\}, \\
M_2 &:= \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}} \middle| \begin{array}{c} \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'_{sMSBs1}(x,y,z_1) \\ \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s1} \cup S_{s2} \text{ and } i_{z_1} < k \end{array} \right\}.
\end{aligned}$$

For shift-polynomials g_{sMSBs2}, we eliminate the term $z_1 z_2$ by using the Durfee-Nguyen technique $z_1 z_2 = N$. By definition, the set of indices are the same as:

$$\begin{aligned}
S_{s1} &\Leftrightarrow i_x = 0, 1, \ldots, m-1-k; i_y = k, k+1, \ldots, m-1-i_x; \\
&\qquad i_{z_1} = k, k+1, \ldots, m-1-i_x, \\
S_{s2} &\Leftrightarrow i_x = 0, 1, \ldots, m-1; i_y = 0, 1, \ldots, m-1-i_x; \\
&\qquad i_{z_1} = 0, 1, \ldots, \min\{k-1, m-1-i_x\}, \\
M_{s1} &\Leftrightarrow i_x = 0, 1, \ldots, m-k; i_y = k, k+1, \ldots, m-i_x; i_{z_1} = k, k+1, \ldots, m-i_x, \\
M_{s2} &\Leftrightarrow i_x = 0, 1, \ldots, m; i_y = 0, 1, \ldots, m-i_x; i_{z_1} = 0, 1, \ldots, \min\{k-1, m-i_x\}.
\end{aligned}$$

All these shift-polynomials $g_{sMSBs1}(x,y,z_1,z_2), g_{sMSBs2}(x,y,z_1,z_2)$ and $g'_{sMSBs1}(x,y,z_1,z_2), g'_{sMSBs2}(x,y,z_1,z_2)$ modulo R_{s1} have the root $(x,y,z_1,z_2) = (-d_{p_1}, \ell, p, q)$ which are the same as $f_{sMSBs}(x,y,z_1)$ and the definition of z_2. In addition, all these shift-polynomials $g_{sMSBs1}(xX, yY, z_1Z_1, z_2Z_2), g_{sMSBs2}(xX, yY, z_1Z_1, z_2Z_2)$ and

$g'_{sMSBs1}(xX, yY, z_1Z_1, z_2Z_2), g'_{sMSBs2}(xX, yY, z_1Z_1, z_2Z_2)$ are divisible by $X^{m-1}Y^{m-1}Z_1^{m-1}Z_2^k = X^{m-1}Y^{m-1}Z_1^{m-k-1}N^k$. We construct a lattice with coefficient vectors of $g_{sMSBs1}(xX, yY, z_1Z_1, z_2Z_2), g_{sMSBs2}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{sMSBs1}(xX, yY, z_1Z_1, z_2Z_2), g'_{sMSBs2}(xX, yY, z_1Z_1, z_2Z_2)$ as the bases. We can obtain two polynomials $h_{s1}(x, y, z_1, z_2)$ and $h_{s2}(x, y, z_1, z_2)$ from LLL outputs. Then, $\tilde{h}_{s1}(x, y, z_1) := z_1^k \cdot h_{s1}(x, y, z_1, z_2)$ and $\tilde{h}_{s2}(x, y, z_1) := z_1^k \cdot h_{s1}(x, y, z_1, z_2)$, which have the root $(x, y, z_1) = (-d_{p_1}, \ell, p)$ modulo $R_{s1} \cdot p^k$, have the root over the integers if the polynomials satisfy Howgrave-Graham's Lemma. In addition, the polynomials $\tilde{h}_{s1}(xX, yY, z_1Z_1)$ and $\tilde{h}_{s2}(xX, yY, z_1Z_1)$ with a common divisor $X^{m-1}Y^{m-1}Z_1^{m-1}N^k$ are algebraically independent of $f_{sMSBs}(x, y, z_1)$ if they contradict to Hinek-Stinson's Lemma. Based on the Jochemsz-May basic strategy [JM06], the conditions can be written as

$$X^{\frac{m^3}{6}+o(m^3)}Y^{\frac{m^3}{3}+o(m^3)}Z_1^{\frac{(1-\eta)^3}{6}m^3+o(m^3)}Z_2^{\left(\frac{\eta^2}{2}-\frac{\eta^3}{6}\right)m^3+o(m^3)} < W_{sMSBs}^{\frac{m^3}{6}+o(m^3)}.$$

Ignoring low order terms of m, and the condition becomes

$$\delta \cdot \frac{1}{6} + \left(\alpha + \beta - \frac{1}{2}\right) \cdot \frac{1}{3} + \frac{1}{2} \cdot \left(\frac{(1-\eta)^3}{6} + \frac{\eta^2}{2} - \frac{\eta^3}{6}\right) < (\alpha + \beta) \cdot \frac{1}{6}.$$

The detailed calculation will be discussed later. We optimize the parameter

$$\eta = 1 - \frac{1}{\sqrt{2}}$$

which satisfies $0 \leq \eta \leq 1$ and obtain the condition,

$$\alpha + \beta + \delta < \frac{1}{\sqrt{2}}.$$

The condition corresponds to the second condition of Theorem 6.

4.3.3 Attacks Based on the Jochemsz-May Extended Strategy

Next, we show our lattice construction based on the Jochemsz-May extended strategy. The lattice construction enables us to solve the equation $f_{sMSBs}(x, y, z_1) = 0$ for larger $\alpha + \beta$ and yields the condition of Theorem 8.

We set an integer

$$\begin{aligned} R_{s2} &:= W_{sMSBs}(XY)^{m-1}Z_1^{m-1+t}Z_2^k \\ &= W_{sMSBs}(XY)^{m-1}Z_1^{m-1-k+t}N^k \end{aligned}$$

with some integers $m, k = \eta m$, and $t = \tau m$ with restrictions

$$0 \leq \tau \leq \eta \leq 1$$

such that $\gcd(c_{sMSBs}, R_{s2}) = 1$. We compute a_{sMSBs2} and

$$f'_{sMSBs2}(x, y, z_1) := a_{sMSBs2} \cdot f_{sMSBs}(x, y, z_1) \pmod{R_{s2}}$$

as in the basic strategy and define a set of shift-polynomials g_{sMSBs3}, g_{sMSBs4} and g'_{sMSBs3}, g'_{sMSBs4} as

$$\begin{aligned}
g_{sMSBs3} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot f'_{sMSBs2}(x, y, z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1+k+t-i_{z_1}} Z_2^k \\
&\qquad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s3}, \\
g_{sMSBs4} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot f'_{sMSBs2}(x, y, z_1) X^{m-1-i_x} Y^{m-1-i_y} Z_1^{m-1+t} Z_2^{i_{z_1}} \\
&\qquad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in S_{s4}, \\
g'_{sMSBs3} &: x^{i_x} y^{i_y} z_1^{i_{z_1}-k} \cdot R_{s2} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s3} \backslash (S_{s3} \cup S_{s4}), \\
g'_{sMSBs4} &: x^{i_x} y^{i_y} z_2^{k-i_{z_1}} \cdot R_{s2} \quad \text{for } x^{i_x} y^{i_y} z_1^{i_{z_1}} \in M_{s4} \backslash (S_{s3} \cup S_{s4}),
\end{aligned}$$

for

$$S_{s3} := \bigcup_{0 \leq j \leq t} \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}+j} \;\middle|\; \begin{array}{c} x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'_{sMSBs2}(x, y, z_1)^{m-1} \\ \text{for } i_{z_1} \geq k \end{array} \right\},$$

$$S_{s4} := \bigcup_{0 \leq j \leq t} \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}+j} \;\middle|\; \begin{array}{c} x^{i_x} y^{i_y} z_1^{i_{z_1}} \text{ is a monomial of } f'_{sMSBs2}(x, y, z_1)^{m-1} \\ \text{for } i_{z_1} < k \end{array} \right\},$$

$$M_{s3} := \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}} \;\middle|\; \begin{array}{c} \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'_{sMSBs2}(x, y, z_1) \\ \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s3} \cup S_{s4} \text{ and } i_{z_1} \geq k \end{array} \right\},$$

$$M_{s4} := \left\{ x^{i_x} y^{i_y} z_1^{i_{z_1}} \;\middle|\; \begin{array}{c} \text{monomials of } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \cdot f'_{sMSBs2}(x, y, z_1) \\ \text{for } x^{i'_x} y^{i'_y} z_1^{i'_{z_1}} \in S_{s3} \cup S_{s4} \text{ and } i_{z_1} < k \end{array} \right\}.$$

For shift-polynomials g_{sMSBs4}, we eliminate the term $z_1 z_2$ by using the Durfee-Nguyen technique $z_1 z_2 = N$. By definition, the set of indices are the same as:

$$\begin{aligned}
S_{s3} \Leftrightarrow\ & i_x = 0, 1, \ldots, m-1-k+t; i_y = k-t, k-t+1, \ldots, m-1-i_x; \\
& i_{z_1} = k, k+1, \ldots, m-1+t-i_x, \\
S_{s4} \Leftrightarrow\ & i_x = 0, 1, \ldots, m-1; i_y = 0, 1, \ldots, m-1-i_x;
\end{aligned}$$

$$\begin{aligned} &i_{z_1} = 0, 1, \ldots, \min\{k-1, m-1+t-i_x\}, \\ M_{s3} \Leftrightarrow\ & i_x = 0, 1, \ldots, m-k+t; i_y = k-t, k-t+1, \ldots, m-i_x; \\ &i_{z_1} = k, k+1, \ldots, m+t-i_x, \\ M_{s4} \Leftrightarrow\ & i_x = 0, 1, \ldots, m; i_y = 0, 1, \ldots, m-i_x; i_{z_1} = 0, 1, \ldots, \min\{k-1, m+t-i_x\}. \end{aligned}$$

All these shift-polynomials $g_{sMSBs3}(x, y, z_1, z_2), g_{sMSBs4}(x, y, z_1, z_2)$ and $g'_{sMSBs3}(x, y, z_1, z_2), g'_{sMSBs4}(x, y, z_1, z_2)$ modulo R_{s1} have the root $(x, y, z_1, z_2) = (-d_{p_1}, \ell, p, q)$ which are the same as $f_{sMSBs}(x, y, z_1)$ and the definition of z_2. In addition, all these shift-polynomials $g_{sMSBs3}(xX, yY, z_1Z_1, z_2Z_2), g_{sMSBs4}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{sMSBs3}(xX, yY, z_1Z_1, z_2Z_2), g'_{sMSBs4}(xX, yY, z_1Z_1, z_2Z_2)$ are divisible by $X^{m-1}Y^{m-1}Z_1^{m-1}Z_2^k = X^{m-1}Y^{m-1}Z_1^{m-k+t-1}N^k$. We construct a lattice with coefficient vectors of $g_{sMSBs3}(xX, yY, z_1Z_1, z_2Z_2), g_{sMSBs4}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{sMSBs3}(xX, yY, z_1Z_1, z_2Z_2), g'_{sMSBs4}(xX, yY, z_1Z_1, z_2Z_2)$ as the bases. We can obtain two polynomials $h_{s3}(x, y, z_1, z_2)$ and $h_{s4}(x, y, z_1, z_2)$ from LLL outputs. Then, $\tilde{h}_{s3}(x, y, z_1) := z_1^k \cdot h_{s3}(x, y, z_1, z_2)$ and $\tilde{h}_{s4}(x, y, z_1) := z_1^k \cdot h_{s4}(x, y, z_1, z_2)$, which have the root $(x, y, z_1) = (-d_{p_1}, \ell, p)$ modulo $R_{s2} \cdot p^k$, have the root over the integers if the polynomials satisfy Howgrave-Graham's Lemma. In addition, the polynomials $\tilde{h}_{s3}(xX, yY, z_1Z_1)$ and $\tilde{h}_{s4}(xX, yY, z_1Z_1)$ with a common divisor $X^{m-1}Y^{m-1}Z_1^{m-1+t}N^k$ are algebraically independent of $f_{sMSBs}(x, y, z_1)$ if they contradict to Hinek-Stinson's Lemma. Based on the Jochemsz-May extended strategy [JM06], the conditions can be written as

$$\begin{aligned} X^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3+o(m^3)} Y^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3+o(m^3)} Z_1^{\frac{(1+\tau-\eta)^3}{6}m^3+o(m^3)} Z_2^{\left(\frac{\eta^2}{2}-\frac{(\eta-\tau)^2}{6}\right)m^3+o(m^3)} \\ < W_{sMSBs}^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3+o(m^3)} \end{aligned}$$

by computing

$$\begin{aligned} s_X &= \sum_{i=0}^{m}\sum_{j=0}^{m-i}(m-i-j) + \sum_{i=0}^{m}\sum_{j=1}^{t}(m-i) = \left(\frac{1}{6}+\frac{\tau}{2}\right)m^3 + o(m^3), \\ s_Y &= \sum_{i=0}^{m}\sum_{j=0}^{m-i}(i+j) + \sum_{i=0}^{m}\sum_{j=1}^{t} i = \left(\frac{1}{3}+\frac{\tau}{2}\right)m^3 + o(m^3), \\ s_{Z_1} &= \sum_{i=s}^{m}\sum_{j=0}^{m-i}(i-s) + \sum_{i=s-t}^{m}\sum_{j=s-t-i}^{t}(i+j-s) = \frac{(1+\tau-\eta)^3}{6}m^3 + o(m^3), \end{aligned}$$

$$s_{Z_2} = \sum_{i=0}^{s}\sum_{j=0}^{m-i}(s-i) + \sum_{i=0}^{s}\sum_{j=1}^{\min\{t,s-i\}}(s-i-j) = \left(\frac{\eta^2}{2} - \frac{(\eta-\tau)^2}{6}\right)m^3 + o(m^3),$$
$$|S| = \sum_{i_x=0}^{m-1}\sum_{i_y=0}^{m-1-i_x}\sum_{i_{z_1}=0}^{m-1+t-i_x} 1 = \left(\frac{1}{6}+\frac{\tau}{2}\right)m^3 + o(m^3).$$

Ignoring low order terms of m, the condition becomes

$$\delta \cdot \left(\frac{1}{6}+\frac{\tau}{2}\right) + \left(\alpha+\beta-\frac{1}{2}\right)\cdot\left(\frac{1}{3}+\frac{\tau}{2}\right) + \frac{1}{2}\cdot\left(\frac{(1+\tau-\eta)^3}{6} + \frac{\eta^2}{2} - \frac{(\eta-\tau)^2}{6}\right) < (\alpha+\beta)\cdot\left(\frac{1}{6}+\frac{\tau}{2}\right).$$

Let $\tau = 0$ and we can obtain the condition based on the Jochemsz-May basic strategy. To recover a larger root, we optimize the parameter

$$\eta = \frac{1-2\delta}{2} \quad \text{and} \quad \tau = \frac{\sqrt{1-4\delta}-2\delta}{2}$$

and obtain the condition,

$$-5 + 8(\alpha+\beta) + 8\delta - 12\delta^2 - 2(1-4\delta)\sqrt{1-4\delta} < 0.$$

Note that the restriction $\tau \le \eta \le 1$ always holds. The restriction $0 \le \tau$ holds only when $\delta \le 1/\sqrt{2} - 1/2$. However, the condition always holds for $\alpha + \beta > 1/2$, which is the smallest choice of $\alpha + \beta$ for CRT-RSA.

4.4 Double Partial Key Exposure Attacks on CRT-RSA by Solving Integer Equations

For double MSBs/LSBs partial key exposure attacks on CRT-RSA, we obtain the following result.

Theorem 9 (Double MSBs/LSBs). *Let $1/2 < \alpha + \beta \le 3/2$. For double MSBs/LSBs partial key exposure attacks on CRT-RSA, when*

$$\delta < \frac{(18-12(\alpha+\beta))\tau^2 + (20-16(\alpha+\beta))\tau + 5 - 4(\alpha+\beta)}{24\tau^3 + 54\tau^2 + 40\tau + 10} \; \textit{for} \; \frac{15}{16} < \alpha+\beta < \frac{3}{2},$$
$$\delta < \frac{5-4(\alpha+\beta)}{10},$$
$$\delta < \frac{(12-24(\alpha+\beta))\tau^3 + (27-30(\alpha+\beta))\tau^2 + (20-16(\alpha+\beta))\tau + 5 - 4(\alpha+\beta)}{36\tau^2 + 40\tau + 10}$$

for $\frac{1}{2} < \alpha + \beta < \frac{15}{26}$,

hold for some $\tau > 0$*, then public RSA modulus* N *can be factorized in polynomial time.*

Note that the second condition is vaild when $1/2 \leq \alpha + \beta \leq 5/4$ and better than the other conditions when $15/26 \leq \alpha + \beta \leq 15/16$.

4.4.1 Attacks Based on the Jochemsz-May Basic Strategy

As in a previous section, we start from the Jochemsz-May basic strategy. The lattice construction yields the second condition of Theorem 9.

Recall the CRT-RSA key generation,

$$ed_p = 1 + \ell_p(p-1) \qquad \text{and} \qquad ed_q = 1 + \ell_q(q-1)$$

with some integers $\ell_p, \ell_q \approx N^{\alpha+\beta-1/2}$. We multiply following two equations

$$ed_p - 1 - \ell_p = \ell_p p \qquad \text{and} \qquad ed_q - 1 - \ell_q = \ell_q q,$$

and obtain

$$e^2 d_p d_q + ed_p(\ell_q - 1) + ed_q(\ell_p - 1) - (N-1)\ell_p\ell_q - (\ell_p + \ell_q - 1) = 0.$$

For the double MSBs partial key exposure attack on CRT-RSA, let

$$d_p = d_{p_0}M + d_{p_1} \text{ and } d_q = d_{q_0}M + d_{q_1}$$

and obtain

$$\begin{aligned} &e^2(d_{p_0}M + d_{p_1})(d_{q_0}M + d_{q_1}) + e(d_{p_0}M + d_{p_1})(\ell_q - 1) \\ &+ e(d_{q_0}M + d_{q_1})(\ell_p - 1) - (N-1)\ell_p\ell_q - (\ell_p + \ell_q - 1) = 0. \end{aligned}$$

Then we consider the following polynomial over the integers:

$$\begin{aligned} f_{dMSBs}(x_1, x_2, y_1, y_2) =& e^2 x_1 x_2 + (e^2 d_{q_0} M - e)x_1 + (e^2 d_{p_0} M - e)x_2 + ex_1 y_2 + ex_2 y_1 \\ &+ (ed_{q_0}M - 1)y_1 + (ed_{p_0}M - 1)y_2 - (N-1)y_1 y_2 + c_{dMSBs} \end{aligned}$$

whose root is $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ where $c_{dMSBs} = e^2 d_{p_0} d_{q_0} M^2 - ed_{p_0}M - ed_{q_0}M + 1$. Absolute of the root are bounded above by $X_1 := N^\delta, X_2 := N^\delta, Y_1 := N^{\alpha+\beta-1/2}, Y_2 := N^{\alpha+\beta-1/2}$ within constant factors.

We set an integer

$$W_{dMSBs} := N^{2(\alpha+\beta)}$$

since $\|f_{dMSBs}(x_1, x_2, y_1, y_2)\|_\infty \geq |(N-1)y_1y_2| \approx N^{2(\alpha+\beta)}$. Note that $f_{dMSBs}(x_1, x_2, y_1, y_2)$ has the same monomials as the polynomial which Jochemsz and May considered in [JM07]. Therefore, we use the same lattice construction as [JM07]. We set an integer

$$R_{d1} := W_{dMSBs}(X_1X_2Y_1Y_2)^{m-1}$$

with some integer m such that $\gcd(c_{dMSBs}, R_{d1}) = 1$. We compute $a_{dMSBs1} = c_{dMSBs}^{-1} \pmod{R_{d1}}$ and compute

$$f'_{dMSBs1}(x_1, x_2, y_1, y_2) := a_{dMSBs1} \cdot f_{dMSBs}(x_1, x_2, y_1, y_2) \pmod{R_{d1}}.$$

We define a set of shift-polynomials g_{dMSBs1} and g'_{dMSBs1} as

$$\begin{aligned} g_{dMSBs1} :& x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \\ & \cdot f'_{dMSBs1}(x_1, x_2, y_1, y_2) X_1^{m-1-i_{x1}} X_2^{m-1-i_{x2}} Y_1^{m-1-i_{y1}} Y_2^{m-1-i_{y2}} \\ & \text{for } x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \in S_{d1}, \\ g'_{dMSBs1} :& x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \cdot R_{d1} \quad \text{for } x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \in M_{d1} \backslash S_{d1}, \end{aligned}$$

for

$$\begin{aligned} S_{d1} &:= \left\{ x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \,\middle|\, \begin{array}{c} x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \text{ is a monomial of} \\ f'_{dMSBs1}(x_1, x_2, y_1, y_2)^{m-1} \end{array} \right\}, \\ M_{d1} &:= \left\{ \begin{array}{c} \text{monomials of} \\ x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \cdot f'_{dMSBs1}(x_1, x_2, y_1, y_2) \end{array} \,\middle|\, x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \in S_{d1} \right\}. \end{aligned}$$

By definition, the set of indices are the same as:

$$\begin{aligned} S_{d1} \Leftrightarrow & \, i_{x_1} = 0, 1, \ldots, m-1-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-1-i_{y_2}; i_{y_1} = 0, 1, \ldots, m-1; \\ & i_{y_2} = 0, 1, \ldots, m-1, \\ M_{d1} \Leftrightarrow & \, i_{x_1} = 0, 1, \ldots, m-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-i_{y_2}; i_{y_1} = 0, 1, \ldots, m; \\ & i_{y_2} = 0, 1, \ldots, m. \end{aligned}$$

Shift-polynomials g_{dMSBs1} and g'_{dMSBs1} modulo R_{d1} have the root $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ which are the same as $f_{dMSBs}(x_1, x_2, y_1, y_2)$. We construct a lattice with coefficient vectors of $g_{dMSBs1}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ and

$g'_{dMSBs1}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs three short lattice vectors which satisfy Howgrave-Graham's Lemma when

$$(X_1X_2)^{\frac{5}{12}m^4+o(m^4)}(Y_1Y_2)^{\frac{5}{12}m^4+o(m^4)} < W_{dMSBs}^{\frac{1}{4}m^4+o(m^4)}.$$

Ignoring low order terms of m, the condition becomes

$$\delta \cdot 2 \cdot \frac{5}{12} + \left(\alpha + \beta - \frac{1}{2}\right) \cdot 2 \cdot \frac{5}{12} < 2(\alpha+\beta) \cdot \frac{1}{4},$$

that is,

$$\delta < \frac{5 - 4(\alpha+\beta)}{10}.$$

The detailed calculation is discussed later.

4.4.2 Attacks Based on the Jochemsz-May Extended Strategy

Next, we show our lattice construction based on the Jochemsz-May extended strategy. The lattice construction enables us to solve the equation $f_{dMSBs}(x_1, x_2, y_1, y_2) = 0$ for larger $\alpha + \beta$ and yields the condition of Theorem 9.

We set an integer

$$R_{d2} := W_{dMSBs}(X_1X_2)^{m-1+t}(Y_1Y_2)^{m-1}$$

with some integers m and $t = \tau m$ such that $\gcd(c_{dMSBs}, R_{d2}) = 1$. We compute $a_{dMSBs2} = c_{dMSBs}^{-1} \pmod{R_{d2}}$ and

$$f'_{dMSBs2}(x_1, x_2, y_1, y_2) := a_{dMSBs2} \cdot f_{dMSBs}(x_1, x_2, y_1, y_2) \pmod{R_{d2}}$$

as in the basic strategy. We define a set of shift-polynomials g_{dMSBs2} and g'_{dMSBs2} as

$$\begin{aligned} g_{dMSBs2} :& x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \cdot f'_{dMSBs2}(x_1, x_2, y_1, y_2) X_1^{m-1+t-i_{x1}} X_2^{m-1+t-i_{x2}} \cdot \\ & Y_1^{m-1-i_{y1}} Y_2^{m-1-i_{y2}} \text{for } x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \in S_{d2}, \\ g'_{dMSBs2} :& x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \cdot R_{d2} \quad \text{for } x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \in M_{d2} \backslash S_{d2}, \end{aligned}$$

for

$$S_{d2} := \bigcup_{0 \le j_1, j_2 \le t} \left\{ x_1^{i_{x1}+j_1} x_2^{i_{x2}+j_2} y_1^{i_{y1}} y_2^{i_{y2}} \,\middle|\, \begin{array}{c} x_1^{i_{x1}} x_2^{i_{x2}} y_1^{i_{y1}} y_2^{i_{y2}} \text{ is a monomial of} \\ f'_{dMSBs2}(x_1, x_2, y_1, y_2)^{m-1} \end{array} \right\},$$

$$M_{d2} := \left\{ \begin{array}{c} \text{monomials of} \\ x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot f'_{dMSBs2}(x_1, x_2, y_1, y_2) \end{array} \middle| \, x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d2} \right\}.$$

By definition, the set of indices are the same as:

$$\begin{aligned} S_{d2} \Leftrightarrow\ & i_{x_1} = 0, 1, \ldots, m-1+t-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-1+t-i_{y_2}; \\ & i_{y_1} = 0, 1, \ldots, m-1; i_{y_2} = 0, 1, \ldots, m-1, \\ M_{d2} \Leftrightarrow\ & i_{x_1} = 0, 1, \ldots, m+t-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m+t-i_{y_2}; i_{y_1} = 0, 1, \ldots, m; \\ & i_{y_2} = 0, 1, \ldots, m. \end{aligned}$$

Shift-polynomials g_{dMSBs2} and g'_{dMSBs2} modulo R_{d2} have the root $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ which are the same as $f_{dMSBs}(x_1, x_2, y_1, y_2)$. We construct a lattice with coefficient vectors of $g_{dMSBs2}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ and $g'_{dMSBs2}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs three short lattice vectors which satisfy Howgrave-Graham's Lemma when[*1]

$$(X_1X_2)^{(\tau^2+\frac{9}{4}\tau^2+\frac{5}{3}\tau+\frac{5}{12})m^4+o(m^4)}(Y_1Y_2)^{(\frac{3}{2}\tau^2+\frac{5}{3}\tau+\frac{5}{12})m^4+o(m^4)} < W_{dMSBs}^{(\tau^2+\tau+\frac{1}{4})m^4+o(m^4)}.$$

Ignoring low order terms of m, the condition becomes

$$\begin{aligned} \delta \cdot 2 \cdot \left(\tau^2 + \frac{9}{4}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right) + \left(\alpha + \beta - \frac{1}{2}\right) \cdot 2 \cdot \left(\frac{3}{2}\tau^2 + \frac{5}{3}\tau + \frac{5}{12}\right) & \\ < 2(\alpha+\beta) \cdot \left(\tau^2 + \tau + \frac{1}{4}\right), & \end{aligned}$$

that is,

$$\delta < \frac{(18 - 12(\alpha+\beta))\tau^2 + (20 - 16(\alpha+\beta))\tau + 5 - 4(\alpha+\beta)}{24\tau^3 + 54\tau^2 + 40\tau + 10}.$$

The condition becomes the same as the first condition of Theorem 9.

Next, we show how to obtain the third condition of Theorem 9. To solve the equation $f_{dMSBs}(x_1, x_2, y_1, y_2) = 0$, we set an integer

$$R_{d3} := W_{dMSBs}(X_1X_2)^{m-1}(Y_1Y_2)^{m-1+t}$$

with some integer m and $t = \tau m$ such that $\gcd(c_{dMSBs}, R_{d3}) = 1$. We compute $a_{dMSBs3} = c_{dMSBs}^{-1} \pmod{R_{d3}}$ and

$$f'_{dMSBs3}(x_1, x_2, y_1, y_2) := a_{dMSBs3} f_{dMSBs}(x_1, x_2, y_1, y_2) \pmod{R_{d3}}.$$

[*1] In this paper, we omit the calculation since that is the same as [JM07]. See the paper for detailed calculation.

We define a set of shift-polynomials g_{dMSBs3} and g'_{dMSBs3} as

$$\begin{aligned} g_{dMSBs3} :& x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot f'_{dMSBs3}(x_1, x_2, y_1, y_2) X_1^{m-1-i_{x_1}} X_2^{m-1-i_{x_2}} \cdot \\ & Y_1^{m-1+t-i_{y_1}} Y_2^{m-1+t-i_{y_2}} \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d3}, \\ g'_{dMSBs3} :& x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot R_{d3} \quad \text{for } x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in M_{d3} \backslash S_{d3}, \end{aligned}$$

for

$$S_{d3} := \bigcup_{0 \le j_1, j_2 \le t} \left\{ x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}+j_1} y_2^{i_{y_2}+j_2} \middle| \begin{array}{c} x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \text{ is a monomial of} \\ f'_{dMSBs3}(x_1, x_2, y_1, y_2)^{m-1} \end{array} \right\},$$

$$M_{d3} := \left\{ \begin{array}{c} \text{monomials of} \\ x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \cdot f'_{dMSBs3}(x_1, x_2, y_1, y_2) \end{array} \middle| x_1^{i_{x_1}} x_2^{i_{x_2}} y_1^{i_{y_1}} y_2^{i_{y_2}} \in S_{d3} \right\}.$$

By definition, the set of indices is the same as:

$$\begin{aligned} S_{d3} \Leftrightarrow i_{x_1} &= 0, 1, \ldots, m-1-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-1-i_{y_2}; \\ i_{y_1} &= 0, 1, \ldots, m-1+t; i_{y_2} = 0, 1, \ldots, m-1+t, \\ M_{d3} \Leftrightarrow i_{x_1} &= 0, 1, \ldots, m-i_{y_1}; i_{x_2} =; 0, 1, \ldots, m-i_{y_2}; i_{y_1} = 0, 1, \ldots, m+t; \\ i_{y_2} &= 0, 1, \ldots, m+t. \end{aligned}$$

Shift-polynomials g_{dMSBs3} and g'_{dMSBs3} modulo R_{d3} have the root $(x_1, x_2, y_1, y_2) = (d_{p_1}, d_{q_1}, \ell_p, \ell_q)$ which is the same as $f_{dMSBs}(x_1, x_2, y_1, y_2)$. We construct a lattice with coefficient vectors of $g_{dMSBs3}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ and $g'_{dMSBs3}(x_1X_1, x_2X_2, y_1Y_1, y_2Y_2)$ as the bases. Based on the Jochemsz-May strategy [JM06], LLL outputs three short lattice vectors which satisfy Howgrave-Graham's Lemma when[*2]

$$(X_1X_2)^{(\tau^2+\frac{9}{4}\tau^2+\frac{5}{3}\tau+\frac{5}{12})m^4+o(m^4)}(Y_1Y_2)^{(\frac{3}{2}\tau^2+\frac{5}{3}\tau+\frac{5}{12})m^4+o(m^4)} < W_{dMSBs}^{(\tau^2+\tau+\frac{1}{4})m^4+o(m^4)}.$$

The condition becomes the same as the third condition of Theorem 9.

4.5 Single Partial Key Exposure Attacks on CRT-RSA by Solving Modular Equations

In this section, we further improve a single partial key exposure attack on CRT-RSA with the least significant bits and obtain the following result.

[*2] In this paper, we omit the calculation since that is the same as [JM07]. See the paper for detailed calculation.

Table 4.1. The comparison of recoverable δ for each attack.

α	Ours	[TK15]	[LZL14]
0	0.25	0.207106	0.25
0.025	0.192823	0.184571	0.185591
0.05	0.170887	0.16529	0.157196
0.075	0.152602	0.148005	0.132106
0.1	0.135829	0.132125	0.107106
0.125	0.120241	0.11731	0.082106
0.15	0.105616	0.103344	0.057106
0.175	0.091797	0.090077	0.032106
0.2	0.078663	0.0774	0.007106
0.225	0.066120	0.065229	0.003794
0.25	0.054097	0.053501	0
0.275	0.042532	0.0421655	–
0.3	0.031378	0.0311793	–
0.325	0.020593	0.0205082	–
0.35	0.010144	0.0101234	–
0.375	0	0	–

Theorem 10. *Let $N = pq$ be a public RSA modulus where the prime factors p and q are the same bit-size. Let $e \approx N^{\alpha}$ denote a public exponent and $d_p \approx N^{0.5}$ denote a CRT exponent such that $ed_p = 1 \pmod{(p-1)}$. Given the public elements (N, e) as well as $\tilde{d}_p > N^{0.5-\delta}$ which is the least significant bits of a CRT exponent. If*

- $\delta < \frac{5-2\sqrt{1+14\alpha}}{14}$ *for* $\frac{1}{18} < \alpha \leq \frac{3}{8}$, *or*
- $\eta\left(\alpha(1-2(\delta-\alpha)) - \delta\left(1-4(\delta-\alpha)\right)^2\right) + \alpha(\delta-\alpha)(1+2\alpha-4\delta) < 0$ *where* $\eta = \frac{2\delta(1-4(\delta-\alpha))+2\sqrt{\delta(\delta-\alpha)(1+2\alpha-8\delta(1-2\delta+2\alpha))}}{1-2(\delta-\alpha)}$ *for* $0 < \alpha \leq \frac{1}{18}$,

then the public modulus N can be factorized in polynomial time.

For the improvement, we solve the same modular equation as Lu et al. where the analysis was written in Section 4.3.1. We obtain the result by designing better lattices to solve the equation. In Section 4.5.1, we observe corrected Lu et al.'s lattice which we studied in Section 4.3.1.

4.5.1 Observation of the Lu et al. Lattice

Let d'_p and $\tilde{d}_p$ be the most/least significant bits of d_p, respectively. As we defined above, $\tilde{d}_p > N^{0.5-\delta}$ and $d'_p < N^{\delta}$. Then the CRT-exponent can be rewritten as $d_p = d'_p M + \tilde{d}_p$ where $M \approx N^{0.5-\delta}$. To thwart the Jochemsz-May attack [JM07], we only consider the case $d_p \approx N^{0.5}$ in this section and omit the analysis of the other case since the generalization is almost trivial. The key generation can be written as

$$e\left(d'_p M + \tilde{d}_p\right) = 1 + \ell(p-1)$$

with some integer ℓ. Lu et al. [LZL14] formulated the following equation:

$$1 - e\tilde{d}_p - eMx - y = 0 \pmod{p}$$

whose solution is $(x, y) = (d'_p, \ell)$. There are two algorithms known to solve the equation due to Herrmann and May [HM08], and Takayasu and Kunihiro [TK14d]. Herrmann and May's algorithm is based on the Jochemsz-May strategy whereas Takayasu and Kunihiro's algorithm is not. The latter algorithm works for larger δ than the former algorithm for small α; when $\alpha \approx 0$, the latter algorithm works for $\delta < 1/4$ and the former algorithm works for $\delta < (\sqrt{2}-1)/2 = 0.20710\cdots$. The fact shows that when we can construct a better attack which cannot be obtained by the Jochemsz-May strategy, it works with less partial information for the same α.

Lu et al., Takayasu and Kunihiro formulated the following equation

$$1 - e\tilde{d}_p + x(y-1) = 0 \pmod{eM}$$

whose solution is $(x, y) = (\ell, p)$. They solved the equation where the lattice construction is based on the Jochemsz-May strategy as the Herrmann-May. However, the formulation affects the resulting attack condition. The latter attack works for large α than the former attack; when $\delta \approx 0$, the latter algorithm works for $\alpha < 3/8$ and the former attack works for $\alpha < (\sqrt{2}-1)/2 = 0.20710\cdots$. The fact shows that the latter formulation, i.e., mod eM equation, yields the attacks which work for larger α than the former equation, i.e., mod p equation.

Our improved attack in this section is constructed by solving the mod eM equation and the lattice does not follow the Jochemsz-May strategy. The improvement is reasonable from the above discussion. Although we solve the same mod eM equation, Lu et al.'s attack is based on the Jochemsz-May strategy. Hence, our attack works for larger δ than the previous attack. Although Lu et al.'s modulo p attack with the Takayasu-Kunihiro attack is not based on the Jochemsz-May strategy, our attack works for larger α than the previous attack. Therefore, our attack is better than the previous best attacks for all α.

Lu et al. constructed a lattice whose basis consists of polynomials which have the same root as the original polynomial modulo $(eM)^m$. We want to analyze the validity of the lattice construction by considering the helpful polynomials strategy [May10, TK14d]. Based on the strategy, as many helpful polynomials (which have diagonals whose sizes are smaller than $(eM)^m$) as possible should be selected and as few unhelpful polynomials (which have diagonals whose sizes are larger than $(eM)^m$) as possible should be eliminated as long as a basis matrix to be triangular.

Then we observe the corrected Lu et al. lattice after the parameter optimization. There are polynomials with diagonals

- $X^{i+j}Y^{i-s}(eM)^{m-i}$ for $i = s, s+1, \ldots, m; j = 0, 1, \ldots, m-i$,
- $X^{i+j}Z^{s-i}(eM)^{m-i}$ for $i = 0, 1, \ldots, s-1; j = 0, 1, \ldots, m-i$,
- $X^{i}Y^{i+j-s}(eM)^{m-i}$ for $i = s-t, s-t+1, \ldots, m; j = s-t-i, s-t-i+1, \ldots, t$,
- $X^{i}Z^{s-i-j}(eM)^{m-i}$ for $i = 0, 1, \ldots, s-1; j = 1, 2, \ldots, \min\{t, s-i\}$.

We focus on the bottom two families of polynomials, i.e., $g'_{[i,j]}(x, y, z)$. The lattice basis does not contain as many helpful polynomials as possible since when polynomials

$$g'_{[i,j]}(x, y, z) \quad \text{for } i = 1, 2, \ldots, s-1; j = s-i$$

are added in the basis, the corresponding diagonals become

- $X^{i}(eM)^{m-i}$ for $i = 1, 2, \ldots, s-1$

and

$$X^{i}(eM)^{m-i} = N^{\left(\alpha+\frac{1}{2}-\delta\right)m-\left(\frac{1}{2}-\delta\right)i} < N^{\left(\alpha+\frac{1}{2}-\delta\right)m} = (eM)^m.$$

Similarly, the lattice basis contains some unhelpful polynomials which do not contribute for the basis matrix to be triangular since the basis matrix is still triangular without polynomials

$$g'_{[i,j]}(x, y, z) \quad \text{for } i = \left\lceil \frac{1-\sqrt{1-4\delta}}{4\delta} m \right\rceil, \left\lceil \frac{1-\sqrt{1-4\delta}}{4\delta} m \right\rceil + 1 \ldots, m; j = t$$

whose corresponding diagonals are

- $X^iY^{i+t-s}(eM)^{m-i}$ for $i = \lceil \frac{1-\sqrt{1-4\delta}}{4\delta}m \rceil, \lceil \frac{1-\sqrt{1-4\delta}}{4\delta}m \rceil + 1, \ldots, m$

and the following inequality holds:

$$X^iY^{i+t-s}(eM)^{m-i} = N^{\left(\alpha+\frac{1}{2}-\delta\right)m+\delta i-\frac{1}{2}(s-t)} > N^{\left(\alpha+\frac{1}{2}-\delta\right)m} = (eM)^m.$$

Notice that

$$\delta i - \frac{1}{2}(s-t) = \delta i - \frac{1}{2}\left(\frac{1-2\delta}{2} - \frac{\sqrt{1-4\delta}-2\delta}{2}\right)m = \delta\left(i - \frac{1-\sqrt{1-4\delta}}{4\delta}m\right) > 0$$

for all $i = \left\lceil \frac{1-\sqrt{1-4\delta}}{4\delta}m \right\rceil, \left\lceil \frac{1-\sqrt{1-4\delta}}{4\delta}m \right\rceil + 1, \ldots, m.$

The above examples are not all the helpful polynomials which are not selected and all the unhelpful polynomials which are selected. Hence, if we can construct more appropriate lattices, the resulting attack condition can be improved.

4.5.2 Improved Lattice Construction for $1/18 < \alpha \leq 3/8$

Based on the above observation, we construct more appropriate lattices than Lu et al. More concretely, we select all helpful $g'_{[i,j]}(x,y,z)$ for $i+j \geq s$ and do not select any unhelpful $g'_{[i,j]}(x,y,z)$ for $i+j \geq s$.

At first, we analyze which $g'_{[i,j]}(x,y,z)$ for $i+j \geq s$ are helpful or not. As we explained, the corresponding diagonals are $X^iY^{i+j-s}(eM)^{m-i}$. Then the polynomials are helpful when

$$\begin{aligned} X^iY^{i+j-s}(eM)^{m-i} < (eM)^m &\Leftrightarrow \alpha i + \frac{1}{2}(i+j-s) < \left(\alpha + \frac{1}{2} - \delta\right)i \\ &\Leftrightarrow j < s - 2\delta i. \end{aligned}$$

Therefore, we collect the following shift-polynomials:

$$\begin{aligned} &g_{[i,j]}(x,y,z) \quad \text{for } i = 0,1,\ldots,m; j = 0,1,\ldots,m-i \text{ and} \\ &g'_{[i,j]}(x,y,z) \quad \text{for } i = 0,1,\ldots,m; j = 1,2,\ldots,\lfloor s-2\delta i \rfloor \end{aligned}$$

in a lattice basis. Here, we do not take into account if polynomials $g_{[i,j]}(x,y,z)$ and $g'_{[i,j]}(x,y,z)$ for $i+j < s$ are helpful or not, however, these polynomials contribute the basis matrix to be triangular. Hence, we use the above collection of shift-polynomials only when $\eta > 2\delta$. Otherwise, polynomials $g_{[i,j]}(x,y,z)$ for $i+j > \frac{\eta}{2\delta}m$ do not contribute the basis matrix to be triangular. We will analyze the other case in the next section.

We compute the resulting attack condition. A dimension n and a determinant of the lattice $\det(L(\boldsymbol{B})) = X^{s_X} Y^{s_Y} Z^{s_Z} (eM)^{s_{eM}}$ are computed by

$$n = \sum_{i=0}^{m} \sum_{j=0}^{m-i} 1 + \sum_{i=0}^{m} \sum_{j=1}^{\lfloor s-2\delta i \rfloor} 1 = \left(\frac{1}{2} - \delta + \eta \right) m^2 + o(m^2),$$

$$s_X = \sum_{i=0}^{m} \sum_{j=0}^{m-i} (i+j) + \sum_{i=0}^{m} \sum_{j=1}^{\lfloor s-2\delta i \rfloor} i = \left(\frac{1-2\delta}{3} + \frac{\eta}{2} \right) m^3 + o(m^3),$$

$$s_Y = \sum_{i=s}^{m} \sum_{j=0}^{m-i} (i-s) + \sum_{i=0}^{m} \sum_{j=\max\{s-i+1,0\}}^{\lfloor s-2\delta i \rfloor} (i+j-s) = \frac{(1-2\delta)^2}{6} m^3 + o(m^3),$$

$$s_Z = \sum_{i=0}^{s-1} \sum_{j=0}^{m-i} (s-i) + \sum_{i=0}^{s-1} \sum_{j=0}^{s-i} (s-i-j) = \frac{\eta^2}{2} m^3 + o(m^3),$$

$$s_{eM} = \sum_{i=0}^{m} \sum_{j=0}^{m-i} (m-i) + \sum_{i=0}^{m} \sum_{j=1}^{\lfloor s-2\delta i \rfloor} (m-i) = \left(\frac{1-\delta}{3} + \frac{\eta}{2} \right) m^3 + o(m^3).$$

LLL outputs short lattice vectors and the corresponding polynomials satisfies Howgrave-Graham's Lemma when $X^{s_X} Y^{s_Y} Z^{s_Z} (eM)^{s_{eM}} < (eM)^{mn}$. Ignoring low order terms of m, the condition becomes

$$\alpha \left(\frac{1-2\delta}{3} + \frac{\eta}{2} \right) + \frac{1}{2} \left(\frac{(1-2\delta)^2}{6} + \frac{\eta^2}{2} \right) < \left(\alpha + \frac{1}{2} - \delta \right) \left(\frac{1}{6} - \frac{2\delta}{3} + \frac{\eta}{2} \right).$$

To maximize the right hand side of the inequality, we set the parameter η to be a solution of

$$\alpha \frac{1}{2} + \frac{1}{2} \eta = \left(\alpha + \frac{1}{2} - \delta \right) \frac{1}{2},$$

that is,

$$\eta = \frac{1-2\delta}{2}.$$

By substituting the parameter, the above attack condition becomes

$$7(1-2\delta)^2 - 4(1-2\delta) - 8(\alpha + 1/2) + 4 > 0.$$

Therefore, the attack works when

$$\delta < \frac{5 - 2\sqrt{1+14\alpha}}{14}$$

as required.

Notice that the attack works only when $\frac{1-2\delta}{2} > 2\delta$, that leads to $\delta < \frac{1}{6}$ and equivalent to

$$\alpha > \frac{1}{18}.$$

4.5.3 Improved Lattice Construction for $0 < \alpha \leq 1/18$

In this section, we propose an improved attack for $0 < \alpha \leq 1/18$, i.e., the second condition of Theorem 10. We defined the collection of shift-polynomials in Section 4.2 by analyzing if polynomials $g'_{[i,j]}(x,y,z)$ for $i+j \geq s$ are helpful or not. As we explained, we use the lattice only when $\eta > 2\delta$. Otherwise, polynomials $g_{[i,j]}(x,y,z)$ for $i+j > \frac{s}{2\delta}$ do not contribute the basis matrix to be triangular.

To improve the attack for $0 < \alpha \leq 1/18$, we analyze which polynomials $g_{[i,j]}(x,y,z)$ for $i+j > \frac{s}{2\delta}$ and $i \geq s$ are helpful or not. As we explained, the corresponding diagonals are $X^{i+j}Y^{i-s}(eM)^{m-i}$. Then the polynomials are helpful when

$$\begin{aligned}X^{i+j}Y^{i-s}(eM)^{m-i} < (eM)^m &\Leftrightarrow \alpha(i+j) + \frac{1}{2}(i-s) < \left(\alpha + \frac{1}{2} - \delta\right) i\\ &\Leftrightarrow j < \frac{s-2\delta i}{2\alpha}.\end{aligned}$$

Therefore, we collect the following shift-polynomials:

$$\begin{aligned}&g_{[i,j]}(x,y,z) \quad \text{for } i = 0,1,\ldots,\lfloor\frac{s}{2\delta}\rfloor; j = 0,1,\ldots,\min\left\{m-i, \lfloor\frac{s-2\delta i}{2\alpha}\rfloor\right\} \text{ and}\\ &g'_{[i,j]}(x,y,z) \quad \text{for } i = 0,1,\ldots,\lfloor\frac{s}{2\delta}\rfloor; j = 1,2,\ldots,\lfloor s-2\delta i\rfloor\end{aligned}$$

in a lattice basis. Here, we do not take into account if polynomials $g_{[i,j]}(x,y,z)$ for $i+j > \frac{s}{2\delta}$ and $i \leq s$ are helpful or not, however, these polynomials contribute the basis matrix to be triangular.

We compute the resulting attack condition. A dimension n and a determinant of the lattice $\det(L(\boldsymbol{B})) = X^{s_X}Y^{s_Y}Z^{s_Z}(eM)^{s_{eM}}$ are computed by

$$\begin{aligned}n &= \sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor} \sum_{j=0}^{\min\left\{m-i,\lfloor\frac{s-2\delta i}{2\alpha}\rfloor\right\}} 1 + \sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor} \sum_{j=1}^{\lfloor s-2\delta i\rfloor} 1\\ &= \left(\frac{\alpha}{2(\delta-\alpha)}\left(1-\frac{\eta}{2\delta}\right)\left(\frac{2\delta-\alpha}{\alpha}\cdot\frac{\eta}{2\delta}-1\right) + \frac{1+2\delta}{2}\left(\frac{\eta}{2\delta}\right)^2\right)m^2 + o(m^2),\\ s_X &= \sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor} \sum_{j=0}^{\min\left\{m-i,\lfloor\frac{s-2\delta i}{2\alpha}\rfloor\right\}} (i+j) + \sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor} \sum_{j=1}^{\lfloor s-2\delta i\rfloor} i\end{aligned}$$

$$
\begin{aligned}
=&\frac{\alpha}{\delta-\alpha}\left(1-\frac{\eta}{2\delta}\right)\left(-\frac{1}{3}+\left(\frac{\delta}{2\alpha}-\frac{1}{3}\right)\frac{\eta}{2\delta}+\left(\frac{\delta}{2\alpha}-\frac{1}{3}\right)\left(\frac{\eta}{2\delta}\right)^2\right)m^3\\
&+\frac{1+\delta}{3}\left(\frac{\eta}{2\delta}\right)^3 m^3+o(m^3),\\
s_Y =&\sum_{i=s}^{\lfloor\frac{s}{2\delta}\rfloor}\sum_{j=0}^{\min\left\{m-i,\lfloor\frac{s-2\delta i}{2\alpha}\rfloor\right\}}(i-s)+\sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor}\sum_{j=\max\{s-i+1,0\}}^{\lfloor s-2\delta i\rfloor}(i+j-s)\\
=&\frac{\alpha^2}{2(\delta-\alpha)^2}\left(1-\frac{\eta}{2\delta}\right)\left(\frac{1}{3}+\left(\frac{1}{3}-\frac{\delta(1+2\alpha-2\delta)}{\alpha}\right)\frac{\eta}{2\delta}\right)m^3\\
&+\frac{\alpha^2}{2(\delta-\alpha)^2}\left(1-\frac{\eta}{2\delta}\right)\left(\frac{\eta}{2\delta}\right)^2\left(\frac{1}{3}-\frac{\delta(1+2\alpha-2\delta)}{\alpha}+\frac{\delta^2(1+2\alpha-2\delta)^2}{\alpha^2}\right)m^3\\
&+\frac{(1-2\delta)^2}{6}\left(\frac{\eta}{2\delta}\right)^3 m^3+o(m^3),\\
s_Z =&\sum_{i=0}^{s-1}\sum_{j=0}^{m-i}(s-i)+\sum_{i=0}^{s-1}\sum_{j=1}^{s-i}(s-i-j)=\frac{\eta^2}{2}m^3+o(m^3),\\
s_{eM} =&\sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor}\sum_{j=0}^{\min\left\{m-i,\lfloor\frac{s-2\delta i}{2\alpha}\rfloor\right\}}(m-i)+\sum_{i=0}^{\lfloor\frac{s}{2\delta}\rfloor}\sum_{j=1}^{\lfloor s-2\delta i\rfloor}(m-i)\\
=&nm-\left(\frac{1+\delta}{3}-\left(\frac{1}{6}\right)\left(\frac{\eta}{2\delta}\right)^3+\frac{\alpha^2}{6(\delta-\alpha)^2}\left(1-\frac{\eta}{2\delta}\right)\right)m^3\\
&+\frac{\alpha^2}{6(\delta-\alpha)^2}\cdot\frac{\eta}{2\delta}\left(1-\frac{\eta}{2\delta}\right)\left(\frac{3\delta-\alpha}{\alpha}-\frac{\alpha^2-3\alpha\delta+3\delta^2}{\alpha^2}\cdot\frac{\eta}{2\delta}\right)m^3+o(m^3).
\end{aligned}
$$

LLL outputs short lattice vectors and the corresponding polynomials satisfies Howgrave-Graham's Lemma when $X^{s_X}Y^{s_Y}Z^{s_Z}(eM)^{s_{eM}} < (eM)^{mn}$. Ignoring low order terms of m, the condition becomes

$$
\delta^2(1-2(\delta-\alpha))\left(\frac{\eta}{2\delta}\right)^3-3\delta^2\left(1-4(\delta-\alpha)\right)\left(\frac{\eta}{2\delta}\right)^2+3\delta\alpha\cdot\frac{\eta}{2\delta}-\alpha^2<0.
$$

To minimize the left hand side of the inequality, we set the parameter η to be a solution of

$$
\delta(1-2(\delta-\alpha))\left(\frac{\eta}{2\delta}\right)^2-2\delta\left(1-4(\delta-\alpha)\right)\cdot\frac{\eta}{2\delta}+\alpha=0,
$$

that is,

$$
\eta=\frac{2\delta\left(1-4(\delta-\alpha)\right)+2\sqrt{\delta(\delta-\alpha)(1+2\alpha-8\delta(1-2\delta+2\alpha))}}{1-2(\delta-\alpha)}.
$$

By substituting the parameter, the above attack condition becomes

$$
\eta\left(\alpha(1-2(\delta-\alpha))-\delta\left(1-4(\delta-\alpha)\right)^2\right)+\alpha(\delta-\alpha)(1+2\alpha-4\delta)<0.
$$

It is equivalent to the second condition of Theorem 10.

4.6 Concluding Remarks

In this chapter, we proposed improved partial key exposure attacks on CRT-RSA when attackers obtain the MSBs/LSBs of d_p or/and d_q. At first, we used Coppersmith's integer equations solving method for the improvement. The approach enables us to obtain the improved attack with the MSBs of d_p or d_q for larger $e < N^{3/8}$ and the improved attack with the MSBs/LSBs of d_p and d_q. Next, we constructed better lattices to solve modular equations and obtained the improvement for the attack with the LSBs of d_p or d_q. The attack works with less partial information for all $e < N^{3/8}$ than previous attacks.

An open problem is whether we can further improved an attack with the MSBs of d_p or d_q. Compared with the analogous attack with the LSBs, the condition is quite unnatural. In particular, the best attack for the smaller e proposed by Blömer-May and that for the larger e by ours work under completely different conditions. Hence, the best attack condition is covered by somewhat unnatural curve. As the attack with the LSBs, we should find attacks that improve the existing ones for all $e < N^{3/8}$.

Chapter 5

Partial Key Exposure Attacks on RSA for General Exposure Scenarios

5.1 Introduction

5.1.1 Background

Let $N = pq$ be a public RSA modulus where p and q are distinct prime factors with the same bit-size. A public/secret exponent e and d such that $ed = 1 \pmod{\Phi(N)}$ where $\Phi(N)$ is Euler's totient function. There is a variant of RSA called Multi-Prime RSA that have a public modulus $N = \prod_{i=1}^{r} p_i$ where p_i's are all distinct primes with the same bit-size. A public/secret exponent of Multi-Prime RSA satisfies the same equation as the standard RSA. Multi-Prime RSA offers faster decryption/signing by combining with Chinese Remainder Theorem.

From the invention of RSA cryptosystems, hardness of the factorization/RSA problem have been intensively studied. One well known approach in the literature is lattice based Coppersmith's methods [Cop96a, Cop96b]. The method showed an RSA modulus $N = pq$ can be factorized in polynomial time with half the most significant bits of a prime factor. Although Coppersmith's methods requires involved technical analyses, the method has revealed the vulnerability of RSA in many papers. One of the most famous result is Boneh and Durfee's small secret exponent attack on RSA [BD00] that factorizes an RSA modulus N in polynomial time when $d < N^{1-1/\sqrt{2}} = N^{0.292\cdots}$. Ciet et al. [CKLQ02] extended the attack for Multi-Prime RSA and their attack works when $d < N^{1-\sqrt{1-1/r}}$.

Boneh, Durfee, and Frankel [BDF98] proposed several attacks on RSA called *partial* *key exposure attacks* that make use of the most/least significant bits (MSBs/LSBs) of d. Afterwards, the research becomes a hot topic and numerous papers have been published. Although the original attacks [BDF98] work only for a small e, several improvements [BM03, EJMdW05, SSM10, TK14d] have been proposed using Coppersmith's methods [Cop96a, Cop96b]. In particular, Ernst et al. [EJMdW05] revealed that RSA becomes vulnerable even for a full size e and Takayasu-Kunihiro's attacks [TK14d] contain Boneh-Durfee's small secret exponent attack [BD00] as a special case. Besides these results, numerous papers have studied partial key exposure attacks for various attack scenarios; attacks on Multi-Prime RSA with the MSBs/LSBs of d [Hin08], attacks on RSA with the MSBs of a prime factor [SMS08], attacks on RSA with the MSBs/LSBs of d and the MSBs of a prime factor [SM08], attacks on RSA where the prime factors share the same LSBs [SWS$^+$08], attacks on RSA where the prime factors are almost the same sizes [dW02], attacks on Multi-Prime RSA where all the prime factors are almost the same sizes [TK14c, ZT13, ZT14], and more.

Indeed, there are many papers that study partial key exposure attacks on RSA. However, the situation does not immediately mean that the problem is worth studying in such many papers. Among the above variants of the attack, some papers capture almost the same attack scenarios. Hence, essentially the same algorithms have been proposed in several papers. We do not think the situation is not desirable for the development of the cryptographic research.

5.1.2 Our Contributions

To resolve the situation, we define a general partial key exposure scenario. For the purpose, we classify some existing works with respect to three properties; attackers know partial information of a *secret exponent* and *prime factors* for *Multi-Prime RSA*. Since there are no results that capture the three properties simultaneously, we define a general attack scenario as follows.

Definition 3 (($\alpha, \beta, \gamma, \delta$)-Partial Key Exposure Attacks on RSA)**.** *Let $N = \prod_{i=1}^{r} p_i$ where all $p_1, \ldots, p_r$ are distinct primes of the same bit-size. Let $e = N^\alpha$ and $d = N^\beta$ such that $ed = 1 \pmod{\Phi(N)}$. Given $(N, e, \tilde{d}, \tilde{\Phi}(N))$ where $\tilde{d} \geq N^{\beta-\gamma}$ is the MSBs/LSBs of d and $|\Phi(N) - \tilde{\Phi}(N)| \leq N^\delta$, the goal of the problem is to compute $\Phi(N)$.*

We parametrize the problem with respect to $(\alpha, \beta, \gamma, \delta)$. Notice that the number of prime factors r is independent of the hardness of the problem. Although partial information of prime factors in previous works are defined in various ways, the above definition captures several exposure scenarios simultaneously. For example, let us focus on an attack on RSA with the most significant bits prime factors and an attack on Multi-Prime RSA. Given $\tilde{p}$ which is the $\delta' \log N$ MSBs of an RSA prime factor p, then we regard $\tilde{\Phi}(N) = N - \tilde{p}N^{1/2-\delta'} - \lfloor N/\tilde{p}N^{1/2-\delta'} \rfloor$ and an attack on RSA with the most significant bits of prime factors is captured by $\delta = 1/2 - \delta'$ since $|\Phi(N) - \tilde{\Phi}(N)|$ is bounded above by $N^{1/2-\delta'}$ within a constant factor [SM08, SMS08]. Similarly, we regard $\tilde{\Phi}(N) = N$ and an attack on Multi-Prime RSA is captured by $\delta = 1 - 1/r$ since $|\Phi(N) - N|$ is bounded above by $N^{1-1/r}$ within a constant factor [Hin08]. Since we analyze all $0 \leq \gamma \leq \beta$ and $0 \leq \delta \leq 1$, our definition covers several existing works simultaneously. Moreover, the definition will cover other unknown variants that will be studied in the future. Then our results can be viewed as a *tool kit* to study partial key exposure attacks as [BM05]. It means that our results enable even beginners of Coppersmith's methods to examine the security of such future variants without understanding the technical detail of this paper.

We use lattice based Coppersmith's methods to solve integer/modular equations as previous works and obtain the following results.

Theorem 11. *Given the MSBs/LSBs of d, there are polynomial time algorithms to solve $(\alpha, \beta, \gamma, \delta)$-Partial Key Exposure Attacks on RSA when*

- $\gamma < \frac{3-\delta-2\sqrt{\delta^2+3(\alpha+\beta-1)\delta}}{3}$.

Theorem 12. *Given the MSBs of d, there are polynomial time algorithms to solve $(1, \beta, \gamma, \delta)$-Partial Key Exposure Attacks on RSA when*

1. $\gamma < 1 - \frac{2}{3}\left(\delta + \sqrt{\delta(4\delta - 3 + 6\beta)}\right)$ *for* $\beta < 1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}}$,
2. $\gamma < \frac{1+\beta-\sqrt{4\delta-3(1-\beta)^2}}{2}$ *for* $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1 - \delta$ *and* $1/3 \leq \delta$, *and for* $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1 - \sqrt{\frac{\delta}{3}}$ *and* $\delta < 1/3$,
3. $3\lambda\tau - 3(1-\delta)\tau^2 + \tau^3 < \frac{(\delta\tau-\beta+\lambda)^3}{\delta(1+\lambda-2\beta)}$ *where* $\lambda = \max\{\gamma, \beta+\delta-1\}$ *and* $\tau = 1 - \frac{\beta+\delta-1}{\delta-\sqrt{1+\lambda-2\beta}}$ *for* $1 - \delta \leq \beta < \frac{3(1-\delta)(1+\delta)}{4}$ *and* $1/3 \leq \delta < 2/3$, *and for* $1 - \delta \leq \beta < \delta - \frac{(2\delta-1)^2}{\delta^2}$ *and* $2/3 \leq \delta$,
4. $\gamma \leq \frac{3(1-\delta)^2}{4}$ *for* $\frac{3(1-\delta)(1+\delta)}{4} \leq \beta < \frac{3(1-\delta)^2+4(1-\delta)}{4}$ *and* $1/3 \leq \delta < 2/3$,
5. $\gamma < \frac{2+\beta-2\delta-2\sqrt{(\beta+\delta-1)(\beta+4\delta-1)}}{3}$ *for* $\frac{3(1-\delta)^2+4(1-\delta)}{4} \leq \beta$ *and* $1/3 \leq \delta$,
6. $\gamma \leq 1 - \frac{2\sqrt{3\delta}}{3}$ *for* $1 - \sqrt{\frac{\delta}{3}} \leq \beta$ *and* $\delta < 1/3$.

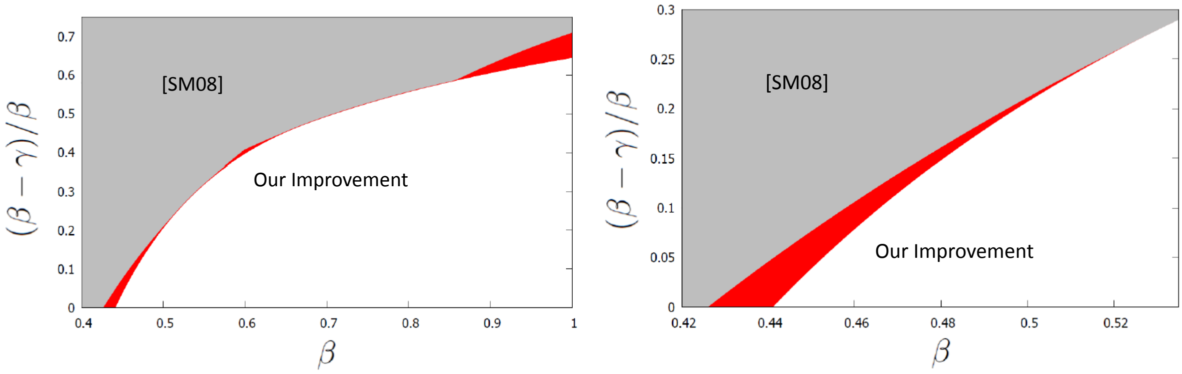


Fig. 5.1. Comparisons of partial key exposure attacks on RSA with the $\approx \frac{3}{16}\log N$ MSBs of p, i.e., $(1,\beta,\gamma,5/16)$-partial key exposure attacks. We compare how much portions of d should be exposed for β between Sarkar and Maitra's attack (gray areas) [SM08] and our Theorem 12 and 3 (red areas). The left (resp. right) figure represents the attack with the MSBs (resp. LSBs).

Theorem 13. *Given the LSBs of d, there are polynomial time algorithms to solve $(1,\beta,\gamma,\delta)$-Partial Key Exposure Attacks on RSA when*

1. $\gamma < 1 - \frac{2}{3}\left(\delta + \sqrt{\delta(4\delta - 3 + 6\beta)}\right)$ *for* $\beta < 1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}}$,
2. $\gamma < \frac{1+\beta-\sqrt{4\delta-3(1-\beta)^2}}{2}$ *for* $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \le \beta < 1 - \frac{\delta}{2} - \frac{\sqrt{3\delta(4-\delta)}}{6}$,
3. $\gamma < 1 - \frac{\delta+2\sqrt{\delta(\delta+3\beta)}}{3}$ *for* $1 - \frac{\delta}{2} - \frac{\sqrt{3\delta(4-\delta)}}{6} \le \beta$.

First of all, our results cover all the known best attacks as special cases, e.g., Theorem 11, the conditions 4–6 of Theorem 12, and the condition 3 of Theorem 13 for $\delta = 1/2$ are the same as Ernst et al.'s attack [EJMdW05]. Extensions of previous works are not trivial at all. In the context of the algorithm construction of Coppersmith's methods, to tackle the equations with the more monomials requires the more involved analyses. Hence, to extend some attacks with more partial information and the extended attacks completely cover the original ones as special cases is challenging in some cases. For example, Ernst et al.'s $(1,\beta,\gamma,1/2)$-partial key exposure attack [EJMdW05] for $\gamma = \beta$ do not cover Boneh and Durfee's $(1,\beta,\beta,1/2)$-partial key exposure attack [BD00]. It takes about ten years until the desired attacks [TK14d] were proposed. Indeed, in this paper, we have to analyze eight attacks to obtain the best results for all the cases.

Furthermore, our results offer improved attacks in some special cases. More con-

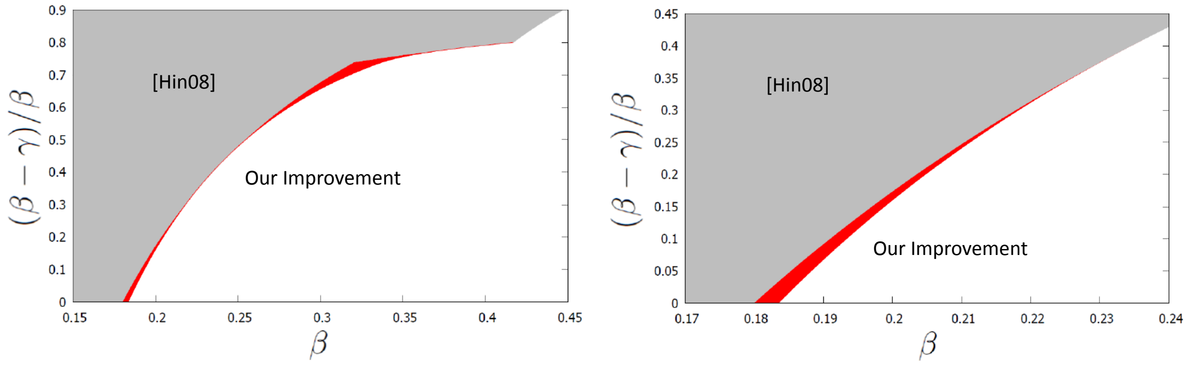


Fig. 5.2. Comparisons of partial key exposure attacks on Multi-Prime RSA for the number of prime factors $r = 3$, i.e., $(1, \beta, \gamma, 2/3)$-partial key exposure attacks. We compare how much portions of d should be exposed for β between Hinek's attack (gray areas) [Hin08] and our Theorem 12 and 3 (red areas). The left (resp. right) figure represents the attack with the MSBs (resp. LSBs).

cretely, we improve Sarkar and Maitra's partial key exposure attacks on RSA with partial information of prime factors [SM08] for small d and Hinek's partial key exposure attacks on Multi-Prime RSA [Hin08]. See Figures 1 and 2 for detailed comparisons. Indeed, our attacks require smaller portions of partial information of d than their attacks.

5.1.3 Technical Overview

To provide better attacks based on Coppersmith's methods is equivalent to provide better lattice constructions to solve the underlying equations. There is a well-known strategy for the construction due to Jochemsz and May [JM06]. The construction may be simple and easy to understand even for beginners of the research area. Ernst et al. [EJMdW05] made use of the strategy for their attacks. Sarkar-Maitra [SM08], Hinek [Hin08], and some other papers extended the attack of Ernst et al. Then, we also follow the strategy and propose extended attacks in Section 5.2; Theorem 11, the conditions 4–6 of Theorem 12, and the condition 3 of Theorem 13. The results based on the strategy are almost naive extensions of the previous attacks although there are some improved analyses in our results; the condition 6 of Theorem 12 in Section 5.2.3 improves Sarkar-Maitra's attack.

Notice that the Jochemsz-May strategy does not always offer the best attacks and lattice constructions that outperform the strategy require involved analyses. For example, Boneh and Durfee's small secret exponent attack [BD00]; $(1, \beta, \beta, 1/2)$-partial key exposure attack, does not seem to be captured by the strategy. To construct better attacks, we make use of Takayasu and Kunihiro's attacks [TK14c, TK14d] where the attack in [TK14c] and [TK14d] solved $(1, \beta, \beta, \delta)$-partial key exposure attacks for $0 \leq \delta \leq 1$ and $(1, \beta, \gamma, 1/2)$-partial key exposure attacks for $0 \leq \gamma \leq \beta$, respectively. Technically, the former and the latter attack constructs a better lattice with respect to the value of δ and γ, respectively. Moreover, they are the only existing partial key exposure attacks that outperform the Jochemsz-May strategy [JM06] except the Boneh-Durfee attack and its straightforward extension. As we suggested above, these lattice constructions [TK14c, TK14d] seem to be technically hard to follow. Indeed, there are only a few papers [TK16a, TK16c] that make use of these results to obtain better results. In this paper, we fully exploit the spirit of the lattice constructions [TK14c, TK14d] and propose $(1, \beta, \gamma, \delta)$-partial key exposure attacks for arbitrary $0 \leq \gamma \leq \beta$ and $0 \leq \delta \leq 1$. Our attacks cover Takayasu and Kunihiro's attacks [TK14c, TK14d] for a fixed $\gamma = \beta$ and $\delta = 1/2$, respectively. We study the attacks with the MSBs and LSBs of d in Section 5.3 and 5.4, respectively.

5.2 Attacks by Solving Integer Equations

In this section, we solve integer equations and propose three attacks, i.e., Attacks 1–3. The Attack 1, 2, and 3 in Section 5.2.1, 5.2.2, and 5.2.3 corresponds to Theorem 11 and the condition 3 of Theorem 13, the conditions 4 and 5 of Theorem 12, and the condition 6 of Theorem 12, respectively. Algorithm constructions in this section are similar to Ernst et al. [EJMdW05].

5.2.1 The Attack 1

In this section, we consider $(\alpha, \beta, \gamma, \delta)$-partial key exposure attacks with the MSBs/LSBs of d. When $\tilde{d}$ which is the MSBs/LSBs of d is given, RSA key generation can be written as $e(\tilde{d}\tilde{M} + d'M') = 1 + k\Phi(N)$ with some integer k such that $|k| \leq N^{\alpha+\beta-1}$. When $\tilde{d}$ is the MSBs (resp. LSBs), d' denotes the LSBs (resp. MSBs) of d, and $\tilde{M} = 2^{\lfloor \gamma \log N \rfloor}$ and $M' = 1$ (resp. $\tilde{M} = 1$ and $M' = 2^{\lfloor (\beta-\gamma) \log N \rfloor}$). Then, we find the root of the following polynomial over the integers:

$$f_{i1}(x, y, z) = c + eM'x + y(\tilde{\Phi} + z),$$

where $c = 1 - e\tilde{d}\tilde{M}$. If we can recover the root $(x, y, z) = (-d', k, \Phi(N) - \tilde{\Phi}(N))$, whole secret information can be computed. By definition, the absolute values of the root are bounded above by $X := N^{\gamma}, Y := N^{\alpha+\beta-1}, Z := N^{\delta}$. By solving the integer equation based on the Jochemsz-May strategy [JM06], Theorem 11 and the condition 3 of Theorem 13 can be obtained.

We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{i1}(xX, yY, zZ)\|_{\infty} \geq \max\{|c|, |eM'X|\} \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1} \cdot Z^{m+r-1+t}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, c) = 1$. We compute $c' = c^{-1} \pmod{R}$ and $f'_{i1}(x, y, z) := c \cdot f_{i1}(x, y, z) \pmod{R}$. We define shift-polynomials g_{i1} and g'_{i1} as

$$\begin{aligned} g_{i1} &: x^{i_X} y^{i_Y} z^{i_Z} \cdot f'_{i1} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z^{m+r-1+t-i_Z} \text{ for } x^{i_X} y^{i_Y} z_1^{i_Z} \in S, \\ g'_{i1} &: x^{i_X} y^{i_Y} z^{i_Z} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_Z} \in M \backslash S, \end{aligned}$$

for sets of monomials

$$\begin{aligned} S &:= \bigcup_{0 \leq j \leq t} \left\{ x^{i_X} y^{i_Y} z^{i_Z+j} \middle| x^{i_X} y^{i_Y} z^{i_Z} \text{ is a monomial of } f_i(x, y, z_1)^{m-1} \right\}, \\ M &:= \left\{ x^{i_X} y^{i_Y} z^{i_Z} \middle| \text{ monomials of } x^{i'_X} y^{i'_Y} z^{i'_Z} \cdot f_i(x, y, z) \text{ for } x^{i'_X} y^{i'_Y} z^{i'_Z} \in S \right\}. \end{aligned}$$

By definition of sets of monomials S and M, it follows that

$$\begin{aligned} x^{i_X} y^{i_y} z^{i_Z} \in S \Leftrightarrow\ & i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\ & i_Z = 0, 1, \ldots, i_Y + t, \\ x^{i_X} y^{i_y} z^{i_Z} \in M \Leftrightarrow\ & i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m - i_X; i_Z = 0, 1, \ldots, i_Y + t. \end{aligned}$$

All these shift-polynomials g_{i1} and g'_{i1} modulo R have the root $(x, y, z) = (-d', k, \Phi(N) - \tilde{\Phi}(N))$ that is the same as $f_{i1}(x, y, z)$. We build a lattice with these polynomials.

Based on the Jochemsz-May strategy, the integer equation $f_{i1}(x, y, z) = 0$ can be solved when

$$\begin{aligned} & X^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} Y^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Z^{\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3} < W^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} \\ \Leftrightarrow\ & \gamma\left(\frac{1}{6}+\frac{\tau}{2}\right) + (\alpha+\beta-1)\left(\frac{1}{3}+\frac{\tau}{2}\right) + \delta\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right) < (\alpha+\beta)\left(\frac{1}{6}+\frac{\tau}{2}\right). \end{aligned}$$

By substituting $\tau = \frac{1-\gamma-\delta}{2\delta}$, the claimed inequality of Theorem 11 can be obtained:

$$\gamma < \frac{3 - \delta - 2\sqrt{\delta^2 + 3(\alpha+\beta-1)\delta}}{3}.$$

The condition 3 of Theorem 13 can be obtained by substituting $\alpha = 1$.

5.2.2 The Attack 2

In this section, we consider $(1, \beta, \gamma, \delta)$-partial key exposure attacks with the MSBs of d. As in Section 5.2.1, when $\tilde{d}$ which is the MSBs of d is given, RSA key generation can be written as $e(\tilde{d}M + d') = 1 + k\Phi(N)$ with some integer k such that $|k| \le N^{\beta}$ and $M = 2^{\lfloor \gamma \log N \rfloor}$. In this section, we use an additional information $\tilde{k} = \lfloor (e\tilde{d} - 1)/\tilde{\Phi}(N) \rfloor$ which is an approximation to k. From the simple calculation,

$$\begin{aligned}
|\tilde{k} - k| &= \left| \frac{e\tilde{d}M - 1}{\tilde{\Phi}(N)} - \frac{ed - 1}{\Phi(N)} \right| = \left| \frac{\Phi(N)(e\tilde{d}M - 1) - \tilde{\Phi}(N)(ed - 1)}{\tilde{\Phi}(N)\Phi(N)} \right| \\
&= \left| \frac{e(\Phi(N)\tilde{d}M - \tilde{\Phi}(N)d) + (\tilde{\Phi}(N) - \Phi(N))}{\tilde{\Phi}(N)\Phi(N)} \right| \\
&= \left| \frac{e\tilde{\Phi}(N)(\tilde{d}M - d) - (\tilde{\Phi}(N) - \Phi(N))(e\tilde{d}M - 1)}{\tilde{\Phi}(N)\Phi(N)} \right| \\
&\le \left| \frac{e(\tilde{d}M - d)}{\Phi(N)} \right| + \left| \frac{(\tilde{\Phi}(N) - \Phi(N))(e\tilde{d}M - 1)}{\tilde{\Phi}(N)\Phi(N)} \right|.
\end{aligned}$$

By definition,

$$\left| \frac{e(\tilde{d}M - d)}{\Phi(N)} \right| \le N^{\gamma} \quad \text{and} \quad \left| \frac{(\tilde{\Phi}(N) - \Phi(N))(e\tilde{d}M - 1)}{\tilde{\Phi}(N)\Phi(N)} \right| \le N^{\beta + \delta - 1}.$$

Therefore, $\tilde{k}$ satisfies the following condition:

$$|\tilde{k} - k| < 2N^{\lambda} \quad \text{where} \quad \lambda = \max\{\gamma, \beta + \delta - 1\}.$$

The approximate value enables us to obtain better results for large β. Since Sarkar and Maitra [SM08] used $\lambda = \max\{\gamma, \beta - 1/2\}$ for $\delta \le 1/2$, we improve the bound although the following lattice construction is completely the same. We find the root of the following polynomial over the integers:

$$f_{i2}(x, y, z) = c + ex + (\tilde{k} + y)(\tilde{\Phi} + z),$$

where $c = 1 - e\tilde{d}\tilde{M}$ as in Section 5.2.1. If we can recover the root $(x, y, z) = (-d', k - \tilde{k}, \Phi(N) - \tilde{\Phi}(N))$, whole secret information can be computed. The absolute values of the root are bounded above by $X := N^{\gamma}, Y := N^{\lambda}, Z := N^{\delta}$ where $\lambda = \max\{\gamma, \beta + \delta - 1\}$. Although the absolute values of solutions become smaller than those in Section

3.1, the result in this section is not always better since the Newton polygon of the polynomial becomes more complex.

We set an (possibly large) integer W such that $W < N^{1+\lambda}$ since $\|f_{i2}(xX, yY, zZ)\|_\infty \geq |\tilde{\Phi}(N)Y| \approx N^{1+\lambda}$. Next, we set an integer $R := WX^{m-1} \cdot Y^{m+r-1+t}Z^{m-1}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, c) = 1$. We compute $c' = c^{-1} \pmod{R}$ and $f'_{i2}(x, y, z) := c \cdot f_{i2}(x, y, z) \pmod{R}$. We define shift-polynomials g_{i1} and g'_{i1} as

$$
\begin{aligned}
&g_{i2} : x^{i_X} y^{i_Y} z^{i_Z} \cdot f'_{i2} \cdot X^{m-1-i_X} Y^{m-1+t-i_Y} Z^{m+r-1-i_Z} \text{ for } x^{i_X} y^{i_Y} z_1^{i_Z} \in S,\\
&g'_{i2} : x^{i_X} y^{i_Y} z^{i_Z} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_Z} \in M \backslash S,
\end{aligned}
$$

for sets of monomials

$$
\begin{aligned}
S &:= \bigcup_{0 \leq j \leq t} \left\{ x^{i_X} y^{i_Y+j} z^{i_Z} \middle| x^{i_X} y^{i_Y} z^{i_Z} \text{ is a monomial of } f_i(x, y, z_1)^{m-1} \right\},\\
M &:= \left\{ x^{i_X} y^{i_Y} z^{i_Z} \middle| \text{ monomials of } x^{i'_X} y^{i'_Y} z^{i'_Z} \cdot f_i(x, y, z) \text{ for } x^{i'_X} y^{i'_Y} z^{i'_Z} \in S \right\}.
\end{aligned}
$$

By definition of sets of monomials S and M, it follows that

$$
\begin{aligned}
x^{i_X} y^{i_y} z^{i_Z} \in S \Leftrightarrow\ & i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1+t-i_X;\\
& i_Z = 0, 1, \ldots, m-1-i_X,\\
x^{i_X} y^{i_y} z^{i_Z} \in M \Leftrightarrow\ & i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m+t-i_X; i_Z = 0, 1, \ldots, m-i_X.
\end{aligned}
$$

All these shift-polynomials g_{i2} and g'_{i2} modulo R have the root $(x, y, z) = (-d', k - \tilde{k}, \Phi(N) - \tilde{\Phi}(N))$ that is the same as $f_{i2}(x, y, z)$. We build a lattice with these polynomials.

Based on the Jochemsz-May strategy [JM06], the integer equation $f_{i1}(x, y, z) = 0$ can be solved when $X^{(\frac{1}{3}+\frac{\tau}{2})m^3} Y^{\left(\frac{1}{2}+\tau+\frac{\tau^2}{2}\right)m^3} Z^{(\frac{1}{2}+\frac{\tau}{2})m^3} < W^{(\frac{1}{3}+\frac{\tau}{2})m^3}$. By substituting $\tau = \frac{1-\gamma-\delta-\lambda}{2\lambda}$, the conditions 4 and 5 of Theorem 12 can be obtained. To follow the definition $\lambda = \max\{\gamma, \beta+\delta-1\}$, $\lambda = \gamma$ when $\beta < \frac{3(1-\delta)^2+4(1-\delta)}{4}$ and $\lambda = \beta+\delta-1$ otherwise.

5.2.3 Attack 3

In this section, we propose a better lattice construction than that in Section 5.2.2. Notice that the Newton polygon of $f_{i2}(x, y, z)$ is symmetric with respect to y and z. Hence, we should add extra shifts for the smaller variable. From the bound of the Attack 2, $Y = N^\lambda = N^{3(1-\delta)^2/4} \geq Z = N^\delta$ when $\delta < 1/3$. Therefore, we add extra shifts for z for such small δ. We construct a lattice that is symmetric with respect to y and z from that in Section 5.2.2 and the integer equation $f_{i2}(x, y, z) = 0$ can be solved when $X^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Y^{\left(\frac{1}{2}+\frac{\tau}{2}\right)m^3} Z^{\left(\frac{1}{2}+\tau+\frac{\tau^2}{2}\right)m^3} < W^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3}$. By substituting $\tau = \frac{1-\lambda-2\delta}{2\delta}$, the condition 6 of Theorem 12 can be obtained. Notice that when $\delta < 1/3$, $\beta + \delta - 1 < \gamma \leq 1 - \frac{2\sqrt{3\delta}}{3}$ always hold for $\beta < 1$.

5.3 Attacks with the MSBs of d by Solving Modular Equations

In this section, we solve modular equations and propose three attacks, i.e., Attacks 4–6, for $(1, \beta, \gamma, \delta)$-partial key exposure attacks with the MSBs of d. The Attack 4, 5, and 6 in Section 5.3.1, 5.3.2, and 5.3.3 correspond to the conditions 2, 3, and 1 of Theorem 12, respectively. Algorithm constructions in Section 5.3.1 and 5.3.2, that in Section 5.3.3 are similar to Takayasu-Kunihiro's [TK14d] and [TK14c], respectively.

5.3.1 The Attack 4

As in Section 5.2.2, when $\tilde{d}$ which is the MSBs of d is given, RSA key generation can be written as $e(\tilde{d}M + d') = 1 + k\Phi(N)$ with some integer k such that $|k| \leq N^\beta$ and $M = 2^{\lfloor \gamma \log N \rfloor}$. Then, we find the root of the following modular polynomial:

$$f_{MSBs,m}(x, y) = 1 + (\tilde{k} + x)(\tilde{\Phi}(N) + y) \pmod{e},$$

where $\tilde{k} = \lfloor (e\tilde{d} - 1)/\tilde{\Phi}(N) \rfloor$ which is an approximation to k as in Section 5.2.2. If we can recover the root $(x, y) = (k - \tilde{k}, \Phi(N) - \tilde{\Phi}(N))$, whole secret information can be computed. To obtain better results than integer equations based method in Section 5.2, we use a linearized variable $z = (\tilde{k} + x)y + 1$. The absolute values of the root are bounded above by $X := N^\lambda, Y := N^\delta, Z := N^{\beta+\delta}$ where $\lambda = \max\{\gamma, \beta + \delta - 1\}$.

To solve the modular equation $f_{MSBs,m}(x, y) = 0$, we use the following shift-polynomials $g_{[u,i]}^{MSBs.m1}(x, y)$ and $g_{[u,i]}^{MSBs.m2}(x, y)$:

$$\begin{aligned} g_{[u,i]}^{MSBs.m1}(x, y) &:= x^{u-i} f_{MSBs,m}(x, y)^i e^{m-i} \quad \text{and} \\ g_{[u,j]}^{MSBs.m2}(x, y) &:= y^j f_{MSBs,m}(x, y)^u e^{m-u}. \end{aligned}$$

All these shift-polynomials $g_{[u,i]}^{MSBs.m1}$ and $g_{[u,j]}^{MSBs.m2}$ modulo e^m have the root $(x, y) = (k - \tilde{k}, \Phi(N) - \tilde{\Phi}(N))$ that is the same as $f_{MSBs,m}(x, y)$. We build a lattice with these polynomials. In this section, we show a basic lattice construction to solve the modular equation and the resulting algorithm works when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1-\delta$ and $1/3 \leq \delta$, and when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1-\sqrt{\frac{\delta}{3}}$ and $\delta < 1/3$. In the lattice construction, we use shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,i]}^{MSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$, where

$$\begin{aligned}
&\mathcal{I}_x \Leftrightarrow\ u=0,1,\ldots,m; i=0,1,\ldots,u \ \text{ and}\\
&\mathcal{I}_y \Leftrightarrow\ u=0,1,\ldots,m; j=1,2,\ldots,\left\lfloor \frac{\beta-\lambda}{\delta}m+\frac{1+\lambda-\delta-2\beta}{\delta}u \right\rfloor,
\end{aligned}$$

respectively. Although the selections of shift-polynomials generate non-triangular basis matrices, we partially apply the linearization $z=(\tilde{k}+x)y+1$ and the basis matrices can be transformed into triangular as in [TK14c]. We follow the result and the basis matrices have diagonals

- $X^{u-\lceil l^{MSBs}(i)\rceil}Y^{i-\lceil l^{MSBs}(i)\rceil}Z^{\lceil l^{MSBs}(i)\rceil}e^{m-i}$ for $g_{[u,i]}^{MSBs.m1}(x,y)$ and
- $X^{u-\lceil l^{MSBs}(u+j)\rceil}Y^{u+j-\lceil l^{MSBs}(u+j)\rceil}Z^{\lceil l^{MSBs}(u+j)\rceil}e^{m-u}$ for $g_{[u,j]}^{MSBs.m2}(x,y)$ where
$$l^{MSBs}(j) := \max\left\{0, \frac{\delta j-(\beta-\lambda)m}{1+\lambda-2\beta}\right\}.$$

Notice that the result is valid only when $\frac{1+\lambda-\delta-2\beta}{\delta} \leq 1$, i.e., $\beta \geq \frac{1+\lambda-2\delta}{2}$, since unravelled linearization does not work well otherwise in the sense that the diagonals of triangular basis matrices become larger. We define the above polynomial selections for all the $g_{[u,j]}^{MSBs.m2}(x,y)$ to be helpful.

Lemma 7. *Assume there are shift-polynomials $g_{[u,u'+j']}^{MSBs.m1}(x,y)$ for $u=u'+j',\ldots,m$ and $g_{[u,u'+j'-u]}^{MSBs.m2}(x,y)$ for $u=u'+1,\ldots,u'+j'-1$ in lattice bases. Then, shift-polynomials $g_{[u',j']}^{MSBs.m2}(x,y)$are helpful polynomials when $u'=0,1,\ldots,m; j'=1,\ldots,\lfloor\frac{\beta-\lambda}{\delta}m+\frac{1+\lambda-\delta-2\beta}{\delta}u\rfloor$, whereas shift-polynomials $g_{[u',j']}^{MSBs.m2}(x,y)$are unhelpful polynomials when $u'=0,1,\ldots,m; j'>\frac{\beta-\lambda}{\delta}m+\frac{1+\lambda-\delta-2\beta}{\delta}u$.*

Proof. Consider the basis matrix $\boldsymbol{B}$. We add a new shift-polynomial $g_{[u',j']}^{MSBs2}(x,y)$ and construct the basis matrix $\boldsymbol{B}^{+}$. The value $\det(\boldsymbol{B}^{+})/\det(\boldsymbol{B})$ can be computed as

$$\frac{\det(\boldsymbol{B}^{+})}{\det(\boldsymbol{B})} = Y^{j'}Z^{u'}e^{m-u'}\cdot\left(\frac{XY}{Z}\right)^{m-u'},$$

where the size is bounded above by $N^{\delta j'+(\beta+\delta)u'+m-u'+(\lambda-\beta)(m-u')}$ within a constant factor. This value is smaller than the size of the modulus e^m, if and only if

$$\delta j'+(\beta+\delta)\,u'+m-u'+(\lambda-\beta)(m-u') \leq m$$

$$\Leftrightarrow j' \le \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u'$$

as required. □

When $m + \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}m = \frac{1-\beta}{\delta}m \le 1$, i.e., $\beta \ge 1-\delta$, shift-polynomials $g_{[u,j]}^{MSBs.m1}(x,y)$ for $u \ge \frac{\beta-\lambda}{2\beta+\delta-\lambda-1}; i \ge \frac{\beta-\lambda}{2\beta+\delta-\lambda-1}$ are unhelpful polynomials and do not contribute for the basis matrices to be triangular. In addition, when $\frac{1+\lambda-\delta-2\beta}{\delta} \le 0$, i.e., $\beta \ge \frac{1+\lambda-\delta}{2}$, not all the $g_{[u,j]}^{MSBs.m2}(x,y)$ become helpful polynomials. Hence, we use the above collection of shift-polynomials only when $\beta < \min\{1-\delta, \frac{1+\lambda-\delta}{2}\}$.

We show that the above lattice yields the condition 2 of Theorem 12. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = \frac{1-\lambda}{2\delta}m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X}Y^{s_Y}Z^{s_Z}e^{s_e}$, where

$$\begin{aligned} s_X &= \sum_{(u,i)\in\mathcal{I}_x}(u - \lceil l_{MSBs}(i)\rceil) + \sum_{(u,j)\in\mathcal{I}_y}(u - \lceil l_{MSBs}(u+j)\rceil) \\ &= \frac{1+\beta-2\lambda}{6\delta}m^3 + o(m^3), \\ s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y}(u+j) = \frac{1-\beta-\lambda+\beta^2-\beta\lambda+\lambda^2}{6\delta^2}m^3 + o(m^3), \\ s_Z &= \sum_{(u,i)\in\mathcal{I}_x}\lceil l_{MSBs}(i)\rceil + \sum_{(u,j)\in\mathcal{I}_y}\lceil l_{MSBs}(u+j)\rceil = \frac{1+\lambda-2\beta}{6\delta}m^3 + o(m^3), \\ s_e &= \sum_{(u,i)\in\mathcal{I}_x}(m-i) + \sum_{(u,j)\in\mathcal{I}_y}(m-u) = \frac{1+\beta-2\lambda+\delta}{6\delta}m^3 + o(m^3), \end{aligned}$$

as required. We can find solutions of $f_{MSBs}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < e^m$. Ignoring low order terms of m, the inequality becomes

$$\lambda^2 - (1+\beta)\lambda + \beta^2 - \beta + 1 - \delta > 0$$

that yields the bound

$$\lambda < \frac{1+\beta-\sqrt{-3+4\delta+6\beta-3\beta^2}}{2}.$$

To satisfy the restriction $\frac{1+\lambda-2\delta}{2} \le \beta < \min\{1-\delta, \frac{1+\lambda-\delta}{2}\}$ discussed above, the condition is valid only when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \le \beta < 1-\delta$ and $1/3 \le \delta$, and when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \le \beta < 1-\sqrt{\frac{\delta}{3}}$ and $\delta < 1/3$. Notice that the bound is always larger than $\beta+\delta-1$. When $\beta \ge 1-\sqrt{\frac{\delta}{3}}$ and $\delta < 1/3$, the Attack 3 becomes the best.

5.3.2 The Attack 5

In this section, we propose an attack for larger β, i.e., $\beta \geq 1-\delta$ for $1/3 \leq \delta$. As discussed above, the polynomial selections in Section 5.3.1 have unhelpful polynomials in this case and we should eliminate them to obtain better results. For the purpose, in this section, we use shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,j]}^{MSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$, where

$$\begin{aligned}
&\mathcal{I}_x \Leftrightarrow u=0,1,\ldots,m; i=0,1,\ldots,\min\{u,t\} \quad \text{and} \\
&\mathcal{I}_y \Leftrightarrow u=0,1,\ldots,m; j=1,2,\ldots,\min\left\{\left\lfloor \frac{\beta-\lambda}{\delta}m+\frac{1+\lambda-\delta-2\beta}{\delta}u \right\rfloor, t-u\right\}
\end{aligned}$$

for some integer t, respectively. The parameter $\tau = t/m$ should be optimized later. The selections of shift-polynomials generate basis matrices that are not triangular. However, we partially apply the linearization $z=(\tilde{k}+x)y+1$ and the basis matrices can be transformed into triangular as in Section 5.2.3. Moreover, the diagonals of the basis matrices are the same as those in Section 5.2.3. Hence, Lemma 7 also holds. We use the above polynomial selections when $\frac{\beta-\lambda}{\delta}m < t$ and $\frac{1+\lambda-\delta-2\beta}{\delta} > 0$ hold, i.e., $\beta < \min\{\delta\tau+\lambda, \frac{1+\lambda-\delta}{2}\}$, since all the $g_{[u,j]}^{MSBs.m2}(x,y)$ do not become helpful polynomials otherwise.

We show that the above lattice yields the condition 3 of Theorem 12. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = \left(\tau - \frac{(\delta\tau-\beta+\lambda)^2}{2\delta(1+\lambda-2\beta)}\right)m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X}Y^{s_Y}Z^{s_Z}e^{s_e}$, where

$$\begin{aligned}
s_X &= \sum_{(u,i)\in\mathcal{I}_x}(u-\lceil l_{MSBs}(i)\rceil) + \sum_{(u,j)\in\mathcal{I}_y}(u-\lceil l_{MSBs}(u+j)\rceil) \\
&= \left(\frac{\tau}{2} - \frac{(\delta\tau-\beta+\lambda)^3}{6\delta(1+\lambda-2\beta)^2}\right)m^3 - s_Z + o(m^3), \\
s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y}(u+j) \\
&= \left(\frac{\tau^2}{2} - \frac{(\delta\tau-\beta+\lambda)^3}{3\delta^2(1+\lambda-2\beta)} - \frac{(\beta-\lambda)(\delta\tau-\beta+\lambda)^2}{2\delta^2(1+\lambda-2\beta)}\right)m^3 + o(m^3), \\
s_Z &= \sum_{(u,i)\in\mathcal{I}_x}\lceil l_{MSBs}(i)\rceil + \sum_{(u,j)\in\mathcal{I}_y}\lceil l_{MSBs}(u+j)\rceil
\end{aligned}$$

$$= \left(\frac{(\delta\tau - \beta + \lambda)^2}{2\delta(1+\lambda-2\beta)} - \frac{(\delta\tau - \beta + \lambda)^3}{3\delta(1+\lambda-2\beta)^2} \right) m^3 + o(m^3),$$

$$s_e = \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-u)$$

$$= \tau m^3 - \frac{\tau^2}{2}m^3 + \frac{\tau^3}{6}m^3 - \frac{(\delta\tau - \beta + \lambda)^2}{2\delta(1+\lambda-2\beta)}m^3 + \frac{(\delta\tau - \beta + \lambda)^3}{6\delta(1+\lambda-2\beta)^2}m^3 + o(m^3).$$

We can find solutions $f_{MSBs}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < e^m$. Ignoring low order terms of m, the inequality becomes

$$\lambda\frac{\tau}{2} - (1-\delta)\frac{\tau^2}{2} + \frac{\tau^3}{6} < \frac{(\delta\tau - \beta + \lambda)^3}{6\delta(1+\lambda-2\beta)}.$$

To maximize the solvable root bounds, we set $\tau = 1 - \frac{\beta+\delta-1}{\delta-\sqrt{1+\lambda-2\beta}}$. To satisfy the restriction $\beta < \min\{\delta\tau + \lambda, \frac{1+\lambda-\delta}{2}\}$ discussed above, the attack works when $1-\delta \le \beta < \frac{3(1-\delta)(1+\delta)}{4}$ and $1/3 \le \delta < 2/3$, and when $1-\delta \le \beta < \delta - \frac{(2\delta-1)^2}{\delta^2}$ and $2/3 \le \delta$. The attack 2 becomes the best for larger β.

5.3.3 The Attack 6

In this section, we propose an attack for smaller β, i.e., $\beta < 1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}}$. As discussed above, the polynomial selections in Section 5.3.1 collect $g_{[u,j]}^{MSBs.m2}(x,y)$ where all the shifts are not helpful. The defect follows from the fact that when $\frac{1+\lambda-\delta-2\beta}{\delta} > 1$, the unravelled linearization does not work well and the diagonals of the resulting triangular basis matrices become larger. Hence, in this section, we use shift-polynomials $g_{[u,i]}^{MSBs.m1}(x,y)$ and $g_{[u,j]}^{MSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$, where

$$\mathcal{I}_x \Leftrightarrow \ u = 0,1,\ldots,m; i = 0,1,\ldots,u \ \text{ and}$$
$$\mathcal{I}_y \Leftrightarrow \ u = 0,1,\ldots,m; j = 1,2,\ldots,t+u,$$

for some integer t, respectively. The parameter $\tau = t/m$ should be optimized later. The selections of shift-polynomials generate basis matrices that are not triangular. However, we partially apply the linearization $z = (\tilde{k}+x)y+1$ and the basis matrices can be transformed into triangular as in Section 5.3.1. Moreover, the diagonals of the basis matrices are the same as those in Section 5.2.3 by modifying

$$l^{MSBs}(k) := \max\left\{0, \frac{k-\tau m}{2}\right\}.$$

Hence, Lemma 7 also holds.

We show that the above lattice yields the condition 1 of Theorem 12. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = (1+\tau)m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e}$, where

$$\begin{aligned} s_X &= \sum_{(u,i)\in\mathcal{I}_x} (u - \lceil l_{MSBs}(i) \rceil) + \sum_{(u,j)\in\mathcal{I}_y} (u - \lceil l_{MSBs}(u+j) \rceil) \\ &= \left(\frac{1}{3} + \frac{\tau}{2}\right) m^3 + o(m^3), \\ s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y} (u+j) = \left(\frac{2}{3} + \tau + \frac{\tau^2}{2}\right) m^3 + o(m^3), \\ s_Z &= \sum_{(u,i)\in\mathcal{I}_x} \lceil l_{MSBs}(i) \rceil + \sum_{(u,j)\in\mathcal{I}_y} \lceil l_{MSBs}(u+j) \rceil = \frac{1}{3} m^3 + o(m^3), \\ s_e &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-u) = \frac{1+\tau}{2} m^3 + o(m^3). \end{aligned}$$

We can find solutions of $f_{MSBs}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < e^m$. Ignoring low order terms of m, the inequality becomes

$$\lambda\left(\frac{1}{3} + \frac{\tau}{2}\right) + \delta\left(\frac{2}{3} + \tau + \frac{\tau^2}{2}\right) + \beta\frac{1}{3} + \frac{1+\tau}{2} < 1 + \tau.$$

To maximize the right hand side of the inequality, we set the parameter $\tau = \frac{1-2\delta-\lambda}{2\delta}$ and the condition becomes

$$\lambda < \frac{3 - 2\delta - 2\sqrt{4\delta^2 - 3\delta + 6\beta\delta}}{3}$$

as required.

5.4 Attacks with the LSBs of d by Solving Modular Equations

In this section, we solve modular equations and propose two attacks, i.e., Attacks 6 and 7, for $(1, \beta, \gamma, \delta)$-partial key exposure attacks with the LSBs of d. The Attack 7 and 8 in Section 5.4.1 and 5.4.2 corresponds to the conditions 2 and 1 of Theorem 13, respectively. Algorithm constructions in Section 5.4.1 and that in Section 5.4.2 is similar to Takayasu-Kunihiro's [TK14d] and [TK14c], respectively.

5.4.1 The Attack 7

As in Section 5.2.1, when $\tilde{d}$ which is the LSBs of d is given, RSA key generation can be written as $e(\tilde{d} + d'M) = 1 + k\Phi(N)$ with some integer k such that $|k| \leq N^{\beta}$ and $M = 2^{\lfloor (\beta-\gamma)\log N \rfloor}$. Then, we find the root of the following modular polynomials:

$$\begin{aligned} f_{LSBs.m1}(x,y) &:= 1 - e\tilde{d} + x(\tilde{\Phi}(N) + y) \pmod{eM}, \\ f_{LSBs.m2}(x,y) &:= 1 + x(\tilde{\Phi}(N) + y) \pmod{e}. \end{aligned}$$

If we can recover the root $(x,y) = (k, \Phi(N) - \tilde{\Phi}(N))$, whole secret information can be computed. To obtain better results than integer equations based method in Section 5.2, we use a linearized variable $z = xy + 1$. The absolute values of the root are bounded above by $X := N^{\beta}, Y := N^{\delta}, Z := N^{\beta+\delta}$.

To solve the modular equations $f_{LSBs.m1}(x,y) = 0$ and $f_{LSBs.m2}(x,y) = 0$, we use the following shift-polynomials $g_{[u,i]}^{LSBs.m1}(x,y)$ and $g_{[u,j]}^{LSBs.m2}(x,y)$:

$$\begin{aligned} g_{[u,i]}^{LSBs.m1}(x,y) &:= x^{u-i} f_{LSBs.m1}(x,y)^{i} (eM)^{m-i} \quad \text{and} \\ g_{[u,j]}^{LSBs.m2}(x,y) &:= y^{j} f_{LSBs.m1}(x,y)^{u-\lceil l^{LSBs}(j) \rceil} f_{LSBs.m2}(x,y)^{\lceil l^{LSBs}(j) \rceil} \cdot \\ &\qquad e^{m-u} M^{m-(u-\lceil l^{LSBs}(j) \rceil)}, \end{aligned}$$

where

$$l^{LSBs}(j) = \max\left\{0, \frac{\delta j - (\beta-\gamma)m}{1 - 2\beta + \gamma - \delta}\right\}.$$

All these shift-polynomials $g_{[u,i]}^{LSBs.m1}$ and $g_{[u,j]}^{LSBs.m2}$ modulo $(eM)^m$ have the root $(x,y) = (k, \Phi(N) - \tilde{\Phi}(N))$ that is the same as $f_{LSBs,m1}(x,y)$ and $f_{LSBs,m2}(x,y)$. We build a lattice with these polynomials. In this section, we show a basic lattice construction to solve the modular equations and the resulting algorithm works when $1 - \delta - \sqrt{\frac{\delta(1-\delta)}{3}} \leq \beta < 1 - \frac{\delta}{2} - \frac{\sqrt{3\delta(4-\delta)}}{6}$. In the lattice construction, we use shift-polynomials $g_{[u,i]}^{LSBs.m1}(x,y)$ and $g_{[u,j]}^{LSBs.m2}(x,y)$ with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$, where

$$\begin{aligned} \mathcal{I}_x &\Leftrightarrow \ u = 0,1,\ldots,m; i = 0,1,\ldots,u \quad \text{and} \\ \mathcal{I}_y &\Leftrightarrow \ u = 0,1,\ldots,m; j = 1,2,\ldots,\left\lfloor \frac{\beta-\lambda}{\delta}m + \frac{1+\lambda-\delta-2\beta}{\delta}u \right\rfloor, \end{aligned}$$

respectively. Although the selections of shift-polynomials generate non-triangular basis matrices, we partially apply the linearization $z = xy + 1$ and the basis matrices can be transformed into triangular as in [TK14c]. We follow the result and the basis matrices have diagonals

- $X^uY^i(eM)^{m-i}$ for $g_{[u,i]}^{LSBs.m1}(x,y)$ and
- $X^{u-\lceil l^{LSBs}(u+j)\rceil}Y^{u+j-\lceil l^{LSBs}(u+j)\rceil}Z^{\lceil l^{LSBs}(u+j)\rceil}e^{m-u}M^{m-(u-\lceil l^{LSBs}(u+j)\rceil)}$ for $g_{[u,j]}^{LSBs.m2}(x,y)$.

Notice that the result is valid only when $\frac{1+\gamma-\delta-2\beta}{\delta} \leq 1$, i.e., $\beta \geq \frac{1+\gamma-2\delta}{2}$, since unravelled linearization does not work well otherwise. We define the above polynomial selections for all the $g_{[u,j]}^{MSBs.m2}(x,y)$ to be helpful.

Lemma 8. *Assume there are shift-polynomials $g_{[u'+i,j'+i]}^{LSBs.m2}(x,y)$ for $i=1,2,\dots,m-u'$ in lattice bases. Then, shift-polynomials $g_{[u',j']}^{LSBs.m2}(x,y)$are helpful polynomials when $u'=0,1,\dots,m; j'=1,\dots,\lfloor\frac{\beta-\gamma}{\delta}m+\frac{1+\gamma-\delta-2\beta}{\delta}u'\rfloor$, whereas shift-polynomials $g_{[u',j']}^{LSBs.m2}(x,y)$are unhelpful polynomials when $u'=0,1,\dots,m; j'>\frac{\beta-\gamma}{\delta}m+\frac{1+\gamma-\delta-2\beta}{\delta}u'$.*

Proof. Consider the basis matrix $\boldsymbol{B}$. We add a new shift-polynomial $g_{[u',k']}^{LSBs.m2}(x,y)$ and construct the basis matrix $\boldsymbol{B}^+$. The value $\det(\boldsymbol{B}^+)/\det(\boldsymbol{B})$ can be computed as

$$\frac{\det(\boldsymbol{B}^+)}{\det(\boldsymbol{B})} = Y^{j'}Z^{u'}e^{m-u'}M^{u'},$$

where the size is bounded above by $N^{\delta j'+(\delta+\beta)u'+m-u'+(\beta-\gamma)u'}$ within a constant factor. This value is smaller than the size of the modulus $(eM)^m$, if and only if

$$\begin{aligned}\delta j' + (\delta+\beta)\,u' + m - u' + (\beta-\gamma)u' &\leq (1+\beta-\gamma)m \\ \Leftrightarrow j' \leq \frac{\beta-\gamma}{\delta}m + \frac{1-2\beta+\gamma-\delta}{\delta}u'\end{aligned}$$

as required. □

When $\frac{1+\gamma-\delta-2\beta}{\delta} \leq 0$, i.e., $\beta \geq \frac{1+\gamma-\delta}{2}$, all the shift-polynomials $g_{[u,j]}^{LSBs.m2}(x,y)$ in the above selection do not become a helpful polynomial since the assumption in Lemma 8 fails. Hence, we use the above collection of shift-polynomials only when $\beta < \frac{1+\gamma-\delta}{2}$.

We show that the above lattice yields the condition 2 of Theorem 13. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = \frac{1-\gamma}{2\delta}m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X}Y^{s_Y}Z^{s_Z}e^{s_e}M^{s_M}$, where

$$s_X + s_Z = \sum_{(u,i)\in\mathcal{I}_x} u + \sum_{(u,j)\in\mathcal{I}_y} u = \frac{1-\beta-\gamma}{6\delta}m^3 + o(m^3),$$

$$\begin{aligned}
s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y} (u+j) = \frac{1-\beta-\gamma+\beta^2-\beta\gamma+\gamma^2}{6\delta^2} m^3 + o(m^3),\\
s_Z &= \sum_{(u,i)\in\mathcal{I}_x} \lceil l_{MSBs}(i)\rceil + \sum_{(u,j)\in\mathcal{I}_y} \lceil l_{MSBs}(u+j)\rceil = \frac{1-2\beta+\gamma}{6\delta} m^3 + o(m^3),\\
s_e &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-u) = \frac{1+\beta-2\gamma+\delta}{6\delta} m^3 + o(m^3),\\
s_M &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-(u-\lceil l^{LSBs}(j)\rceil)) = \frac{2-\beta-\gamma}{6\delta} m^3 + o(m^3).
\end{aligned}$$

We can find solutions of $f_{LSBs.m1}(x,y) = 0$ and $f_{LSBs.m2}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < (eM)^m$. Ignoring low order terms of m, the inequality becomes

$$\gamma^2 - (1+\beta)\gamma + \beta^2 - \beta + 1 - \delta > 0$$

that yields the bound

$$\gamma < \frac{1+\beta-\sqrt{-3+4\delta+6\beta-3\beta^2}}{2}$$

as required. To satisfy the restriction $\frac{1+\gamma-2\delta}{2} \le \beta < \frac{1+\gamma-\delta}{2}$ discussed above, the condition is valid only when $1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}} \le \beta < 1-\frac{\delta}{2}-\frac{\sqrt{3\delta(4-\delta)}}{6}$. When $1-\frac{\delta}{2}-\frac{\sqrt{3\delta(4-\delta)}}{6} \le \beta$, Theorem 11 becomes the best.

5.4.2 The Attack 8

In this section we propose an attack that works when $\beta < 1-\delta-\sqrt{\frac{\delta(1-\delta)}{3}}$. In the lattice construction, we use the same shift-polynomials $g_{[u,i]}^{LSBs.m1}(x,y)$ and $g_{[u,j]}^{LSBs.m2}(x,y)$ where

$$l^{LSBs}(j) = \max\{0, j-\tau m\}$$

with indices in $\mathcal{I}_x$ and $\mathcal{I}_y$, where

$$\begin{aligned}
\mathcal{I}_x &\Leftrightarrow u = 0,1,\ldots,m; i = 0,1,\ldots,u \text{ and}\\
\mathcal{I}_y &\Leftrightarrow u = 0,1,\ldots,m; j = 1,2,\ldots,t+u,
\end{aligned}$$

respectively. The parameter $\tau = t/m$ should be optimized later. Although the selections of shift-polynomials generate non-triangular basis matrices, we partially apply the linearization $z = xy+1$ and the basis matrices can be transformed into triangular as in Section 5.4.1. The basis matrices have the same diagonals as those in Section 5.4.1 although the function $l^{LSBs}(j)$ is modified.

We show that the above lattice yields the condition 1 of Theorem 12. For the purpose, we compute the dimension

$$n = |\mathcal{I}_x \cup \mathcal{I}_y| = (1+\tau)m^2 + o(m^2),$$

and the determinant of the lattices $\det(\boldsymbol{B}) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e} M^{s_M}$, where

$$\begin{aligned}
s_X &= \sum_{(u,i)\in\mathcal{I}_x} u + \sum_{(u,j)\in\mathcal{I}_y} u = \left(\frac{2}{3}+\frac{\tau}{2}\right)m^3 + o(m^3),\\
s_Y + s_Z &= \sum_{(u,i)\in\mathcal{I}_x} i + \sum_{(u,j)\in\mathcal{I}_y} (u+j) = \left(\frac{2}{3}+\tau+\frac{\tau^2}{2}\right)m^3 + o(m^3),\\
s_e &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-u) = \frac{1+\tau}{2}m^3 + o(m^3),\\
s_M &= \sum_{(u,i)\in\mathcal{I}_x} (m-i) + \sum_{(u,j)\in\mathcal{I}_y} (m-(u-\lceil l^{LSBs}(j)\rceil))\\
&= \left(\frac{2}{3}m^3 + \frac{\tau}{2}\right)m^3 + o(m^3).
\end{aligned}$$

We can find solutions of $f_{LSBs.m1}(x,y) = 0$ and $f_{LSBs.m2}(x,y) = 0$ provided that $(\det(\boldsymbol{B}))^{1/n} < (eM)^m$. Ignoring low order terms of m, the inequality becomes

$$\beta\left(\frac{2}{3}+\frac{\tau}{2}\right) + \delta\left(\frac{2}{3}+\tau+\frac{\tau^2}{2}\right) + \frac{1+\tau}{2} + (\beta-\gamma)\left(\frac{2}{3}+\frac{\tau}{2}\right) < (1+\beta-\gamma)(1+\tau).$$

To maximize the right hand side of the inequality, we set the parameter $\tau = \frac{1-2\delta-\gamma}{2\delta}$ and the condition becomes

$$\gamma < \frac{3-2\delta-2\sqrt{4\delta^2-3\delta+6\beta\delta}}{3}$$

as required.

5.5 Concluding Remarks

In this paper, we defined partial key exposure attacks on RSA to capture general scenarios. Indeed, several existing works can be viewed as special cases of our general definition. Then we constructed eight attacks for the scenario. These attacks contain all the state-of-the-art partial key exposure attacks as special cases. Furthermore, our attacks improve several existing attacks in some cases. Due to our generalized definition of partial key exposure scenarios, we believe that our attacks can be used as a tool kit. The results enable even beginners of Coppersmith's methods to examine the security of several future variants of RSA and upcoming partial key exposure scenarios.

Although we tried to capture as wide class of partial key exposure scenarios as possible in this paper, we could only capture Multi-Prime RSA with partial information. There are other papers that studied partial key exposure attacks on other variants of RSA; RSA with moduli $N = p^r q$ [LZPL15, Sar16, TK16a], CRT-RSA [BM03, TK15, TK16b], RSA with multiple exponent pairs [PHL$^+$15, TK14b, TK16c], and more. It should be interesting open problems to study generalized partial key exposure scenarios for these variants as our work.

Chapter 6

Cryptanalyses of RSA with Moduli $N = p^r q$

6.1 Introduction

6.1.1 Background

RSA [RSA78] is one of the most well-known cryptosystems. Let N be the public RSA modulus, a product of two distinct primes p and q with the same bit-size. The public and secret exponents are positive integers such that

$$ed = 1 \pmod{(p-1)(q-1)}.$$

The RSA cryptosystem has been extensively studied in numerous papers including lattice based cryptanalysis. In this paper, we introduce two well-analyzed attacks; *small secret exponent attacks* and *partial key exposure attacks*. Boneh and Durfee [BD00] showed that a public RSA modulus N can be factorized when a secret exponent d is small, e.g., they proposed a weaker result $d < N^{0.284}$ and a stronger result $d < N^{0.292}$. Several papers [BM03, EJMdW05, SSM10, TK14d] have studied the security of RSA when some portions of the most significant bits (MSBs) or the least significant bits (LSBs) of d are exposed to attackers. The attack of Ernst et al. [EJMdW05] are the best results for general cases, e.g., the MSBs or the LSBs are exposed for general sizes of e and d. Although Blömer and May [BM03] and Sarkar et al. [SSM10] achieved the same result, they are only special cases of Ernst et al., e.g., Blömer and May's attack works only with the LSBs and the attack of Sarkar et al. works only with the MSBs and large e. Takayasu and Kunihiro [TK14d] proposed an improved attack of Ernst et al. for specific parameters, e.g., small d.

There are some variants of RSA. In this paper, we study two of them that we call *Takagi's RSA* [Tak98] and the *prime power RSA*. Both have a public RSA modulus

$$N = p^r q$$

for $r \geq 2$ with distinct primes p and q with the same bit-size. A public and a secret exponent $e \approx N^{\alpha}$ and $d \approx N^{\beta}$ satisfy

$$ed = 1 \pmod{(p-1)(q-1)}$$

for Takagi's RSA and

$$ed = 1 \pmod{p^{r-1}(p-1)(q-1)}$$

for the prime power RSA, respectively. The security of the variants have been analyzed; May [May04b] proposed small secret exponent attacks and partial key exposure attacks on the prime power RSA, and Itoh et al. [IKK08] proposed small secret exponent attacks on Takagi's RSA. Recently, the research area becomes a hot topic and several papers have been published. Huang et al. [HHX$^+$14] proposed partial key exposure attacks on Takagi's RSA. Sarkar [Sar14] proposed small secret exponent attacks on the prime power RSA, and further improved the result in [Sar16] with a result for partial key exposure attacks. The result is better than May for small r. Lu et al. [LZPL15] proposed small secret exponent attacks and partial key exposure attacks on the prime power RSA that fully improve May's attack and are better than Sarkar's attack for $r \geq 5$.

Attacks of May [May04b], and Lu et al. [LZPL15] make use of the special structure of a public modulus $N = p^r q$ and a key generation equality of the prime power RSA. Then, their attacks do not work for the standard RSA. However, a naive approach for the analysis of RSA variants should be generalizations of the attacks on the standard RSA. By definition, Takagi's RSA and the prime power RSA become the same as the standard RSA for $r = 1$. Hence, the attacks on the variants for $r = 1$ should completely cover the currently known best attacks on the standard RSA; the stronger Boneh-Durfee small secret exponent attack, partial key exposure attacks of Ernst et al., and Takayasu and Kunihiro. Since a public modulus N and key generations for the variants are more involved than the standard RSA, the analyses also become involved. Indeed, almost all the algorithm constructions and their strategies are too complicated to understand since the connections with those for the standard RSA are unclear. Moreover, existing attacks on the variants for $r = 1$ do not fully cover the currently known best attacks on the standard RSA.

6.1.2 Our Contributions

In this paper, we study the security of Takagi's RSA and the prime power RSA. The main focus of this paper is to generalize the currently known best attacks on the standard RSA, e.g., small secret exponent attacks and partial key exposure attacks, to the variants and to exploit the connections between their algorithm constructions. We show that the lattices used to attack the standard RSA can be transformed into lattices to attack the variants with simple operations. More concretely, the lattices used to attack the standard RSA can be transformed into lattices to attack Takagi's RSA (resp. the prime power RSA) by multiplying $\{1, q, pq, p^2q, \ldots, p^{r-1}q\}$ (resp. $\{q^a, pq^a, p^2q^a, \ldots, p^{r-1}q^a, p^{r-1}q^{a+1}\}$ with some integer a) to all the polynomials in the bases. Hence, dimensions of the lattices that we use to attack the variants are larger by a factor of $(r + 1)$ of the original lattices to attack the standard RSA. We believe that the connections offer better understanding for our algorithm constructions and enable us to easily generalize other attacks for their variants. As applications of our generalizations, we obtain the following results:

- In Section 6.2, we propose a partial key exposure attack on Takagi's RSA that fully generalizes the attack of Ernst et al. [EJMdW05]. Our attack becomes the same as Huang et al. [HHX$^+$14] with the exposed LSBs and better than the attack with the exposed MSBs for all α, β, and r.
- In Section 6.3, we give a simpler proof for the Itoh et al. small secret exponent attack on Takagi's RSA that fully generalizes the stronger Boneh-Durfee attack [BD00]. Our alternative proof fully generalizes that of Herrmann and May [HM10] for the stronger Boneh-Durfee attack and enables us to understand the Itoh et al. attack in detail. Based on the understanding, we propose a partial key exposure attack on Takagi's RSA with the exposed LSBs that fully generalizes Takayasu and Kunihiro's attack [TK14d]. The attack is better than our attack in Section 6.2 and that of Huang et al. [HHX$^+$14] for all α and r when β is small.
- In Section 6.4, we propose a small secret exponent attack on the prime power RSA that fully generalizes the weaker Boneh-Durfee attack [BD00]. To obtain the attack is technically easy since it is an extension of Sarkar's attack [Sar16] for arbitrary α. However, the extension reveals an important fact. Although Sarkar's attack, which captures only for $\alpha = 1$, is weaker than Lu et al. [LZPL15] for $r \geq 5$, our attack is better than Lu et al. for all r when

α is small. In addition, we propose a partial key exposure attack that fully generalizes the Ernst et al. [EJMdW05]. Our attack is better than Sarkar's result for small α and β, and is better than Lu et al. [LZPL15] for small r.

- In Section 6.5, we propose a small secret exponent attack on the prime power RSA that (almost) fully generalizes the stronger Boneh-Durfee [BD00]. The attack is better than our attack in Section 6.4. In addition, we propose a partial key exposure attack that (almost) fully generalizes Takayasu and Kunihiro [TK14d]. The attack is better than all known attacks for small r and β.

Since the elliptic curve method factorization [Len87] becomes efficient for large r and Boneh et al. [BDH99] revealed that only a $1/(r+1)$ fraction of the most significant bits of p suffices to factorize the modulus, they are the more important for small r. Then, we mainly compare our results and previous works for $r = 2$ and 3 throughout the paper, although we analyze the security for arbitrary r.

6.1.3 Technical Overview

In 1996, Coppersmith introduced lattice based methods to solve univariate modular equations [Cop96b] and bivariate integer equations [Cop96a], and they can be extended to more variables with a reasonable assumption (that we discuss later). The method is useful to evaluate the security of RSA. See [Cop97, Cop01, NS01, May03, May10]. Indeed, small secret exponent attack was firstly mentioned by Wiener [Wie90]. The attack is based on a continued fraction approach and works when $d < N^{0.25}$. Later, Boneh and Durfee revisited the attack and improved the bound to $d < N^{0.292}$ using Coppersmith's method. Although the original Coppersmith method is conceptually involved, simpler reformulations have been proposed; for modular equations by Howgrave-Graham [How97] and for integer equations by Coron [Cor04, Cor07]. In short, the methods construct a lattice whose bases consist of coefficients of polynomials that have the same roots as the original equations. By finding short lattice vectors using the LLL reduction, the original equations can be solved. The methods can solve modular (resp. integer) equations when sizes of roots are to some extent smaller than the modulus (resp. the norm of polynomial).

To maximize solvable root bounds, appropriate selections of lattice bases are essential. Jochemsz and May [JM06] proposed a conceptually simple strategy for the lattice constructions. Although the strategy does not always offer the best results, usually offers the best or similar bounds. For example, the Boneh-Durfee weaker result

$d < N^{0.284}$ can be obtained based on the strategy. Especially, the strategy is the more compatible with integer equations based analysis. To the best of our knowledge, there are no algorithms solving integer equations outperforming the Jochemsz-May strategy; currently known best algorithms solving any integer equations can be captured by the Jochemsz-May strategy. Furthermore, most algorithms by solving modular equations based on the Jochemsz-May strategy can also be obtained by solving integer equations based on the strategy although reverse does not always hold. For example, in the context of partial key exposure attacks on the standard RSA, Ernst et al. [EJMdW05] solved integer equations, whereas Blömer and May [BM03], and Sarkar et al. [SSM10] solved modular equations, and all these results are captured by the Jochemsz-May strategy. As we noted, attacks of Blömer and May, and Sarkar et al. are only the special cases of Ernst et al. However, in the context of security analyses of Takagi's RSA and the prime power RSA, there are no results known that solved integer equations. Therefore, we solve integer equations for Takagi's RSA (Section 6.2) and the prime power RSA (Section 6.4), and fully generalize the weaker Boneh-Durfee and Ernst et al.

Although the differences are small, there are some results that outperform the Jochemsz-May strategy by solving modular equations, e.g., the stronger Boneh-Durfee attack $d < N^{0.292}$ [BD00]. In general, analyses to obtain attacks outperforming the Jochemsz-May strategy are difficult. Indeed, there are no results known that attack Takagi's RSA or the prime power RSA outperforming the Jochemsz-May strategy except the Itoh et al. small secret exponent attack on Takagi's RSA [IKK08]. In the context of the stronger Boneh-Durfee attack, the proof is involved since determinants of lattices, whose basis matrices are non-triangular, should be calculated. For the purpose, Boneh and Durfee introduced geometrically progressive matrix although the notion is unfamiliar. Since Itoh et al. followed the proof, the analysis is also involved. The fact makes it difficult to obtain partial key exposure attacks on Takagi's RSA outperforming the Jochemsz-May strategy. As the hope of such situations, Herrmann and May [HM10] gave a simpler proof for the stronger Boneh-Durfee attack. They used unravelled linearization [HM09] and transformed Boneh and Durfee's non-triangular basis matrices to be triangular. The simpler proof offers better understanding of the attack. Based on the understanding, Takayasu and Kunihiro extended the stronger Boneh-Durfee attack to partial key exposure attacks outperforming the Jochemsz-May strategy. As the same way, we give a simpler proof of the Itoh et al. and propose a partial key exposure attack on Takagi's RSA outperforming the Jochemsz-May strategy (Section 6.3). Moreover, we analyze better lattice constructions and propose small secret exponent attacks and partial key exposure attacks on the prime power RSA outperforming the Jochemsz-May strategy (Section 6.5).

6.2 Attacks on Takagi's RSA by Solving Integer Equations

In this section, we analyze the security of Takagi's RSA by solving integer equations. In Section 6.2.1, we give an alternative proof of the Itoh et al. small secret exponent attack [IKK08] that was proposed by solving modular equations. In Section 6.2.2, we propose a partial key exposure attack that fully generalizes the attack of Ernst et al. [EJMdW05].

6.2.1 Small Secret Exponent Attack

In this section, we revisit the Itoh et al. small secret exponent attacks [IKK08]. The result fully generalizes the weaker Boneh-Durfee [BD00] in the sense that it completely covers their attack, i.e.,

$$\beta < \frac{7 - 2\sqrt{7}}{6}$$

for $r = 1$ and $\alpha = 1$.

Theorem 14 ([IKK08])**.** *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of Takagi's RSA, respectively. If*

$$\beta < \frac{7 - 2\sqrt{1 + 3(r+1)\alpha}}{3(r+1)} \text{ for } \alpha \le \frac{1}{r+1}$$

holds, then Takagi's RSA modulus N can be factorized in polynomial time.

Although the original paper [IKK08] solved modular equations for the attack, we solve integer equations and give an alternative proof. The proof is convenient to analyze partial key exposure attacks in Section 6.2.2. Moreover, we exploit the exact connection between the algorithm constructions of Itoh et al. and the weaker Boneh-Durfee.

Proof. Recall the key generation for Takagi's RSA;

$$ed = 1 + \ell(p-1)(q-1)$$

with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. To recover the secret exponent d, we use the following polynomial

$$f_{T.SSE.i}(x, y, z_1, z_2) = 1 + ex + y(z_1 + 1)(z_2 + 1)$$

whose root over the integers is

$$(x, y, z_1, z_2) = (-d, \ell, -p, -q).$$

The absolute values of the root for (x, y, z_1) are bounded above by

$$X := N^{\beta}, Y := N^{\alpha+\beta-2/(r+1)}, Z_1 := N^{1/(r+1)}$$

within constant factors. For the notational convenience, we also use $Z_2 := N/Z_1^r$. We set an (possibly large) integer W such that

$$W < N^{\alpha+\beta}$$

since $\|f_{T.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)\|_\infty \geq |eX| \approx N^{\alpha+\beta}$. Next, we set an integer

$$R := W(XY)^{m-1} Z_1^{m+r-1+t} Z_2^{m-1+t}$$

with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$. We define shift-polynomials $g_{T.SSE.i}$ and $g'_{T.SSE.i}$ as

$$\begin{aligned}
g_{T.SSE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot f_{T.SSE.i} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z_1^{m+r-1+t-i_{Z_1}} Z_2^{m-1+t-i_{Z_2}} \\
&\quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S_1 \cup S_2, \\
g'_{T.SSE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in (M_1 \cup M_2) \backslash (S_1 \cup S_2),
\end{aligned}$$

for sets of monomials

$$S_1 := \bigcup_{0 \leq j \leq t} \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}+j} \;\middle|\; x^{i_X} y^{i_Y} z_1^{i_{Z_1}} \text{ is a monomial of } f_{T.SSE.i}(x, y, z_1, z_2)^{m-1} \right\},$$

$$S_2 := \bigcup_{0 \leq j \leq t} \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}+j} \;\middle|\; \begin{array}{c} x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \text{ is a monomial of} \\ \tilde{s} \cdot f_{T.SSE.i}(x, y, z_1, z_2)^{m-1} \text{ for } i_{Z_2} \geq 1 \\ \text{where } \tilde{s} = \{z_1^{r-1} z_2, z_1^{r-2} z_2, \ldots, z_1 z_2\} \end{array} \right\},$$

$$M_1 := \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} \;\middle|\; \begin{array}{c} \text{monomials of } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} \cdot f_{T.SSE.i}(x, y, z_1, z_2) \\ \text{for } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} \in S_1 \end{array} \right\},$$

$$M_2 := \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \;\middle|\; \begin{array}{c} \text{monomials of } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \cdot f_{T.SSE.i}(x, y, z_1, z_2) \\ \text{for } i_{Z_2} \geq 1 \text{ where } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \in S_2 \end{array} \right\}.$$

By definition of sets of monomial S_1, S_2, M_1, and M_2, it follows that

$$x^{i_X} y^{i_y} z_1^{i_{Z_1}} \in S_1 \Leftrightarrow \; i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X;$$

$$\begin{aligned}
& i_{Z_1} = 0,1,\ldots,i_Y+t,\\
x^{i_X}y^{i_y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \in S_2 \Leftrightarrow\ & i_X = 0,1,\ldots,m-1; i_Y = 0,1,\ldots,m-1-i_X;\\
& i_{Z_1} = 0,1,\ldots,r-1; i_{Z_2} = 1,2,\ldots,i_Y+t+1,\\
x^{i_X}y^{i_y}z_1^{i_{Z_1}} \in M_1 \Leftrightarrow\ & i_X = 0,1,\ldots,m; i_Y = 0,1,\ldots,m-i_X;\\
& i_{Z_1} = 0,1,\ldots,i_Y+t,\\
x^{i_X}y^{i_y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \in M_2 \Leftrightarrow\ & i_X = 0,1,\ldots,m; i_Y = 0,1,\ldots,m-i_X; i_{Z_1} = 0,1,\ldots,r-1;\\
& i_{Z_2} = 1,2,\ldots,i_Y+t+1.
\end{aligned}$$

All these shift-polynomials $g_{T.SSE.i}(x,y,z_1,z_2)$ and $g'_{T.SSE.i}(x,y,z_1,z_2)$ modulo R have the root $(x,y,z_1,z_2) = (-d,\ell,-p,-q)$ that are the same as $f_{T.SSE.i}(x,y,z_1,z_2)$. All these shift-polynomials $g_{T.SSE.i}(xX,yY,z_1Z_1,z_2Z_2)$ and $g'_{T.SSE.i}(xX,yY,z_1Z_1,z_2Z_2)$ have a common divisor R. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{T.SSE.i}(xX,yY,z_1Z_1,z_2Z_2)$ and $g'_{T.SSE.i}(xX,yY,z_1Z_1,z_2Z_2)$ as the bases. The shift-polynomials generate a triangular basis matrix. We compute

$$\begin{aligned}
|S_1+S_2| &= (r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3 + o(m^3),\\
s_X &= \sum_{\substack{x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\\ \in (M_1\cup M_2)\backslash(S_1\cup S_2)}} i_X = (r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3 + o(m^3),\\
s_Y &= \sum_{\substack{x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\\ \in (M_1\cup M_2)\backslash(S_1\cup S_2)}} i_Y = (r+1)\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3 + o(m^3),\\
s_Z &= \sum_{\substack{x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}}\\ \in (M_1\cup M_2)\backslash(S_1\cup S_2)}} (i_{Z_1}+i_{Z_2}) = (r+1)\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3 + o(m^3).
\end{aligned}$$

Ignoring low order terms of m, based on the Jochemsz-May strategy, LLL outputs short vectors that satisfy Howgrave-Graham's Lemma and that contradict Hinek-Stinson's Lemma when $X^{s_X}Y^{s_Y}Z^{s_Z} < W^{|S_1+S_2|}$ holds. The condition becomes

$$X^{(r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} Y^{(r+1)\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Z^{(r+1)\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3} < W^{(r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3}. \tag{6.1}$$

Then, the inequality becomes

$$\begin{aligned}&\beta(r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)+\left(\alpha+\beta-\frac{2}{r+1}\right)(r+1)\left(\frac{1}{3}+\frac{\tau}{2}\right)\\&+\frac{1}{r+1}(r+1)\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)<(\alpha+\beta)(r+1)\left(\frac{1}{6}+\frac{\tau}{2}\right)\end{aligned}$$

that leads to

$$0 < -(r+1)\alpha - (r+1)(2+3\tau)\beta + 3 + 3\tau - 3\tau^2.$$

To maximize the right hand side of the inequality, we set the parameter

$$\tau = \frac{1-(r+1)\beta}{2}$$

and the condition becomes

$$\beta < \frac{7-2\sqrt{1+3(r+1)\alpha}}{3(r+1)}$$

as required. To satisfy the restriction $\tau \geq 0$, the condition $\beta \leq \frac{1}{r+1}$ should hold. The condition results in $\alpha \geq \frac{1}{r+1}$. □

The algorithm construction fully generalizes that of Ernst et al. that is a partial key exposure extension of the weaker Boneh-Durfee by solving integer equations, although the connection is hard to follow from the original proof in [IKK08]. In [EJMdW05], Ernst et al. used a similar polynomial as $f_{T.SSE.i}$ and the condition becomes

$$X^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3} Y^{\left(\frac{1}{3}+\frac{\tau}{2}\right)m^3} Z^{\left(\frac{1}{6}+\frac{\tau}{2}+\frac{\tau^2}{2}\right)m^3} < W^{\left(\frac{1}{6}+\frac{\tau}{2}\right)m^3}.$$

Clearly, the condition relates to the above one. The connection comes from our definition of sets of monomials S_1, S_2, M_1, and M_2 that are generalizations of those of Ernst et al. by a factor of $(r+1)$. More concretely, each of our S_1 and S_2 for $i_{Z_1} = 0, 1, \ldots, r-1$ play the same role as that for Ernst et al. and so do M_1 and M_2 for $i_{Z_1} = 0, 1, \ldots, r-1$. Hence, our n, s_X, s_Y, and s_Z are larger by a factor of $(r+1)$ of Ernst et al. As a result, we successfully proposed a generalization the weaker Boneh-Durfee. In Section 6.2.2, we use the same sets of monomials S_1, S_2, M_1, and M_2 and construct a generalization of the partial key exposure attack of Ernst et al.

6.2.2 Partial Key Exposure Attack

In this section, we propose partial key exposure attacks on Takagi's RSA that satisfy the following property.

Theorem 15. *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of Takagi's RSA, respectively. When $(\beta - \delta)\log N$ bits of the most significant bits or the least significant bits are exposed, if*

$$\delta < \frac{5 - 2\sqrt{-5 + 3(r+1)(\alpha+\beta)}}{3(r+1)} \quad \textit{for} \quad \frac{2}{r+1} \le \alpha + \beta$$

holds, then Takagi's RSA modulus N can be factorized in polynomial time.

The result fully generalizes Ernst et al. [EJMdW05] in the sense that it completely covers their attack, i.e.,

$$\beta < \frac{5 - 2\sqrt{-5 + 6(\alpha+\beta)}}{6}$$

for $r = 1$. When the LSBs are exposed, our attack becomes the same as Huang et al. [HHX$^+$14]. Although the attack of Huang et al. with the MSBs is weaker than that with the LSBs, our attacks work in the same conditions. We can obtain the advantage by solving integer equations. When the MSBs are exposed, our attack is always better than Huang et al. [HHX$^+$14] that works when

$$\delta < \frac{7 - \sqrt{-39 + 24(r+1)(\alpha+\beta)}}{4(r+1)}.$$

Figures 6.1 compare Theorem 15 and Huang et al. for $r = 2$ and 3. Our attack is the better for all β, e.g., our attack works with less partial information.

Proof. Recall the key generation for Takagi's RSA with the exposed bits (regardless of the MSBs or the LSBs);

$$e\left(\tilde{d} + (d - \tilde{d})\right) = 1 + \ell(p-1)(q-1)$$

with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. To recover unknown parts $d - \tilde{d}$, we use the following polynomial

$$f_{T.PKE.i}(x, y, z_1, z_2) = 1 - e\tilde{d} + eMx + y(z_1 + 1)(z_2 + 1),$$

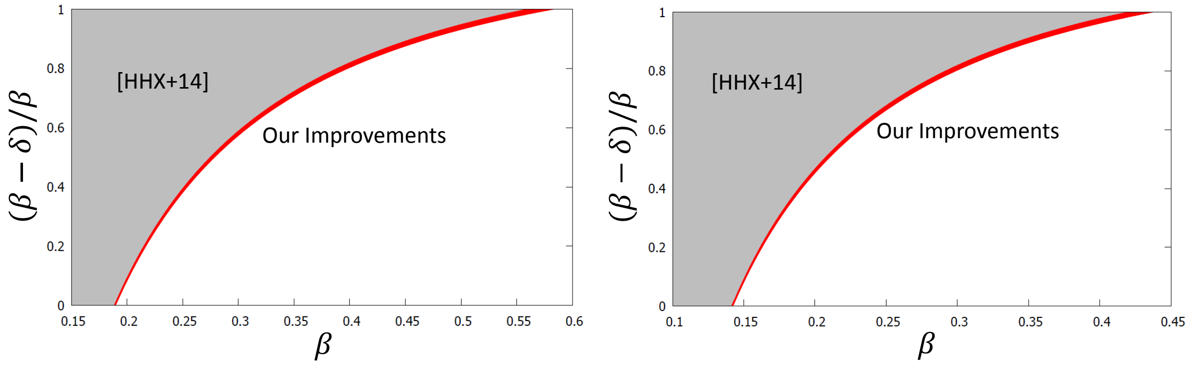


Fig. 6.1. Comparisons of partial key exposure attacks on Takagi's RSA when the MSBs are exposed for $\alpha = 1/(r+1)$. We compare how much portions of d should be exposed for β between the attack of Huang et al. [HHX$^+$14] and our Theorem 15. The left figure is for $r = 2$ and the right figure is for $r = 3$.

where $M = 1$ (resp. $M = 2^{\lfloor(\beta-\delta)\log N\rfloor}$) with the exposed MSBs (resp. LSBs) whose root over the integers is

$$(x, y, z_1, z_2) = \left(-(d - \tilde{d}), \ell, -p, -q\right).$$

The absolute values of the root (x, y, z_1) are bounded by

$$X := N^{\delta}, Y := N^{\alpha+\beta-2/(r+1)}, Z_1 := 2N^{1/(r+1)}.$$

For the notational convenience, we also use the notation $Z_2 := N/Z_1^r$.

These formulations and those for small secret exponent attacks in Section 6.2.1 are essentially the same when we use the Jochemsz-May strategy. That means the Newton polygons of polynomials $f_{T.SSE.i}(x, y, z_1, z_2)$ and $f_{T.PKE.i}(x, y, z_1, z_2)$ are the same, e.g., there are six monomials for variables $1, x, y, yz_1, yz_2$, and yz_1z_2. Hence, we use almost the same algorithm construction. We set an (possibly large) integer W such that

$$W < N^{\alpha+\beta}$$

since $\|f_{T.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)\|_\infty \geq \max\{|1 - e\tilde{d}|, |eMX|\} \approx N^{\alpha+\beta}$. Next, we set an integer

$$R := W(XY)^{m-1} \cdot Z_1^{m+r-1+t} Z_2^{m-1+t}$$

with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, 1 - e\tilde{d}) = 1$.

We compute $c = (1 - e\tilde{d})^{-1} \pmod{R}$ and

$$f'_{T.PKE.i}(x, y, z_1, z_2) := c \cdot f_{T.PKE.i}(x, y, z_1, z_2) \pmod{R}.$$

We define shift-polynomials $g_{T.PKE.i}$ and $g'_{T.PKE.i}$ as

$$\begin{aligned} g_{T.PKE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot f'_{T.PKE.i} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z^{m+r-1+t-i_{Z_1}-i_{Z_2}} \\ &\quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S_1 \cup S_2, \\ g'_{T.PKE.i} &: x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in (M_1 \cup M_2) \backslash (S_1 \cup S_2), \end{aligned}$$

for sets of monomials S_1, S_2, M_1, and M_2 that are the same as in Section 6.2.1 where $f_{T.SSE.i}$ is replaced by $f'_{T.PKE.i}$. All these shift-polynomials $g_{T.PKE.i}$ and $g'_{T.PKE.i}$ modulo R have the root $(x, y, z_1, z_2) = (-(d - \tilde{d}), \ell, -p, -q)$ that are the same as $f_{T.PKE.i}(x, y, z_1, z_2)$. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{T.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{T.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)$ as the bases. Hence, ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short lattice vectors that satisfy Howgrave-Graham's Lemma when the inequality (5.1) holds. For partial key exposure attacks (regardless of the MSBs or the LSBs are exposed), the inequality becomes

$$\begin{aligned} &\delta(r+1)\left(\frac{1}{6} + \frac{\tau}{2}\right) + \left(\alpha + \beta - \frac{2}{r+1}\right)(r+1)\left(\frac{1}{3} + \frac{\tau}{2}\right) \\ &+ \frac{1}{r+1}(r+1)\left(\frac{1}{6} + \frac{\tau}{2} + \frac{\tau^2}{2}\right) < (\alpha + \beta)(r+1)\left(\frac{1}{6} + \frac{\tau}{2}\right) \end{aligned}$$

that leads to

$$0 < -(r+1)(\alpha + \beta) - (r+1)\delta(1 + 3\tau) + 3 + 3\tau - 3\tau^2.$$

To maximize the right hand side of the inequality, we set the parameter

$$\tau = \frac{1 - (r+1)\delta}{2}$$

and the condition becomes

$$\delta < \frac{5 - 2\sqrt{-5 + 3(r+1)(\alpha + \beta)}}{3(r+1)}$$

as required. To satisfy the restriction $\eta \geq 0$, the condition $\delta \leq \frac{1}{r+1}$ should hold. The condition results in $\frac{2}{r+1} \leq \alpha + \beta$. □

As we claimed in Section 6.2.1, the algorithm construction fully generalizes Ernst et al.

In Section 6.3.2, we propose an improved attack when the LSBs are exposed. It seems that our Theorem 15 with the exposed MSBs is hard to be improved. Although there exist attacks that are better than Ernst et al. (the other attack of Ernst et al. [EJMdW05] and Takayasu and Kunihiro's attack [TK14d]), by definition, it seems difficult to generalize the attacks for Takagi's RSA since both attacks make use of the MSBs of ℓ. To compute the MSBs of ℓ, we have to know the MSBs of $(p-1)(q-1)$. It is possible for the standard RSA since $pq = N$. However, it seems difficult for Takagi's RSA. Hence, to improve Theorem 15, we have to exploit the special structure of Takagi's RSA or improve the attacks on the standard RSA without the knowledge of the MSBs of ℓ.

6.3 Attacks on Takagi's RSA by Solving Modular Equations

In this section, we analyze the security of Takagi's RSA by solving modular equations. In Section 6.3.1, we give an alternative proof of the Itoh et al. small secret exponent attack [IKK08] that is analogous to Herrmann and May [HM10]. In Section 6.3.2, we propose a partial key exposure attack that fully generalizes Takayasu and Kunihiro's result [TK14d].

6.3.1 Small Secret Exponent Attack

In this section, we prove the following Itoh et al. small secret exponent attack. The result fully generalizes the stronger Boneh-Durfee [BD00] in the sense that it completely covers their attack, i.e., $\beta < 1 - 1/\sqrt{2}$ for $r = 1$ and $\alpha = 1$.

Theorem 16 ([IKK08])**.** *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of Takagi's RSA, respectively. If*

$$\beta < \frac{2 - \sqrt{(r+1)\alpha}}{r+1} \text{ for } \frac{1}{r+1} \leq \alpha$$

holds, then Takagi's RSA modulus N can be factorized in polynomial time.

The original proof in [IKK08] is involved since they used geometrically progressive matrix. We use unravelled linearization [HM09] and offer simpler proof. Moreover, we exploit the exact connection between the algorithm constructions of Itoh et al. and the stronger Boneh-Durfee.

Proof. Recall the key generation for Takagi's RSA modulo $N = p^r q$,

$$ed = 1 + \ell(p-1)(q-1)$$

with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. Itoh et al. [IKK08] considered a polynomial

$$f_{T.SSE.m}(x, y_1, y_2) = 1 + x(y_1+1)(y_2+1).$$

The polynomial modulo e has the root

$$(x, y_1, y_2) = (\ell, -p, -q).$$

The absolute values are bounded above by

$$X := N^{\alpha+\beta-2/(r+1)}, Y_1 = Y_2 := N^{1/(r+1)}.$$

Let $m = \omega(r)$ be an integer and $\tau \geq 0$. To solve a modular equation $f_{T.SSE.m}(x, y_1, y_2) = 0 \pmod{e}$, we use shift-polynomials

$$g_{T.SSE.m}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{i_{Y_2}} f^u_{T.SSE.m}(x, y_1, y_2) e^{m-u}$$

with indices in

$$\begin{aligned}
\mathcal{I}_{x1} &\Leftrightarrow\ u = 0, 1, \dots, m; i_X = 0, 1, \dots, m-u; i_{Y_1} = 0; i_{Y_2} = 0, \text{or} \\
\mathcal{I}_{x2} &\Leftrightarrow\ u = 0, 1, \dots, m; i_X = 0, 1, \dots, m-u; i_{Y_1} = 0, 1, \dots, r-1; i_{Y_2} = 1, \\
\mathcal{I}_{y1} &\Leftrightarrow\ u = 0, 1, \dots, m; i_X = 0; i_{Y_1} = 1, 2, \dots, \lceil \tau u \rceil; i_{Y_2} = 0, \text{or} \\
\mathcal{I}_{y2} &\Leftrightarrow\ u = 0, 1, \dots, m; i_X = 0; i_{Y_1} = 0, 1, \dots, r-1; i_{Y_2} = 2, 3, \dots, \lceil \tau u \rceil.
\end{aligned}$$

All these shift-polynomials $g_{T.SSE.m}$ modulo e^m have the roots $(x, y_1, y_2) = (\ell, -p, -q)$ that are the same as $f_{T.SSE.m}$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{T.SSE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases.

Here, we observe why the construction offers a bound outperforming the Jochemsz-May strategy. In the above $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$, i_{Y_1} and i_{Y_2} are upper bounded by $\lceil \tau u \rceil$ that depend on u. In the Jochemsz-May strategy, the corresponding indices ($i_{Z_1} - i_Y$ and $i_{Z_2} - i_Y$ in S_1, S_2, M_1, and M_2 in Section 6.2.1) are bounded by $t = \tau m$ that only depends m. Since the former covers the latter, we can analyze broader classes of lattice constructions. The restriction of the Jochemsz-May strategy offers simpler analysis with a triangular basis matrix although that does not always offer the best bound. Moreover, the parameter is eventually set to $\tau = 1-(r+1)\beta$. The optimization follows from the fact that shift-polynomials $g_{T.SSE.m}$ with indices in $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$ reduce the norm of outputs of the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than the modulus e^m. This observation enables readers to understand our improvements in Section 6.5 easily.

However, the former selection requires involved analysis since the shift-polynomials generate non-triangular basis matrices. The dependence of the Jochemsz-May strategy always generates triangular basis matrices and the analysis is easy. To construct partial key exposure attacks outperforming the Jochemsz-May strategy, we require better understanding for small secret exponent attacks. For the purpose, we show an analogous elementary proof to Herrmann and May [HM10]. Although the above shift-polynomials generate non-triangular basis matrices, we can transform it to be triangular by using unravelled linearization.

Lemma 9. *Using a linearization $z_1 = 1 + xy_1$ and $z_2 = 1 + xy_2$, the above shift-polynomials generate a triangular basis matrix. The diagonals of the basis matrix for $g_{T.SSE.m}$ are*

- $X^{u+i_X} Y_1^u e^{m-u}$ *for indices in $\mathcal{I}_{x1}$,*
- $X^{u+i_X} Y_1^{i_{Y_1}} Y_2^{u+1} e^{m-u}$ *for indices in $\mathcal{I}_{x2}$,*
- $Y_1^{i_{Y_1}} Z_1^u e^{m-u}$ *for indices in $\mathcal{I}_{y1}$,*
- $Y_1^{i_{Y_1}} Y_2 Z_2^u e^{m-u}$ *for indices in $\mathcal{I}_{y2}$.*

Indeed, the transformation is analogous to Herrmann and May [HM10], and show the exact connection with the stronger Boneh-Durfee and the Itoh et al. attack although the connection is hard to follow from the original proof [IKK08]. The shift-polynomials for indices in $\mathcal{I}_{x1}$ and $\mathcal{I}_{x2}$ for $i_{Y_1} = 0, 1, \ldots, r-1$ (resp. $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$ for $i_{Y_1} = 0, 1, \ldots, r-1$) play the same role as x-shifts (resp. y-shifts) of the stronger Boneh-Durfee. Ignoring low order terms of m, the dimension of the lattice is $(r+1)\left(\frac{1}{2} + \frac{\tau}{2}\right) m^2$, and the determinant of the basis matrix is $X^{(r+1)\left(\frac{1}{3}+\frac{\tau}{3}\right)m^3} Y^{(r+1)\left(\frac{1}{6}+\frac{\tau}{3}+\frac{\tau^2}{6}\right)m^3} e^{(r+1)\left(\frac{1}{3}+\frac{\tau}{6}\right)m^3}$. Notice that $Z_1 = Z_2 \approx XY$. Again, we stress the connection with the stronger Boneh-Durfee. In the proof, a dimension of a lattice is $\left(\frac{1}{2} + \frac{\tau}{2}\right) m^2$ and its determinant is $X^{\left(\frac{1}{3}+\frac{\tau}{3}\right)m^3} Y^{\left(\frac{1}{6}+\frac{\tau}{3}+\frac{\tau^2}{6}\right)m^3} e^{\left(\frac{1}{3}+\frac{\tau}{6}\right)m^3}$. Hence, it is clear that the algorithm construction of Itoh et al. is a generalization of that for the stronger Boneh-Durfee. We set the parameter $\tau = 1 - (r+1)\beta$, and obtain Theorem 16. Here, we omit overall calculations since they are completely the same as those in [IKK08]. □

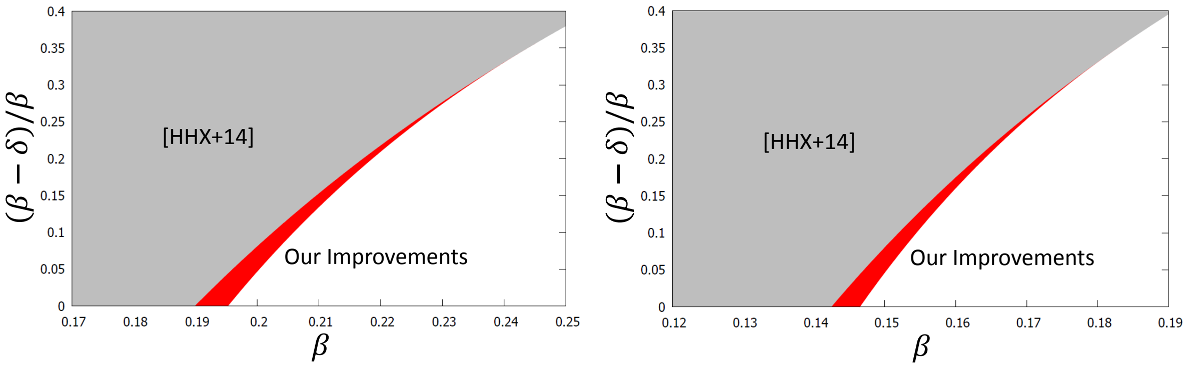


Fig. 6.2. Comparisons of partial key exposure attacks on Takagi's RSA when the LSBs are exposed and $\alpha = 1/(r+1)$. We compare how much portions of d should be exposed for β between the attack of Huang et al. [HHX$^+$14] and our Theorem 17. The left figure is for $r = 2$ and the right figure is for $r = 3$.

6.3.2 Partial Key Exposure Attack

In this section, we propose a partial key exposure attack on Takagi's RSA that satisfies the following property.

Theorem 17. *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of Takagi's RSA, respectively. When $(\beta - \delta)\log N$ bits of the least significant bits are exposed, if*

$$\delta < \frac{2+(r+1)\beta - \sqrt{-12+4(r+1)\alpha+12(r+1)\beta-3(r+1)^2\beta^2}}{2(r+1)} \quad \textit{and}$$
$$\beta \leq \frac{9-\sqrt{-3+12(r+1)\alpha}}{6(r+1)}$$

hold, then Takagi's RSA modulus N can be factorized in polynomial time.

The result fully generalizes Takayasu and Kunihiro's result [TK14d] in the sense that it completely covers their attack, i.e.,

$$\delta < \frac{1+\beta-\sqrt{-1+6\beta-3\beta^2}}{2} \quad \text{and} \quad \beta < \frac{9-\sqrt{21}}{12}$$

for $r = 1$ and $\alpha = 1$.

When the LSBs are exposed and $\beta \leq \frac{9-\sqrt{-3+12(r+1)\alpha}}{6(r+1)}$, our attack is better than

Huang et al. [HHX$^+$14] that works when $\delta < \frac{5-2\sqrt{-5+3(r+1)(\alpha+\beta)}}{3(r+1)}$. Figures 6.2 compare our results and Huang et al. for $r = 2$ and 3. Our attack is the better for small β, e.g., our attack works with less partial information.

Proof. Recall the key generation for Takagi's RSA with the exposed LSBs;

$$e(d_1 M + d_0) = 1 + \ell(p-1)(q-1)$$

with some integer $|\ell| \approx N^{\alpha+\beta-2/(r+1)}$. To recover the unknown MSBs of the secret exponent d_1, we use the following polynomials

$$\begin{aligned} f_{T.PKE.m1}(x, y_1, y_2) &= 1 - ed_0 + x(y_1+1)(y_2+1) \text{ and} \\ f_{T.PKE.m2}(x, y_1, y_2) &= 1 + x(y_1+1)(y_2+1) \end{aligned}$$

whose roots with appropriate moduli are

$$(x, y_1, y_2) = (\ell, -p, -q),$$

e.g., $f_{T.PKE.m1}(\ell, -p, -q) = 0 \pmod{eM}$ and $f_{T.PKE.m2}(\ell, -p, -q) = 0 \pmod{e}$. The absolute values are bounded above by

$$X := N^{\alpha+\beta-2/(r+1)}, Y_1 = Y_2 := 2N^{1/(r+1)}$$

within constant factors. Let $m = \omega(r)$ be an integer and define a function

$$l_r(k) = \max\left\{0, \frac{k-(r+1)(\beta-\delta)m}{1+(r+1)(\delta-2\beta)}\right\}.$$

To solve modular equations $f_{T.PKE.m1}(x, y_1, y_2) = 0 \pmod{eM}$ and $f_{T.PKE.m2}(x, y_1, y_2) = 0 \pmod{e}$ simultaneously, we use following shift-polynomials

$$\begin{aligned} g_{T.PKE.m1}(x, y_1, y_2) &= x^{i_X} y_1^{i_{Y_1}} y_2^{i_{Y_2}} f^u_{T.PKE.m1}(x, y_1, y_2)(eM)^{m-u}, \\ g_{T.PKE.m2}(x, y_1, y_2) &= y_1^{i_{Y_1}+k_1} y_2^{i_{Y_2}+k_2} f^{u-\lceil l_r(k_1+k_2)\rceil}_{T.PKE.m1}(x, y_1, y_2) \cdot \\ &\qquad f^{\lceil l_r(k_1+k_2)\rceil}_{T.PKE.m2}(x, y_1, y_2) e^{m-u} M^{m-(u-\lceil l_r(k_1+k_2)\rceil)}. \end{aligned}$$

To construct a lattice we use $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x1}, \mathcal{I}_{x2}$ and $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y1}, \mathcal{I}_{y2}$ where

$$\begin{aligned} \mathcal{I}_{x1} &\Leftrightarrow \ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0; i_{Y_2} = 0, \\ \mathcal{I}_{x2} &\Leftrightarrow \ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 1, \end{aligned}$$

$$\begin{aligned}
\mathcal{I}_{y1} \Leftrightarrow\ & u = 0,1,\ldots,m; i_{Y_1} = 0; i_{Y_2} = 0;\\
& k_1 = 1,2,\ldots,\lfloor (r+1)(\beta-\delta)m + (1+(r+1)(\delta-2\beta))u \rfloor; k_2 = 0,\\
\mathcal{I}_{y2} \Leftrightarrow\ & u = 0,1,\ldots,m; i_{Y_1} = 0,1,\ldots,r-1; i_{Y_2} = 1; k_1 = 0;\\
& k_2 = 1,2,\ldots,\lfloor (r+1)(\beta-\delta)m + (1+(r+1)(\delta-2\beta))u \rfloor.
\end{aligned}$$

All these shift-polynomials $g_{T.PKE.m1}$ and $g_{T.PKE.m2}$ modulo $(eM)^m$ have the root $(x, y_1, y_2) = (\ell, -p, -q)$ that is the same as $f_{T.PKE.m}$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{T.PKE.m1}(xX, y_1Y_1, y_2Y_2)$ and $g_{T.PKE.m2}(xX, y_1Y_1, y_2Y_2)$ as the bases.

As in the proof of Theorem 16, the shift-polynomials $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x1}$ and $\mathcal{I}_{x2}$ for $i_{Y_1} = 0,1,\ldots,r-1$ (resp. $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$ for $i_{Y_1} = 0,1,\ldots,r-1$) play the same role as x-shifts (resp. y-shifts) of Takayasu and Kunihiro. The shift-polynomials generate a triangular basis matrix using a linearization $z_1 = 1 + xy_1$ and $z_2 = 1 + xy_2$. Assume $1 + (r+1)(\delta - 2\beta) \geq 0$ and the diagonals of the basis matrix are

- $X^{u+i_X} Y_1^u e^{m-u}$ for $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x1}$,
- $X^{u+i_X} Y_1^{i_{Y_1}} Y_2^{u+1} e^{m-u}$ for $g_{T.PKE.m1}$ with indices in $\mathcal{I}_{x2}$,
- $X^{u-\lceil l_r(k_1)\rceil} Y_1^{u-\lceil l_r(k_1)\rceil+k_1} Z_1^{\lceil l_r(k_1)\rceil} e^{m-u} M^{m-(u-\lceil l_r(k_1)\rceil)}$ for $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y1}$,
- $X^{u-\lceil l_r(k_2)\rceil} Y_1^{i_{Y_1}} Y_2^{u-\lceil l_r(k_2)\rceil+k_1+1} Z_2^{\lceil l_r(k_2)\rceil} e^{m-u} M^{m-(u-\lceil l_r(k_2)\rceil)}$ for $g_{T.PKE.m2}$ with indices in $\mathcal{I}_{y2}$.

In $\mathcal{I}_{y1}$ and $\mathcal{I}_{y2}$, k_1 and k_2 are upper bounded by $\lfloor (r+1)(\beta-\delta)m + (1+(r+1)(\delta-2\beta))u \rfloor$. As Takayasu and Kunihiro, the definition follows from the fact that the shift-polynomials reduce norms of output vectors by the LLL algorithm.

As the proof of Theorem 16, all these values are larger by a factor of $(r+1)$ of Takayasu and Kunihiro's. We compute a dimension

$$n = |\mathcal{I}_1 \cup \mathcal{I}_2 \cup \mathcal{I}_3 \cup \mathcal{I}_4| = (r+1)\left(1 - \frac{r+1}{2}\delta\right) m^2 + o(m^2),$$

and a determinant of the lattice $\det(L(\boldsymbol{B})) = X^{s_X} Y^{s_Y} Z^{s_Z} e^{s_e} M^{s_M}$, where

$$\begin{aligned}
s_X + s_Z &= \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2})\\ \in \mathcal{I}_1 \cup \mathcal{I}_2}} (u + i_X) + \sum_{\substack{(u, i_{Y_1}, i_{Y_2}, k_1, k_2)\\ \in \mathcal{I}_3 \cup \mathcal{I}_4}} u\\
&= (r+1)\left(\frac{2}{3} - \frac{r+1}{6}(\beta+\delta)\right) m^3 + o(m^3),
\end{aligned}$$

$$\begin{aligned}
s_Y + s_Z = & \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in \mathcal{I}_1 \cup \mathcal{I}_2}} (u + i_{Y_1} + i_{Y_2}) \\
& + \sum_{\substack{(u, i_{Y_1}, i_{Y_2}, k_1, k_2) \\ \in \mathcal{I}_3 \cup \mathcal{I}_4}} (u + i_{Y_1} + i_{Y_2} + k_1 + k_2) \\
& = (r+1)\left(\frac{2}{3} - \frac{r+1}{3}(\delta + \beta) + \frac{(r+1)^2}{6}(\delta^2 - \beta\delta + \beta^2)\right) m^3 + o(m^3), \\
s_e = & \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in \mathcal{I}_1 \cup \mathcal{I}_2}} (m - u) + \sum_{\substack{(u, i_{Y_1}, i_{Y_2}, k_1, k_2) \\ \in \mathcal{I}_3 \cup \mathcal{I}_4}} (m - u) \\
& = (r+1)\left(\frac{1}{2} + \frac{r+1}{6}\beta - \frac{r+1}{3}\delta\right) m^3 + o(m^3), \\
s_M = & \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in \mathcal{I}_1 \cup \mathcal{I}_2}} (m - u) + \sum_{\substack{(u, i_{Y_1}, i_{Y_2}, k_1, k_2) \\ \in \mathcal{I}_3 \cup \mathcal{I}_4}} (m - (u - \lceil l(k_1 + k_2) \rceil)) \\
& = (r+1)\left(\frac{2}{3} - \frac{r+1}{6}(\beta + \delta)\right) m^3 + o(m^3).
\end{aligned}$$

LLL outputs short lattice vectors that satisfy Howgrave-Graham's Lemma when $(\det(L(\boldsymbol{B})))^{1/n} < (eM)^m$ that leads to

$$\begin{aligned}
& \left(\alpha + \beta - \frac{2}{r+1}\right)(r+1)\left(\frac{2}{3} - \frac{r+1}{6}(\beta + \delta)\right) \\
& + \frac{1}{r+1}(r+1)\left(\frac{2}{3} - \frac{r+1}{3}(\delta + \beta) + \frac{(r+1)^2}{6}(\delta^2 - \beta\delta + \beta^2)\right) \\
& + \alpha(r+1)\left(\frac{1}{2} + \frac{r+1}{6}\beta - \frac{r+1}{3}\delta\right) + (\beta - \delta)(r+1)\left(\frac{2}{3} - \frac{r+1}{6}(\beta + \delta)\right) \\
& < (\alpha + \beta - \delta)(r+1)\left(1 - \frac{r+1}{2}\delta\right).
\end{aligned}$$

Ignoring low order term of m, the inequality becomes

$$(r+1)^2\delta^2 - (r+1)(2 + (r+1)\beta)\delta + 4 - (r+1)\alpha - 2(r+1)\beta + (r+1)^2\beta^2 > 0.$$

Hence, we obtain the bound of Theorem 17

$$\delta < \frac{2+(r+1)\beta - \sqrt{-12+4(r+1)\alpha+12(r+1)\beta-3(r+1)^2\beta^2}}{2(r+1)}$$

as required. To satisfy the restriction $1+(r+1)(\delta-2\beta) \geq 0$, the condition $\beta \leq \frac{9-\sqrt{-3+12(r+1)\alpha}}{6(r+1)}$ should hold. □

6.4 Attacks on the Prime Power RSA by Solving Integer Equations

In this section, we analyze the security of the prime power RSA by solving integer equations. In Section 6.4.1, we propose a small secret exponent attack that fully generalizes the weaker Boneh-Durfee result [BD00]. In Section 6.4.2, we propose a partial key exposure attack that fully generalizes Ernst et al. [EJMdW05].

6.4.1 Small Secret Exponent Attack

In this section, we propose small secret exponent attacks on the prime power RSA that satisfy the following property.

Theorem 18. *Let $N = p^r q$ be a public modulus for $r \geq 2$ and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of the prime power RSA, respectively. If*

$$\begin{aligned}&0 < -r(r+1)^2\alpha + r(r+1)(1-\beta)(2(r+1)+3r\tau) - 1 - 3r\eta(1+r\eta) - \\ &r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3 \text{ where } \eta = \frac{r(r+1)(1-\beta)-1}{2r} \\ &\quad\text{and } \tau = \eta - \frac{r-\sqrt{-r+(r+1)^2(1-\beta)}}{r+1} \text{ for } \frac{3r^3+r^2+r-1}{4(r+1)} \leq \alpha, \text{ or} \\ &\beta < \frac{r+(\sqrt{r}-1)^2}{2r(r+1)} - \frac{\alpha}{2} \text{ for } \frac{r+(\sqrt{r}-1)^2}{r(r+1)} < \alpha \leq \frac{3r^3+r^2+r-1}{4(r+1)}\end{aligned}$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

The result extends Sarkar's attack [Sar16] for arbitrary α although they solved modular equations. The result for $r = 1$ does not cover the weaker Boneh-Durfee [BD00]. Moreover, the second condition becomes $\beta < 1/4$ for $r = 1$ and $\alpha = 1$ that is the same as Wiener's result [Wie90]. Indeed, Sarkar did not claim the connection with their attack and the weaker Boneh-Durfee at all. However, we think that the result fully generalizes the weaker Boneh-Durfee. Although we should use parameters (η and τ such that $\eta \geq \tau$ in the following proof) that do not exactly cover lattices for the weaker Boneh-Durfee to make use of the special structure of the prime power RSA, the construction is conceptually the same. Moreover, we will show in Section 6.4.2 that our construction covers Ernst et al. [EJMdW05] that is a partial key exposure extension of the weaker Boneh-Durfee. The proof is convenient to analyze partial key exposure attacks in Section 6.2.2.

Proof. Recall the key generation for the prime power RSA; $ed = 1 + \ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover the secret exponent d, we use the following polynomial

$$f_{PP.SSE.i}(x, y, z_1, z_2) = 1 + ex + yz_1^{r-1}(z_1 - 1)(z_2 - 1)$$

whose root over the integers is $(x, y, z_1, z_2) = (-d, \ell, p, q)$. The absolute values of the root (x, y, z_1) are bounded by $X := N^{\beta}, Y := N^{\alpha+\beta-1}, Z_1 := 2N^{1/(r+1)}$. For the notational convenience, we also use $Z_2 := N/Z_1^r$. We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{PP.SSE}(xX, yY, z_1Z_1, z_2Z_2)\|_\infty \geq |eX| \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1}Z_1^{r(m-1-a+t)}Z_2^{m-1}$ with some integers $m = \omega(r), t = \tau m$, and $a = \eta m$ where $\tau \geq 0$ and $\eta \geq \tau$. We define shift-polynomials $g_{PP.SSE.i}$ and $g'_{PP.SSE.i}$ as

$$\begin{aligned}
&g_{PP.SSE.i} : x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot f_{PP.SSE.i} \cdot X^{m-1-i_X} Y^{m-1-i_Y} Z_1^{r(m-1-a+t)-i_{Z_1}} Z_2^{m-1-i_{Z_2}} \\
&\quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S, \\
&g'_{PP.SSE.i} : x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M \backslash S,
\end{aligned}$$

for sets of monomials

$$S := \bigcup_{0 \leq j \leq rt} \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}+j} z_2^{i_{Z_2}} \;\middle|\; \begin{array}{c} x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \text{ is a monomial of} \\ \tilde{s} \cdot f_{PP.SSE.i}(x, y, z_1, z_2)^{m-1} \text{ where} \\ \tilde{s} = \left\{ z_2^a, z_1 z_2^a, z_1^2 z_2^a, \ldots, z_1^r z_2^a, z_1^{r-1} z_2^{a+1} \right\} \end{array} \right\},$$

$$M := \left\{ x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \;\middle|\; \begin{array}{c} \text{monomials of } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \cdot f_{PP.SSE.i}(x, y, z_1, z_2) \\ \text{where } x^{i'_X} y^{i'_Y} z_1^{i'_{Z_1}} z_2^{i'_{Z_2}} \in S \end{array} \right\},$$

with an integer $a = \eta m$ for $\eta \geq \tau$. By definition, it follows that

$$\begin{aligned}
x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in S \Leftrightarrow\; & i_X = 0, 1, \ldots, m - a + t - 1; \\
& i_Y = a - t, a - t + 1, \ldots, m - 1 - i_X;
\end{aligned}$$

$$\begin{aligned}
& i_{Z_1} = 0, 1, \ldots, r(i_Y - a + t); i_{Z_2} = 0, \text{ and} \\
& i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\
& i_{Z_1} = \max\{0, r - i_Y + r(i_{Z_2} - 1 - a)\}, \ldots, r-1; \\
& i_{Z_2} = a+1, a+2, \ldots, a + \lceil (i_Y + 1)/r \rceil, \quad \text{and} \\
& i_X = 0, 1, \ldots, m-1; i_Y = 0, 1, \ldots, m-1-i_X; \\
& i_{Z_1} = 0, 1, \ldots, r-1; i_{Z_2} = \max\{0, -i_Y + a - t\}, \ldots, a, \\
x^{i_X} y^{i_y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \in M \Leftrightarrow \; & i_X = 0, 1, \ldots, m - a + t; i_Y = a - t, a - t + 1, \ldots, m - i_X; \\
& i_{Z_1} = 0, 1, \ldots, r(i_Y - a + t); i_{Z_2} = 0, \text{ and} \\
& i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m - i_X; \\
& i_{Z_1} = \max\{0, r - i_Y + r(i_{Z_2} - 1 - a)\}, \ldots, r-1; \\
& i_{Z_2} = a+1, a+2, \ldots, a + \lceil (i_Y + 1)/r \rceil, \quad \text{and} \\
& i_X = 0, 1, \ldots, m; i_Y = 0, 1, \ldots, m - i_X; i_{Z_1} = 0, 1, \ldots, r-1; \\
& i_{Z_2} = \max\{0, -i_Y + a - t\}, \ldots, a.
\end{aligned}$$

All these shift-polynomials $g_{PP.SSE.i}(x, y, z_1, z_2)$ and $g'_{PP.SSE.i}(x, y, z_1, z_2)$ modulo R have the root $(x, y, z_1, z_2) = (-d, \ell, -p, -q)$ that are the same as $f_{PP.SSE.i}(x, y, z_1, z_2)$. All these shift-polynomials $g_{PP.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{PP.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ have a common divisor R. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{PP.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{PP.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ as the bases. The shift-polynomials generate a triangular basis matrix.

We compute

$$\begin{aligned}
|S| &= \left(\frac{r+1}{6} + \frac{r}{2}\tau\right) m^3 + o(m^3), \\
s_X &= \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \backslash S}} i_X = \left(\frac{r+1}{6} + \frac{r}{2}\tau\right) m^3 + o(m^3), \\
s_Y &= \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \backslash S}} i_Y = \left(\frac{r+1}{3} + \frac{r}{2}\tau\right) m^3 + o(m^3),
\end{aligned}$$

$$s_{Z_1} = \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \setminus S}} i_{Z_1} = \left(\frac{r^2(1-\eta+\tau)^3}{6}\right) m^3 + o(m^3),$$

$$s_{Z_2} = \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \setminus S}} i_{Z_2} = \left(\frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2 - \frac{r}{6}(\eta-\tau)^3\right) m^3 + o(m^3).$$

Ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short vectors that satisfy Howgrave-Graham's Lemma and contradict Hinek-Stinson's Lemma when $X^{s_X} Y^{s_Y} Z_1^{s_{Z_1}} Z_2^{s_{Z_2}} < W^{|S|}$ holds. The condition becomes

$$X^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3} Y^{\left(\frac{r+1}{3}+\frac{r}{2}\tau\right)m^3} Z_1^{\left(\frac{r^2(1-\eta+\tau)^3}{6}\right)m^3} Z_2^{\left(\frac{1}{6r}+\frac{1}{2}\eta+\frac{r}{2}\eta^2-\frac{r}{6}(\eta-\tau)^3\right)m^3} < W^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3} \tag{6.2}$$

Then, the inequality becomes

$$\begin{aligned} &\beta\left(\frac{r+1}{6}+\frac{r}{2}\tau\right) + (\alpha+\beta-1)\left(\frac{r+1}{3}+\frac{r}{2}\tau\right) \\ &+\frac{1}{r+1}\left(\frac{r^2(1-\eta+\tau)^3}{6} + \frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2 - \frac{r}{6}(\eta-\tau)^3\right) \\ <&(\alpha+\beta)\left(\frac{r+1}{6}+\frac{r}{2}\tau\right) \end{aligned}$$

that leads to

$$\begin{aligned} 0 <& -r(r+1)^2\alpha + r(r+1)(1-\beta)(2(r+1)+3r\tau) - 1 \\ &- 3r\eta(1+r\eta) - r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3. \end{aligned} \tag{6.3}$$

To maximize the right hand side of the inequality, we set parameters

$$\eta = \frac{r(r+1)(1-\beta)-1}{2r} \text{ and } \tau = \eta - \frac{r - \sqrt{-r+(r+1)^2(1-\beta)}}{r+1}$$

that result in the first condition of Theorem 18.

To satisfy the restriction $\tau \geq 0$, the condition $\beta \leq \frac{r^2-r-1+2\sqrt{r}}{r(r+1)}$ should hold. The condition results in $\alpha \geq \frac{3r^3+r^2+r-1}{4(r+1)}$. Other restrictions $\eta \geq \tau$ and $\eta \geq 0$ always hold.

In the other cases, e.g. $\alpha \leq \frac{3r^3+r^2+r-1}{4(r+1)}$, we fix the parameter $\tau = 0$. To maximize the right hand side of the inequality (6.3), we set the other parameter

$$\eta = 1 - \frac{1}{\sqrt{r}}$$

and the condition becomes

$$\beta < \frac{r + (\sqrt{r} - 1)^2}{2r(r+1)} - \frac{\alpha}{2}$$

as required. Since the prime power RSA satisfies $\alpha + \beta > 1$ by definition, $\alpha > \frac{r+(\sqrt{r}-1)^2}{r(r+1)}$ should hold. □

This attack is an extension of Sarkar's attack [Sar16] for arbitrary α. However, the extension offers an advantage of the approach although Sarkar did not claim. Lu et al. [LZPL15] claimed that their attack, which works when $\beta < \frac{r(r-1)}{(r+1)^2}$, is better than Sarkar's attack for $r \geq 5$. Indeed, the attack of Lu et al. is better than Theorem 18 for $\alpha = 1$ (that is equivalent to Sarkar's attack). However, our attack becomes better than the attack of Lu et al. for small α. Considering the restriction $\alpha + \beta > 1$, although the attack of Lu et al. works when $\alpha > \frac{3r+1}{(r+1)^2}$, our attack works when $\alpha > \frac{r+(\sqrt{r}-1)^2}{r(r+1)}$. Hence, our attack works for smaller α than Lu et al. In Section 6.5.1, we propose further (although slight) improvements and compare our results and Lu et al.

We note that the restriction $\eta \geq \tau$ comes from the fact that we can obtain better results than $\eta < \tau$ for small secret exponent attacks on the prime power RSA for $r \geq 2$. As we claimed, the algorithm construction fully generalizes the weaker Boneh-Durfee. That means the weaker Boneh-Durfee result can be obtained by setting $\eta < \tau$. The connection is hard to follow from Sarkar's proof [Sar16] and they did not claim it. As our previous proofs, the construction comes from our definition of sets of monomials S and M that play the same roles as those for Ernst et al. that is a partial key exposure extension of the weaker Boneh-Durfee. More concretely, each of our S for $\tilde{s} = \left\{z_2^a, z_1 z_2^a, z_1^2 z_2^a, \ldots, z_1^{r-1} z_2^a, z_1^{r-1} z_2^{a+1}\right\}$ play the same role as that for Ernst et al. and so do M. However, our n, s_X, s_Y, and s_Z do not become larger by a factor of $(r+1)$ of those of Ernst et al for the asymmetry of p and q for the prime power RSA key generation. So far, the asymmetry made it difficult to exploit the connection between the standard RSA and the prime power RSA, and to generalize attacks on the standard RSA to the prime power RSA.

6.4.2 Partial Key Exposure Attack.

In this section, we propose partial key exposure attacks on the prime power RSA that satisfy the following property.

Theorem 19. *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of prime power RSA, respectively. When $(\beta - \delta)\log N$*

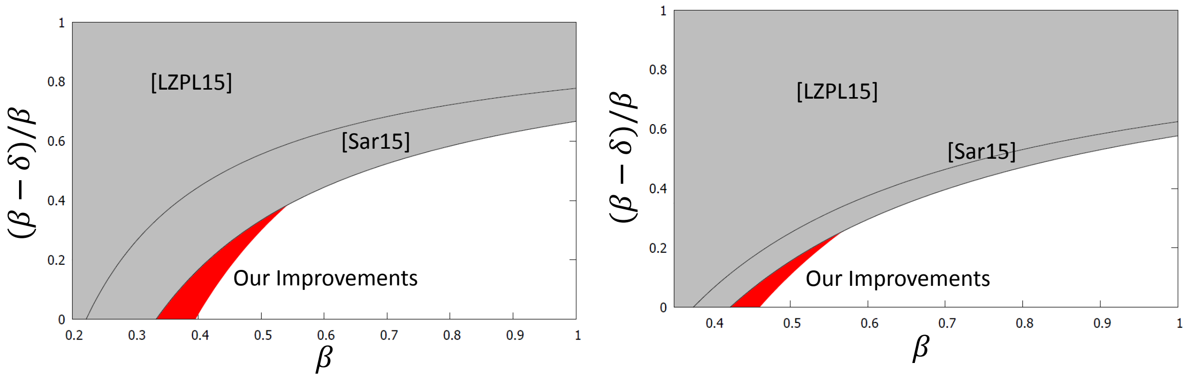


Fig. 6.3. Comparisons of partial key exposure attacks on the prime power RSA when the MSBs are exposed for $\alpha = 1$. We compare how much portions of d should be exposed for β between the attack of Lu et al. [LZPL15], Sarkar [Sar16], and our Theorem 19. The left figure is for $r = 2$ and the right figure is for $r = 3$.

bits of the most significant bits or the least significant bits are exposed, if

$$\begin{aligned} 0 < & -r(r+1)^2(\alpha+\beta) + r(r+1)(1-\delta)((r+1)+3r\tau) + r(r+1)^2 - 1 \\ & - 3r\eta(1+r\eta) - r^3(1-\eta+\tau)^3 + r^2(\eta-\tau)^3 \ \textit{where} \end{aligned}$$

$$\eta = \frac{r(r+1)(1-\delta)-1}{2r} \ \textit{and} \ \tau = \eta - \frac{r - \sqrt{-r+(r+1)^2(1-\delta)}}{r+1}$$

$$\textit{for} \ 1 < \alpha+\beta \le \frac{3r^3+r^2+5r-1}{4r(r+1)}, \textit{or}$$

$$\delta < 1 - \frac{r + \sqrt{12r^2(r+1)(\alpha+\beta) - r(9r^2+14r-3)}}{3r(r+1)} \ \textit{for} \ \frac{3r^3+r^2+5r-1}{4r(r+1)} \le \alpha+\beta$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

The result fully generalizes Ernst et al. [EJMdW05] in the sense that it completely covers their attack, i.e., $\beta < \left(5 - 2\sqrt{-5+6(\alpha+\beta)}\right)/6$ for $r = 1$. Moreover, we exploit the exact connection between the algorithm constructions of Theorem 19 and the Ernst et al.

When the MSBs are exposed, our attack is better than that of Sarkar when $\alpha+\beta$ is small and is better than that of Lu et al. when r is small. Figures 6.3 compare Theorem 19 and those of Lu et al. and Sarkar for $r = 2$ and 3. Our attack is the better for small β, e.g., our attack works with less partial information.

Proof. Recall the key generation for prime power RSA with the exposed bits (regardless of the MSBs or the LSBs); $e(\tilde{d}+(d-\tilde{d})) = 1+\ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover unknown parts $d - \tilde{d}$, we use the following polynomial

$$f_{PP.PKE.i}(x, y, z_1, z_2) = 1 - e\tilde{d} + eMx + yz_1^{r-1}(z_1 - 1)(z_2 - 1),$$

where $M = 1$ (resp. $M|2^{\lfloor(\beta-\delta)\log N\rfloor}$) with the exposed MSBs (resp. LSBs) whose roots over the integers are $(x, y, z_1, z_2) = (-(d - \tilde{d}), \ell, p, q)$. The absolute values are bounded by $X := N^{\delta}, Y := N^{\alpha+\beta-1}, Z_1 := 2N^{1/(r+1)}$. For the notational convenience, we also use $Z_2 := N/Z_1^r$.

These formulations and that for small secret exponent attacks in Section 6.4.1 are essentially the same when we use the Jochemsz-May strategy. That means the Newton polygons of polynomials $f_{PP.PKE.i}(x, y, z_1, z_2)$ and $f_{PP.PKE.i}(x, y, z_1, z_2)$ are the same, e.g., there are six monomials for variables $1, x, yz_1^{r-1}, yz_1^r, yz_1^{r-1}z_2$, and y. Hence, we use almost the same algorithm construction. We set an (possibly large) integer W such that $W < N^{\alpha+\beta}$ since $\|f_{PP.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)\|_\infty \geq \max\{|1 - e\tilde{d}|, |eMX|\} \approx N^{\alpha+\beta}$. Next, we set an integer $R := W(XY)^{m-1} \cdot Z_1^{r(m-1-a+t)}Z_2^{m-1}$ with some integers $m = \omega(r)$ and $t = \tau m$ where $\tau \geq 0$ such that $\gcd(R, 1-e\tilde{d}) = 1$. We compute $c = (1-e\tilde{d})^{-1} \pmod{R}$ and $f'_{PP.PKE.i}(x, y, z_1, z_2) := c \cdot f_{PP.PKE.i}(x, y, z_1, z_2) \pmod{R}$. We define shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ as

$$\begin{aligned}
g_{PP.PKE.i} :&x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \cdot f'_{PP.PKE.i} \cdot X^{m-1-i_X}Y^{m-1-i_Y}Z_1^{r(m-1-a+t)-i_{Z_1}}Z_2^{m-1-i_{Z_2}} \\
&\text{for } x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \in S, \\
g'_{PP.PKE.i} :&x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \cdot R \quad \text{for } x^{i_X}y^{i_Y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \in M\backslash S,
\end{aligned}$$

for sets of monomials S and M that are the same as in Section 6.4.1 where $f_{PP.SSE.i}$ is replaced by $f'_{PP.PKE.i}$. All these shift-polynomials $g_{PP.PKE.i}(x, y, z_1, z_2)$ and $g'_{PP.PKE.i}(x, y, z_1, z_2)$ modulo R have the root $(x, y, z_1, z_2) = (-(d - \tilde{d}), \ell, -p, -q)$ that are the same as $f_{PP.PKE.i}(x, y, z_1, z_2)$. All these shift-polynomials $g_{PP.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{PP.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)$ have a common divisor R. Hence, based on the Jochemsz-May strategy [JM06], LLL outputs short lattice vectors that satisfy Howgrave-Graham's Lemma and contradict Hinek-Stinson's Lemma when the inequality (6.2) holds. For partial key exposure attacks (regardless of the MSBs or the LSBs are exposed), the inequality becomes

$$\begin{aligned}
&\delta\left(\frac{r+1}{6} + \frac{r}{2}\tau\right) + (\alpha+\beta-1)\left(\frac{r+1}{3} + \frac{r}{2}\tau\right) \\
&+ \frac{1}{r+1}\left(\frac{r^2(1-\eta+\tau)^3}{6} + \frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2 - \frac{r}{6}(\eta-\tau)^3\right)
\end{aligned}$$

$$<(\alpha+\beta)\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)$$

that leads to

$$\begin{aligned}0 <& -r(r+1)^2(\alpha+\beta)+r(r+1)(1-\delta)((r+1)+3r\tau)+r(r+1)^2\\ &-1-3r\eta(1+r\eta)-r^3(1-\eta+\tau)^3+r^2(\eta-\tau)^3.\end{aligned}$$

To maximize the right hand side of the inequality, we set parameters

$$\eta = \frac{r(r+1)(1-\delta)-1}{2r} \text{ and } \tau = \eta - \frac{r-\sqrt{-r+(r+1)^2(1-\delta)}}{r+1}$$

that result in the first condition of Theorem 19. To satisfy the restriction $\eta \geq \tau$, the condition $\delta \geq \frac{1}{r+1}$ should hold. The condition results in $\alpha+\beta \leq \frac{3r^3+r^2+5r-1}{4r(r+1)}$. Notice that other restrictions $\tau \geq 0$ and $\eta \geq 0$ always hold.

For smaller $\alpha+\beta$, we use the other lattice construction that fully generalizes Ernst et al. However, the construction is essentially the same as previous one as we noted in the proof of Theorem 18. Indeed, we use the same shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ with the same sets of monomials S and M. The only difference is a restriction of parameters $\eta \leq \tau$. Hence, by definition, it follows that

$$\begin{aligned}x^{i_X}y^{i_y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \in S \Leftrightarrow\ & i_X = 0,1,\ldots,m-a+t-1;\\ & i_Y = a-t, a-t+1,\ldots,m-1-i_X;\\ & i_{Z_1} = 0,1,\ldots,r(i_Y-a+t); i_{Z_2} = 0, \text{ and}\\ & i_X = 0,1,\ldots,m-1; i_Y = 0,1,\ldots,m-1-i_X;\\ & i_{Z_1} = \max\{0, r-i_Y+r(i_{Z_2}-1-a)\},\ldots,r-1;\\ & i_{Z_2} = a+1,a+2,\ldots,a+\lceil(i_Y+1)/r\rceil, \text{ and}\\ & i_X = 0,1,\ldots,m-1; i_Y = 0,1,\ldots,m-1-i_X;\\ & i_{Z_1} = 0,1,\ldots,r-1; i_{Z_2} = \max\{0,-i_Y+a-t\},\ldots,a,\\ x^{i_X}y^{i_y}z_1^{i_{Z_1}}z_2^{i_{Z_2}} \in M \Leftrightarrow\ & i_X = 0,1,\ldots,m-a+t; i_Y = a-t,a-t+1,\ldots,m-i_X;\\ & i_{Z_1} = 0,1,\ldots,r(i_Y-a+t); i_{Z_2} = 0, \text{ and}\\ & i_X = 0,1,\ldots,m; i_Y = 0,1,\ldots,m-i_X;\\ & i_{Z_1} = \max\{0, r-i_Y+r(i_{Z_2}-1-a)\},\ldots,r-1;\\ & i_{Z_2} = a+1,a+2,\ldots,a+\lceil(i_Y+1)/r\rceil, \text{ and}\\ & i_X = 0,1,\ldots,m; i_Y = 0,1,\ldots,m-i_X; i_{Z_1} = 0,1,\ldots,r-1;\\ & i_{Z_2} = \max\{0,-i_Y+a-t\},\ldots,a.\end{aligned}$$

All these shift-polynomials $g_{PP.PKE.i}$ and $g'_{PP.PKE.i}$ modulo R have the roots $(x, y, z_1, z_2) = (-d, \ell, -p, -q)$ that are the same as $f_{PP.PKE.i}(x, y, z_1, z_2)$. We replace each occurrence of $z_1^r z_2$ by N and construct a lattice with coefficients of $g_{PP.PKE.i}(xX, yY, z_1Z_1, z_2Z_2)$ and $g'_{PP.SSE.i}(xX, yY, z_1Z_1, z_2Z_2)$ as the bases. The shift-polynomials generate a triangular basis matrix.

We compute

$$|S| = \left(\frac{r+1}{6} + \frac{r}{2}\tau\right) m^3 + o(m^3),$$

$$s_X = \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \backslash S}} i_X = \left(\frac{r+1}{6} + \frac{r}{2}\tau\right) m^3 + o(m^3),$$

$$s_Y = \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \backslash S}} i_Y = \left(\frac{r+1}{3} + \frac{r}{2}\tau\right) m^3 + o(m^3),$$

$$s_{Z_1} = \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \backslash S}} i_{Z_1} = \left(\frac{r^2(1-\eta+\tau)^3}{6} - \frac{r^2(\tau-\eta)^3}{6}\right) m^3 + o(m^3),$$

$$s_{Z_2} = \sum_{\substack{x^{i_X} y^{i_Y} z_1^{i_{Z_1}} z_2^{i_{Z_2}} \\ \in M \backslash S}} i_{Z_2} = \left(\frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2\right) m^3 + o(m^3).$$

Ignoring low order terms of m, based on the Jochemsz-May strategy [JM06], LLL outputs short vectors that satisfy Howgrave-Graham's Lemma and contradict Hinek-Stinson's Lemma when $X^{s_X} Y^{s_Y} Z_1^{s_{Z_1}} Z_2^{s_{Z_2}} < W^{|S|}$ holds. The condition becomes the inequality

$$X^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3} Y^{\left(\frac{r+1}{3}+\frac{r}{2}\tau\right)m^3} Z_1^{\left(\frac{r^2(1+\tau-\eta)^3}{6} - \frac{r^2(\tau-\eta)^3}{6}\right)m^3} Z_2^{\left(\frac{1}{6r}+\frac{1}{2}\eta+\frac{r}{2}\eta^2\right)m^3} < W^{\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)m^3}.$$

Then, the inequality becomes

$$\beta\left(\frac{r+1}{6} + \frac{r}{2}\tau\right) + (\alpha+\beta-1)\left(\frac{r+1}{3} + \frac{r}{2}\tau\right)$$

$$
\begin{aligned}
&+\frac{1}{r+1}\left(\frac{r^2(1+\tau-\eta)^3}{6}-\frac{r^2}{6}(\tau-\eta)^3+\frac{1}{6r}+\frac{1}{2}\eta+\frac{r}{2}\eta^2\right)\\
<&(\alpha+\beta)\left(\frac{r+1}{6}+\frac{r}{2}\tau\right)
\end{aligned}
$$

that leads to

$$
\begin{aligned}
0<&-(r+1)^2(\alpha+\beta)+(2(r+1)^2+3r(r+1)\tau)-\delta((r+1)^2+3r(r+1)\tau)\\
&-r^2(1+\tau-\eta)^3+r^2(\tau-\eta)^3-\frac{1}{r}-3\eta-3r\eta^2.
\end{aligned}
$$

To maximize the right hand side of the inequality, we set parameters

$$
\eta=\frac{r(r+1)(1-\delta)-1}{2r}\text{ and }\tau=\eta+\frac{(r+1)(1-\delta)-r}{2r}
$$

and the condition becomes

$$
\delta<1-\frac{r+\sqrt{12r^2(r+1)(\alpha+\beta)-r(9r^2+14r-3)}}{3r(r+1)}
$$

as required. To satisfy the restriction $\eta \le \tau$, the condition $\delta \le \frac{1}{r+1}$ should hold. The condition results in $\frac{3r^3+r^2+5r-1}{4r(r+1)} \le \alpha+\beta$. Notice that other restrictions $\tau \ge 0$ and $\eta \ge 0$ always hold. □

In Section 6.5.2, we propose an improved attack with the LSBs. However, it seems that our Theorem 19 with the exposed MSBs also has room for improvements. As opposed to Takagi's RSA, and as the standard RSA, we can compute the MSBs of ℓ since we know the MSBs of $p^{r-1}(p-1)(q-1)$. Indeed, the result of Sarkar makes use of the fact and generalize the other attack of Ernst et al. In addition, there exists better attacks by Takayasu and Kunihiro for small β. To generalize the attack to the prime power RSA remains as a future work.

6.5 Attacks on the Prime Power RSA by Solving Modular Equations

In this section, we analyze the security of prime power RSA by solving modular equations. In Section 6.5.1, we propose a small secret exponent attack that (almost) fully generalizes the stronger Boneh-Durfee result [BD00]. In Section 6.5.2, we propose a partial key exposure attack that (almost) fully generalizes Takayasu and Kunihiro's result [TK14d].

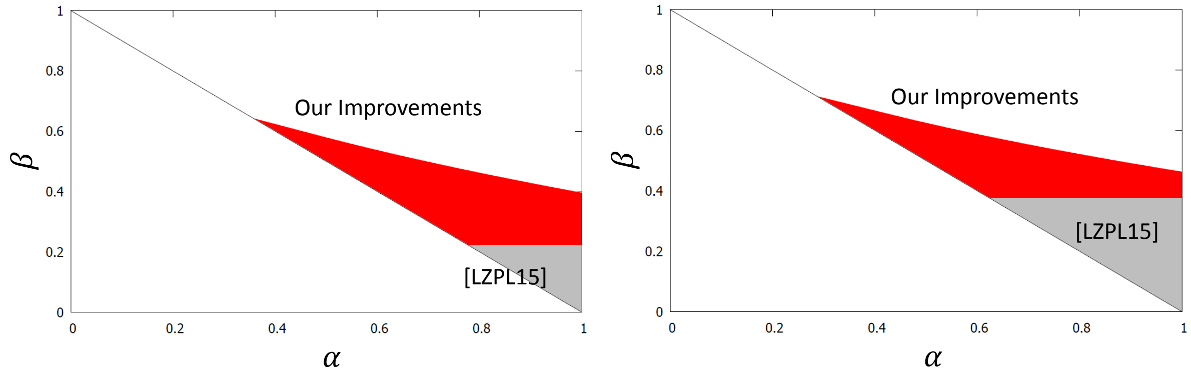


Fig. 6.4. Comparisons of small secret exponent attacks on the prime power RSA. We compare recoverable values β for α between the attack of Lu et al. [LZPL15] and our Theorem 20. The left figure is for $r = 2$ and the right figure is for $r = 3$.

6.5.1 Small Secret Exponent Attack

In this section, we propose small secret exponent attacks on the prime power RSA that satisfy the following property.

Theorem 20. *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of prime power RSA, respectively. If*

$$\beta < 1 - \frac{-r + \sqrt{4r(r+1) + 4r^2(3r+4)(r+1)^2\alpha}}{r(3r+4)(r+1)}$$

$$\text{for} \quad \alpha \geq \frac{9(r+1)^2}{(r+2)^2(3r+4)} - \frac{1}{r(r+1)(3r+4)}, \quad \text{or}$$

$$\beta < \frac{7r^2 + 17r + 9 - \sqrt{36r^4 + 204r^3 + 376r^2 + 292r + 84 + 4r(r+1)^2(r+3)\alpha}}{r(r+1)}$$

$$\text{for } \alpha > \frac{-4r^2 - 8r - 3 + 2\sqrt{(r+1)(4r^3 + 15r^2 + 10r + 3)}}{r(r+1)}$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

The result (almost) fully generalizes the stronger Boneh-Durfee [BD00] in the sense that it is better than the weaker Boneh-Durfee and weaker than the stronger Boneh-Durfee for $r = 1$, i.e., $\beta < (15 - 2\sqrt{30})/14 = 0.28896\cdots$. Since the results of Theorem 20 are better than those of Theorem 18, they are outperforming the Jochemsz-May.

Since Theorem 20 works when $\alpha > \frac{-4r^2-8r-3+2\sqrt{(r+1)(4r^3+15r^2+10r+3)}}{r(r+1)}$, it works for

Table 6.1. Comparisons of small secret exponent attacks on the prime power RSA. We compare recoverable values β for α between the attack of Lu et al. [LZPL15], our Theorem 18, and Theorem 20 for $r = 5$.

α	[LZPL15]	Theorem 18	Theorem 20
1	0.5555	0.5442	0.5495
0.9	0.5555	0.5670	0.5730
0.8	0.5555	0.5911	0.5979
0.7	0.5555	0.6167	0.6244
0.6	0.5555	0.6442	0.6528
0.5	0.5555	0.6741	0.6837
0.4	–	0.7073	0.7179
0.3	–	0.7452	0.7561

smaller α than Theorem 18. Indeed, Theorem 20 is (although slightly) always better than Theorem 18. Figures 6.4 compare Theorem 20 and Lu et al. for $r = 2$ and 3. Theorem 20 is the better for all α and the differences become larger for smaller α. Moreover, Tables 6.1 and 6.2 compare Lu et al., Theorem 18, and Theorem 20 for $r = 5$ and 6, respectively. When $\alpha = 1$, Lu et al. is the best. However, our attack becomes the better for smaller α.

Proof. Recall the key generation for the prime power RSA; $ed = 1+\ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover the secret exponent d, we use the following polynomial

$$f_{PP.SSE.m}(x, y_1, y_2) = 1 + xy_1^{r-1}(y_1 - 1)(y_2 - 1).$$

The polynomial modulo e has roots $(x, y_1, y_2) = (\ell, p, q)$. The absolute values are bounded by $X := N^{\alpha+\beta-1}, Y_1 = Y_2 := 2N^{1/(r+1)}$. Let $m = \omega(r)$ and $a = \eta m$ be integers. To solve a modular equation $f_{PP.SSE.m}(x, y_1, y_2) = 0 \pmod{e}$, we use shift-polynomials

$$g_{PP.SSE.m}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{a+i_{Y_2}} f^u_{PP.SSE.m}(x, y_1, y_2)e^{m-u}$$

with indices in

$$\mathcal{I}_{x1} \Leftrightarrow \ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m - u; i_{Y_1} = 0, 1, \ldots, r - 1; i_{Y_2} = 0,$$

Table 6.2. Comparisons of small secret exponent attacks on the prime power RSA. We compare recoverable values β for α between the attack of Lu et al. [LZPL15], our Theorem 18, and Theorem 20 for $r = 6$.

α	[LZPL15]	Theorem 18	Theorem 20
1	0.6122	0.5738	0.5798
0.9	0.6122	0.5950	0.6017
0.8	0.6122	0.6174	0.6248
0.7	0.6122	0.6412	0.6494
0.6	0.6122	0.6668	0.6759
0.5	0.6122	0.6946	0.7046
0.4	0.6122	0.7254	0.7364
0.3	–	0.7607	0.7724
0.2	–	0.8036	0.8106

$$\mathcal{I}_{x2} \Leftrightarrow \ u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = r-1; i_{Y_2} = 1,$$
$$\mathcal{I}_y \Leftrightarrow \ u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 1, 2, \ldots, \lfloor (1-(r+1)\beta)u \rfloor + ra; i_{Y_2} = 0.$$

All these shift-polynomials $g_{PP.SSE.m}$ modulo e^m have the roots $(x, y_1, y_2) = (\ell, -p, -q)$ that are the same as $f_{PP.sse.m}(x, y_1, y_2)$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{PP.SSE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases.

As in the proof of Theorem 18, the shift-polynomials $g_{PP.SSE.m}$ with indices in $\mathcal{I}_{x1}$ for $i_{Y_1} = 0, 1, \ldots, r-1$ and $\mathcal{I}_{x2}$ play the same role as x-shifts of the stronger Boneh-Durfee by a factor of $(r+1)$. Although $g_{PP.SSE.m}$ with indices in $\mathcal{I}_y$ plays the same role as y-shifts of the stronger Boneh-Durfee by a factor of r since i_{Y_1} is upper bounded by $\lfloor (1-(r+1)\beta)u \rfloor + ra$ that depends on u. However, there are no additional y-shifts which play the same role as the stronger Boneh-Durfee. Notice that all polynomials are multiplied by y_2^a and the operation plays the same role as the y-shifts of the weaker Boneh-Durfee. Hence, our Theorem 20 (almost) fully generalizes the stronger Boneh-Durfee and is always better than Theorem 18. We do not know how to fully generalize the stronger Boneh-Durfee and we think there may be room for improvements.

Assume that $\lfloor (1-(r+1)\beta)u \rfloor + ra \geq 0$, e.g., $\eta \geq ((r+1)\beta - 1)/r$, and the shift-polynomials generate triangular basis matrix with diagonals

- $X^{u+i_X} Y_1^{\max\{0, r(u-a)+i_{Y_1}\}} Y_2^{\max\{a-\lfloor u+i_{Y_1}/r \rfloor, 0\}} e^{m-u}$ for indices in $\mathcal{I}_{x1}$,
- $X^{u+i_X} Y_2^{a+\lceil (u+1)/r \rceil} e^{m-u}$ for indices in $\mathcal{I}_{x2}$,
- $X^u Y_1^{ru+i_{Y_1}} e^{m-u}$ for indices in $\mathcal{I}_y$.

In $\mathcal{I}_y$, i_{Y_1} is upper bounded by $\lfloor (1-(r+1)\beta)u \rfloor + ra$. The definition follows from the fact that the shift-polynomials reduce norms of outputs by the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than e^m.

We compute a dimension

$$n = |\mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y| = \left(\frac{1+(r+1)(1-\beta)}{2} + r\eta \right) m^2 + o(m^2),$$

and a determinant of the lattice $\det(L(\boldsymbol{B})) = X^{s_X} Y_1^{i_{Y_1}} Y_2^{i_{Y_2}} e^{s_e}$ where

$$s_X = \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in \mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y}} (u + i_X) = \left(\frac{1+(r+1)(1-\beta)}{3} + \frac{r}{2}\eta \right) m^3 + o(m^3),$$

$$\begin{aligned} s_{Y_1} &= \sum_{(u,i_X,i_{Y_1},i_{Y_2}) \in \mathcal{I}_{x1}} \max\{0, r(u-a)+i_{Y_1}\} + \sum_{(u,i_X,i_{Y_1},i_{Y_2}) \in \mathcal{I}_y} (ru + i_{Y_1}) \\ &= \frac{(r+1)^2(1-\beta)^2}{6} m^3 + o(m^3), \\ s_{Y_2} &= \sum_{(u,i_X,i_{Y_1},i_{Y_2}) \in \mathcal{I}_{x1}} \max\{a - \lfloor u + i_{Y_1}/r \rfloor, 0\} + \sum_{(u,i_X,i_{Y_1},i_{Y_2}) \in \mathcal{I}_{x2}} (a + \lceil (u+1)/r \rceil) \\ &= \left(\frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2 \right) m^3 + o(m^3), \end{aligned}$$

$$s_e = \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in \mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y}} (m-u) = \left(\frac{2r+3-(r+1)\beta}{6} + \frac{r}{2}\eta \right) m^3 + o(m^3).$$

Ignoring low order terms of m, LLL outputs short lattice vectors that satisfy Howgrave-Graham's Lemma when $(\det(L(\boldsymbol{B})))^{1/n} < (eM)^m$ that leads to

$$\begin{aligned} &(\alpha+\beta-1)\left(\frac{1+(r+1)(1-\beta)}{3} + \frac{r}{2}\eta \right) + \frac{1}{r+1}\left(\frac{(r+1)^2(1-\beta)^2}{6} + \frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2 \right) \\ &+\alpha \left(\frac{2r+3-(r+1)\beta}{6} + \frac{r}{2}\eta \right) < \alpha \left(\frac{1+(r+1)(1-\beta)}{2} + r\eta \right) \end{aligned}$$

that results in

$$0 < -r(r+1)^2\alpha - 1 - 3r\eta(1+r\eta) + r(r+1)(2+3r\eta)(1-\delta) + r(r+1)^2(1-\delta)^2.$$

To maximize the right hand side of the inequality, we set the parameter

$$\eta = \frac{r(r+1)(1-\beta)-1}{2r}$$

and the condition becomes

$$\beta < 1 - \frac{-r + \sqrt{4r(r+1) + 4r^2(3r+4)(r+1)^2\alpha}}{r(3r+4)(r+1)}$$

as required. To satisfy the restriction $\eta \geq ((r+1)\beta - 1)/r$, the condition $\beta < \frac{r(r+1)+1}{(r+2)(r+1)}$ should hold. The condition results in $\frac{9(r+1)^2}{(r+2)^2(3r+4)} - \frac{1}{r(r+1)(3r+4)} \leq \alpha$.

For smaller α, we propose an alternative lattice construction. We use the same shift-polynomials $g_{PP.SSE.m}(x, y_1, y_2)$ with indices in

$$\begin{aligned}
\mathcal{I}_{x1} \Leftrightarrow\ & u = 0,1,\ldots,m; i_X = 0,1,\ldots,m-u; i_{Y_1} = 0,1,\ldots,r-1; i_{Y_2} = 0,\\
\mathcal{I}_{x2} \Leftrightarrow\ & u = 0,1,\ldots,m; i_X = 0,1,\ldots,m-u; i_{Y_1} = r-1; i_{Y_2} = 1,\\
\mathcal{I}'_y \Leftrightarrow\ & u = 0,1,\ldots,m; i_X = 0; i_{Y_1} = 1,2,\ldots,\lfloor r(a-\eta u)\rfloor; i_{Y_2} = 0.
\end{aligned}$$

We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{PP.SSE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases. Assume $0 \leq \eta$ and the shift-polynomials generate a triangular basis matrix with the same diagonals as previous ones.

As previous cases, we should define $\mathcal{I}'_y$ such that the shift-polynomials reduce norms of outputs by the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than e^m. However, that is not the case and the definition is a suboptimal. Therefore, we think there may be room for improvements.

We compute the dimension of the lattice

$$n = |\mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y| = \left(\frac{r+1}{2} + \frac{r}{2}\eta\right) m^2 + o(m^2),$$

and its determinant $|\det B| = X^{s_X} Y_1^{i_{Y_1}} Y_2^{i_{Y_2}} e^{s_e}$ where

$$\begin{aligned}
s_X &= \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2})\\ \in \mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y}} (u + i_X) = \left(\frac{r+1}{3} + \frac{r}{6}\eta\right) m^3 + o(m^3),\\
s_{Y_1} &= \sum_{(u,i_X,i_{Y_1},i_{Y_2}) \in \mathcal{I}_{x1}} \max\{0, r(u-a) + i_{Y_1}\} + \sum_{(u,i_X,i_{Y_1},i_{Y_2}) \in \mathcal{I}_y} (ru + i_{Y_1})\\
&= \frac{r^2(1-\eta)^2}{6} m^3 + o(m^3),
\end{aligned}$$

$$\begin{aligned} s_{Y_2} &= \sum_{(u,i_X,i_{Y_1},i_{Y_2})\in\mathcal{I}_{x1}} \max\{a - \lfloor u + i_{Y_1}/r \rfloor, 0\} + \sum_{(u,i_X,i_{Y_1},i_{Y_2})\in\mathcal{I}_{x2}} (a + \lceil (u+1)/r \rceil) \\ &= \left(\frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2\right) m^3 + o(m^3), \\ s_e &= \sum_{\substack{(u,\, i_X,\, i_{Y_1},\, i_{Y_2}) \\ \in\, \mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y}} (m-u) = \left(\frac{r+1}{3} + \frac{r}{3}\eta\right) m^3 + o(m^3). \end{aligned}$$

Ignoring low order terms of m, LLL outputs short lattice vectors that satisfy Howgrave-Graham's Lemma when $(\det(L(\boldsymbol{B})))^{1/n} < (eM)^m$ that leads to

$$(\alpha+\beta-1)\left(\frac{r+1}{3} + \frac{r}{6}\eta\right) + \frac{1}{r+1}\left(\frac{r^2(1-\eta)^2}{6} + \frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2\right) + \alpha\left(\frac{r+1}{3} + \frac{r}{3}\eta\right) < \alpha\left(\frac{r+1}{2} + \frac{r}{2}\eta\right)$$

that results in

$$0 < -r(r+1)^2\alpha + r(1-\beta)\left(2(r+1)^2 + r(r+1)\eta\right) - r^3(1-\eta)^2 - 1 - 3r\eta(1+r\eta).$$

To maximize the right hand side of the inequality, we set the parameter

$$\eta = \frac{r(r+1)(1-\beta) + 2r^2 - 3}{2r^2 + 6r}$$

and the condition becomes

$$\beta < \frac{7r^2 + 17r + 9 - \sqrt{36r^4 + 204r^3 + 376r^2 + 292r + 84 + 4r(r+1)^2(r+3)\alpha}}{r(r+1)}$$

as required. To satisfy $\alpha + \beta > 1$, the condition $\alpha > \frac{-4r^2-8r-3+2\sqrt{(r+1)(4r^3+15r^2+10r+3)}}{r(r+1)}$ should hold. The restriction $\eta \geq 0$ always holds. □

6.5.2 Partial Key Exposure Attack

In this section, we propose small secret exponent attacks on the prime power RSA that satisfy the following property.

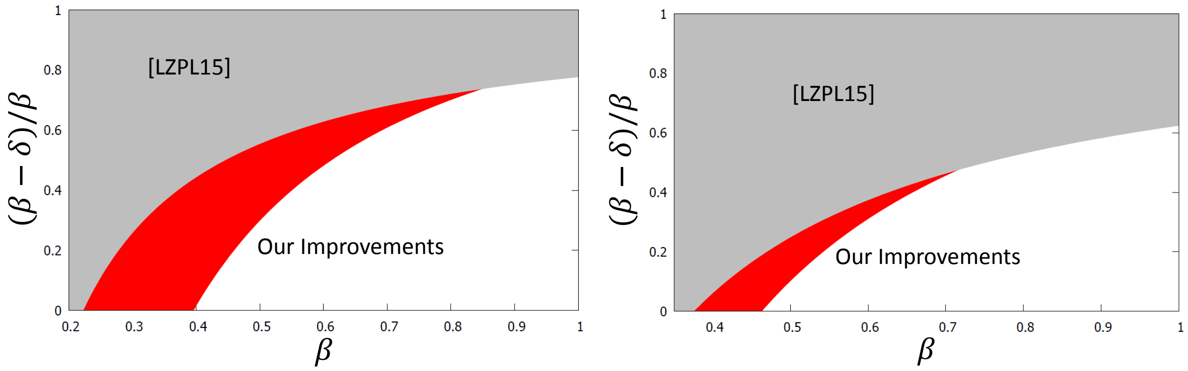


Fig. 6.5. Comparisons of partial key exposure attacks on the prime power RSA for $\alpha = 1$ when the least significant bits are exposed. We compare how much portions of d should be exposed for β between the attack of Lu et al. [LZPL15] and our Theorem 21. The left figure is for $r = 2$ and the right figure is for $r = 3$.

Theorem 21. *Let $N = p^r q$ be a public modulus and let $e \approx N^\alpha$ and $d \approx N^\beta$ be public exponent and secret exponent of prime power RSA, respectively. When $(\beta - \delta)\log N$ bits of the least significant bits are exposed, if*

$$\delta < 1 - \frac{r(2r+1) + 2\sqrt{r(r+1)(r(r+1)(3r+4)(\alpha+\beta) - 3r^3 - 6r^2 - 4r + 1)}}{r(r+1)(3r+4)}$$

$$\textit{for}\ \frac{30r^3 + 51r^2 + 25r - 4}{4r(r+1)(3r+4)} \le \alpha + \beta$$

holds, then prime power RSA modulus N can be factorized in polynomial time.

As Theorem 20, the result (only almost) fully generalizes Takayasu and Kunihiro's attack. However, the result is better than Theorem 19 with the exposed LSBs.

When the LSBs are exposed, our attack is better than that of Lu et al. when r is small. Figures 6.5 compare Theorem 21 and Lu et al. for $r = 2$ and 3. Our attack is the better for all β, e.g., our attack works with less partial information.

Proof. Recall the key generation for prime power RSA with the exposed LSBs; $e(d_1 M + d_0) = 1 + \ell p^{r-1}(p-1)(q-1)$ with some integer $|\ell| \approx N^{\alpha+\beta-1}$. To recover the unknown MSBs of the secret exponent d_1, we use the following polynomials

$$f_{PP.PKE.m}(x, y_1, y_2) = 1 - ed_0 + xy_1^{r-1}(y_1 - 1)(y_2 - 1)$$

whose root modulo e is $(x, y_1, y_2) = (\ell, p, q)$.

To solve a modular equation $f_{PP.PKE.m}(x, y_1, y_2) = 0 \pmod{e}$, we use the following shift-polynomials

$$g_{PP.PKE.m}(x, y_1, y_2) = x^{i_X} y_1^{i_{Y_1}} y_2^{a+i_{Y_2}} f^u_{PP.SSE.m}(x, y_1, y_2)(eM)^{m-u}$$

with indices in

$$\begin{aligned}
\mathcal{I}_{x1} \Leftrightarrow \;\; & u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = 0, 1, \ldots, r-1; i_{Y_2} = 0, \\
\mathcal{I}_{x2} \Leftrightarrow \;\; & u = 0, 1, \ldots, m; i_X = 0, 1, \ldots, m-u; i_{Y_1} = r-1; i_{Y_2} = 1, \\
\mathcal{I}_{y} \Leftrightarrow \;\; & u = 0, 1, \ldots, m; i_X = 0; i_{Y_1} = 1, 2, \ldots, \lfloor ((r+1)(1-\delta)-1)u \rfloor + ra; i_{Y_2} = 0.
\end{aligned}$$

All these shift-polynomials modulo $(eM)^m$ have roots $(x, y_1, y_2) = (\ell, p, q)$ that are the same as $g_{PP.PKE.m}$. We replace each occurrence of $y_1^r y_2$ by N and construct a lattice with coefficients of $g_{PP.PKE.m}(xX, y_1Y_1, y_2Y_2)$ as the bases. The shift-polynomials generate a triangular basis matrix with diagonals

- $X^{u+i_X} Y_1^{\max\{0, r(u-a)+i_{Y_1}\}} Y_2^{\max\{a-\lfloor u+i_{Y_1}/r \rfloor, 0\}} (eM)^{m-u}$ with indices in $\mathcal{I}_{x1}$,
- $X^{u+i_X} Y_2^{a+\lceil (u+1)/r \rceil} (eM)^{m-u}$ with indices in $\mathcal{I}_{x2}$,
- $X^u Y_1^{ru+i_{Y_1}} (eM)^{m-u}$ with indices in $\mathcal{I}_y$.

In $\mathcal{I}_y$, i_{Y_1} is upper bounded by $\lfloor ((r+1)(1-\delta)-1)u \rfloor + ra$. The definition follows from the fact that the shift-polynomials reduce norms of outputs by the LLL algorithm, e.g., the diagonals for the shift-polynomials are smaller than the modulus $(eM)^m$.

We compute the dimension

$$n = |\mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y| = \left(\frac{1 + (r+1)(1-\delta)}{2} + r\eta \right) m^2 + o(m^2),$$

and a determinant of the lattice $\det(L(\boldsymbol{B})) = X^{s_X} Y_1^{i_{Y_1}} Y_2^{i_{Y_2}} (eM)^{s_{eM}}$, where

$$\begin{aligned}
s_X &= \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in\, \mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y}} (u + i_X) = \left(\frac{1 + (r+1)(1-\delta)}{3} + \frac{r}{2}\eta \right) m^3 + o(m^3), \\
s_{Y_1} &= \sum_{(u, i_X, i_{Y_1}, i_{Y_2}) \in \mathcal{I}_{x1}} \max\{0, r(u-a) + i_{Y_1}\} + \sum_{(u, i_X, i_{Y_1}, i_{Y_2}) \in \mathcal{I}_y} (ru + i_{Y_1}) \\
&= \frac{(r+1)^2(1-\delta)^2}{6} m^3 + o(m^3), \\
s_{Y_2} &= \sum_{(u, i_X, i_{Y_1}, i_{Y_2}) \in \mathcal{I}_{x1}} \max\{a - \lfloor u + i_{Y_1}/r \rfloor, 0\} + \sum_{(u, i_X, i_{Y_1}, i_{Y_2}) \in \mathcal{I}_{x2}} (a + \lceil (u+1)/r \rceil)
\end{aligned}$$

$$= \left(\frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2\right) m^3 + o(m^3),$$

$$s_{eM} = \sum_{\substack{(u, i_X, i_{Y_1}, i_{Y_2}) \\ \in \mathcal{I}_{x1} \cup \mathcal{I}_{x2} \cup \mathcal{I}_y}} (m-u) = \left(\frac{2r+3-(r+1)\delta}{6} + \frac{r}{2}\eta\right) m^3 + o(m^3).$$

LLL outputs short lattice vectors that satisfy Howgrave-Graham's Lemma when $(\det(L(\boldsymbol{B})))^{1/n} < (eM)^m$ that leads to

$$(\alpha+\beta-1)\left(\frac{1+(r+1)(1-\delta)}{3} + \frac{r}{2}\eta\right) + \frac{1}{r+1}\left(\frac{(r+1)^2(1-\delta)^2}{6} + \frac{1}{6r} + \frac{1}{2}\eta + \frac{r}{2}\eta^2\right)$$
$$+(\alpha+\beta-\delta)\left(\frac{2r+3-(r+1)\delta}{6} + \frac{r}{2}\eta\right) < (\alpha+\beta-\delta)\left(\frac{1+(r+1)(1-\delta)}{2} + r\eta\right).$$

Ignoring low order terms of m, the inequality becomes

$$\begin{aligned} 0 < &- r(r+1)^2(\alpha+\beta-1) - 1 - 3r\eta(1+r\eta) \\ &- r(r+1)(r-1-3r\eta)(1-\delta) + r(r+1)^2(1-\delta)^2. \end{aligned}$$

To maximize the right hand side of the inequality, we set the parameter

$$\eta = \frac{r(r+1)(1-\delta)-1}{2r}$$

and the condition becomes

$$\delta < 1 - \frac{r(2r+1) + 2\sqrt{r(r+1)(r(r+1)(3r+4)(\alpha+\beta) - 3r^3 - 6r^2 - 4r + 1)}}{r(r+1)(3r+4)}$$

as required. To satisfy the restriction $\eta \geq 0$, $\delta \leq 1 - \frac{1}{r(r+1)}$ should hold. The condition results in $\frac{30r^3+51r^2+25r-4}{4r(r+1)(3r+4)} \leq \alpha + \beta$. □

6.6 Concluding Remarks

In this chapter, we study the security of RSA variants with moduli $N = p^r q$; Takagi's RSA and the prime power RSA. Analyses for the variants are difficult due to the complex moduli and key generations. Hence, existing results are hard to follow. To resolve the problems, we proposed the simple transformations that convert lattices for the original RSA to the lattices for the variants. Our technique enables us to understand the attacks on the variants. Furthermore, we obtained better results of small secret exponent attacks and partial key exposure attacks on the variants.

Chapter 7

Conclusion

7.1 Summary of the Results

In Chapter 3, we proposed the improved algorithm for solving the (δ, β)-SIP for $0 \leq \beta < 1/4$. We obtained the result from our better lattice construction that contains lattices for Boneh-Durfee's two attacks as special cases. Based on our proposed algorithm, we obtained the improved attack on the Multi-Prime RSA where its prime factors are similar sizes.

In Chapter 4, we proposed the improved partial key exposure attacks on CRT-RSA with the most/least significant bits of d_p or/and d_q. For the single partial key exposure situations, which utilized the partial bits of d_p or d_q, we apply Coppersmith's method for solving integer equations and obtained better attacks. If the most significant bits are exposed, our attack is the first result that works for larger public exponent e such that $N^{1/4} < e \leq N^{3/8}$. If the least significant bits are exposed, our attack works for $e < N^{3/8}$ as a previous attack, however, our attack works with less partial information. For the double partial key exposure situations, which utilized the partial bits of d_p and d_q, we obtained the first attack that works for $d_p, d_q \approx N^{1/2}$. Furthermore, the attack works for $e < N$. Furthermore, by solving the modular equations, we proposed the improved attack with the least significant bits of d_p or d_q. The attack is better than previous ones for all $e < N^{3/8}$.

In Chapter 5, we defined general partial key exposure scenarios that contain several existing problems as special cases. For the general scenarios, we proposed attacks that contain all the currently known best attacks as special cases. Then, we improved the attacks for two scenarios; partial key exposure attacks on RSA with the most significant bits of prime factors and partial key exposure attacks on the multi-prime RSA.

In Chapter 6, we proposed the generic transformation that convert the lattice for attacking the standard RSA to lattices for attacking Takagi's RSA and the prime power RSA whose public modulus has the form $N = p^r q$. Based on the transformation, we obtained better small secret exponent attacks and partial key exposure attacks with simple lattice constructions. Technically, we obtained the results by solving integer equations and constructing better lattices for solving modular equations.

7.2 Open Problems

Since the RSA cryptosystems are practically used, the security evaluation of RSA is one of the most important research topic in the cryptographic community. Therefore, further evaluations have to be developed. Some results proposed in this paper may contribute to revealing new RSA vulnerabilities that are still not known.

Technically, the most fascinating open problem is if there exist integer equations solving algorithms that are better than ones based on the Jochemsz-May strategy. In Chapters 4 and 6, the method is used to construct improved attacks on RSA, however, in some sense the constructions are simple since we follow the Jochemsz-May strategy. Hence, if improved algorithms can be constructed, they have to be impressive results. The other open problem is clarifying general strategies for optimal lattice constructions for Coppersmith's method. If such strategies can be summarized, the security evaluation of RSA will further be developed.

Bibliography

[AASW12] Yoshinori Aono, Manindra Agrawal, Takakazu Satoh, and Osamu Watanabe. On the optimality of lattices for the coppersmith technique. In Willy Susilo, Yi Mu, and Jennifer Seberry, editors, *Information Security and Privacy - 17th Australasian Conference, ACISP 2012*, volume 7372 of *Lecture Notes in Computer Science*, pages 376–389. Springer, 2012.

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer, 2010.

[ACLL15] Martin R. Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois. Implementing candidate graded encoding schemes from ideal lattices. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, volume 9453 of *Lecture Notes in Computer Science*, pages 752–775. Springer, 2015.

[ACM12] Michel Abdalla, Angelo De Caro, and Karina Mochetti. Lattice-based hierarchical inner product encryption. In Alejandro Hevia and Gregory Neven, editors, *Progress in Cryptology - LATINCRYPT 2012 - 2nd International Conference on Cryptology and Information Security in Latin America*, volume 7533 of *Lecture Notes in Computer Science*, pages 121–138. Springer, 2012.

[AD97] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In Frank Thomson Leighton and Peter W. Shor, editors, *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing*, pages 284–293. ACM, 1997.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling: Extended abstract. In Rocco A. Servedio and Ronitt Rubinfeld, editors, *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015*, pages 733–742. ACM, 2015.

[AFH$^+$16] Martin R. Albrecht, Pooya Farshim, Dennis Hofheinz, Enrique Larraia, and Kenneth G. Paterson. Multilinear maps from obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A*, volume 9562 of *Lecture Notes in Computer Science*, pages 446–473. Springer, 2016.

[AFL16] Daniel Apon, Xiong Fan, and Feng-Hao Liu. Fully-secure lattice-based IBE as compact as PKE. *IACR Cryptology ePrint Archive*, 2016:125, 2016.

[AFV11] Shweta Agrawal, David Mandell Freeman, and Vinod Vaikuntanathan. Functional encryption for inner product predicates from learning with errors. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security*, volume 7073 of *Lecture Notes in Computer Science*, pages 21–40. Springer, 2011.

[AHY15] Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. A framework for identity-based encryption with almost tight security. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, volume 9452 of *Lecture Notes in Computer Science*, pages 521–549. Springer, 2015.

[Ajt98] Miklós Ajtai. The shortest vector problem in L_2 is *NP*-hard for randomized reductions (extended abstract). In Jeffrey Scott Vitter, editor, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, pages 10–19. ACM, 1998.

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In Jeffrey Scott Vitter, Paul G. Spirakis, and Mihalis Yannakakis, editors, *Proceedings on 33rd Annual ACM Symposium on Theory of Computing*, pages 601–610. ACM, 2001.

[AM09] Divesh Aggarwal and Ueli M. Maurer. Breaking RSA generically is equivalent to factoring. In Antoine Joux, editor, *Advances in Cryptol-*

ogy - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, volume 5479 of *Lecture Notes in Computer Science*, pages 36–53. Springer, 2009.

[Aon09] Yoshinori Aono. A new lattice construction for partial key exposure attack for RSA. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 34–53. Springer, 2009.

[Aon13] Yoshinori Aono. Minkowski sum based lattice construction for multivariate simultaneous coppersmith's technique and applications to RSA. In Colin Boyd and Leonie Simpson, editors, *Information Security and Privacy - 18th Australasian Conference, ACISP 2013*, volume 7959 of *Lecture Notes in Computer Science*, pages 88–103. Springer, 2013.

[Att14] Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 8441 of *Lecture Notes in Computer Science*, pages 557–577. Springer, 2014.

[AWHT16] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9665 of *Lecture Notes in Computer Science*, pages 789–819. Springer, 2016.

[AY15] Nuttapong Attrapadung and Shota Yamada. Duality in ABE: converting attribute based encryption for dual predicate and dual policy via computational encodings. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 87–105. Springer, 2015.

[BB04] Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConfer-*

ence, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, 2004.

[BB11] Dan Boneh and Xavier Boyen. Efficient selective identity-based encryption without random oracles. *J. Cryptology*, 24(4):659–693, 2011.

[BBD$^+$13] Guillaume Barbu, Alberto Battistello, Guillaume Dabosville, Christophe Giraud, Guénaël Renault, Soline Renner, and Rina Zeitoun. Combined attack on CRT-RSA - why public verification must not be public? In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 198–215. Springer, 2013.

[BBN12] Hatem M. Bahig, Ashraf Bhery, and Dieaa I. Nassr. Cryptanalysis of multi-prime RSA with small prime difference. In Tat Wing Chim and Tsz Hon Yuen, editors, *Information and Communications Security - 14th International Conference, ICICS 2012*, volume 7618 of *Lecture Notes in Computer Science*, pages 33–44. Springer, 2012.

[BCC$^+$13] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren. Factoring RSA keys from certified smart cards: Coppersmith in the wild. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security*, volume 8270 of *Lecture Notes in Computer Science*, pages 341–360. Springer, 2013.

[BD00] Dan Boneh and Glenn Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Trans. Information Theory*, 46(4):1339–1349, 2000.

[BDF98] Dan Boneh, Glenn Durfee, and Yair Frankel. An attack on RSA given a small fraction of the private key bits. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security*, volume 1514 of *Lecture Notes in Computer Science*, pages 25–34. Springer, 1998.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016*, pages 10–24. SIAM, 2016.

[BDH99] Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham. Factoring $N = p^r q$ for large r. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference*, volume 1666 of *Lecture Notes in Computer Science*, pages 326–337. Springer, 1999.

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 1997.

[BF03] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[BGG$^+$14] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 8441 of *Lecture Notes in Computer Science*, pages 533–556. Springer, 2014.

[BGV14] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. *TOCT*, 6(3):13:1–13:36, 2014.

[BM01] Johannes Blömer and Alexander May. Low secret exponent RSA revisited. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 4–19. Springer, 2001.

[BM03] Johannes Blömer and Alexander May. New partial key exposure attacks on RSA. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference*, volume 2729 of *Lecture Notes in Computer Science*, pages 27–43. Springer, 2003.

[BM05] Johannes Blömer and Alexander May. A tool kit for finding small roots of bivariate polynomials over the integers. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual In-*

ternational Conference on the Theory and Applications of Cryptographic Techniques, volume 3494 of *Lecture Notes in Computer Science*, pages 251–267. Springer, 2005.

[BM06] Daniel Bleichenbacher and Alexander May. New attacks on RSA with small secret crt-exponents. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2006.

[BNNT11] Eric Brier, David Naccache, Phong Q. Nguyen, and Mehdi Tibouchi. Modulus fault attacks against RSA-CRT signatures. *J. Cryptographic Engineering*, 1(3):243–253, 2011.

[Bon99] Dan Boneh. Twenty years of attacks on the rsa cryptosystem. *NOTICES OF THE AMS*, 46:203–213, 1999.

[Bra12] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference*, volume 7417 of *Lecture Notes in Computer Science*, pages 868–886. Springer, 2012.

[BV98] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may not be equivalent to factoring. In Kaisa Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1403 of *Lecture Notes in Computer Science*, pages 59–71. Springer, 1998.

[BV14a] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM J. Comput.*, 43(2):831–871, 2014.

[BV14b] Zvika Brakerski and Vinod Vaikuntanathan. Lattice-based FHE as secure as PKE. In Moni Naor, editor, *Innovations in Theoretical Computer Science, ITCS'14*, pages 1–12. ACM, 2014.

[BW06] Xavier Boyen and Brent Waters. Anonymous hierarchical identity-based encryption (without random oracles). In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference*, volume 4117 of *Lecture Notes in Computer Science*, pages 290–307. Springer, 2006.

[BWZ14] Dan Boneh, Brent Waters, and Mark Zhandry. Low overhead broadcast encryption from multilinear maps. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference*, volume 8616 of *Lecture Notes in Computer Science*, pages 206–223. Springer, 2014.

[CCK$^+$13] Jung Hee Cheon, Jean-Sébastien Coron, Jinsu Kim, Moon Sung Lee, Tancrède Lepoint, Mehdi Tibouchi, and Aaram Yun. Batch fully homomorphic encryption over the integers. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7881 of *Lecture Notes in Computer Science*, pages 315–335. Springer, 2013.

[CFL$^+$16] Jung Hee Cheon, Pierre-Alain Fouque, Changmin Lee, Brice Minaud, and Hansol Ryu. Cryptanalysis of the new CLT multilinear map over the integers. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9665 of *Lecture Notes in Computer Science*, pages 509–536. Springer, 2016.

[CGH$^+$15] Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrède Lepoint, Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai, and Mehdi Tibouchi. Zeroizing without low-level zeroes: New MMAP attacks and their limitations. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference*, volume 9215 of *Lecture Notes in Computer Science*, pages 247–266. Springer, 2015.

[CGW15] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9057 of *Lecture Notes in Computer Science*, pages 595–624. Springer, 2015.

[CHHS16] Ted Chinburg, Brett Hemenway, Nadia Heninger, and Zachary Scherr. Cryptographic applications of capacity theory: On the optimality of coppersmith's method for univariate polynomials. *CoRR*, abs/1605.08065, 2016.

[CHKP12] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *J. Cryptology*, 25(4):601–639, 2012.

[CHL$^+$15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9056 of *Lecture Notes in Computer Science*, pages 3–12. Springer, 2015.

[CJK$^+$09] Jean-Sébastien Coron, Antoine Joux, Ilya Kizhvatov, David Naccache, and Pascal Paillier. Fault attacks on RSA signatures with partially unknown messages. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop*, volume 5747 of *Lecture Notes in Computer Science*, pages 444–456. Springer, 2009.

[CJL$^+$92] Matthijs J. Coster, Antoine Joux, Brian A. LaMacchia, Andrew M. Odlyzko, Claus-Peter Schnorr, and Jacques Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2:111–128, 1992.

[CKLQ02] Mathieu Ciet, Francois Koeune, Fabien Laguillaumie, and Jean-Jacques Quisquater. Short private exponent attacks on fast variants of rsa. *UCL Crypto Group Technical Report Series CG-2002/4, University Catholique de Louvain*, 2002.

[CLLT16] Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi. Cryptanalysis of GGH15 multilinear maps. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference*, volume 9815 of *Lecture Notes in Computer Science*, pages 607–628. Springer, 2016.

[CLT13] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8042 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2013.

[CLT14] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Scale-invariant fully homomorphic encryption over the integers. In Hugo Krawczyk, editor, *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography*, volume 8383 of *Lecture Notes in Computer Science*, pages 311–328.

Springer, 2014.

[CLT15] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference*, volume 9215 of *Lecture Notes in Computer Science*, pages 267–286. Springer, 2015.

[CM07] Jean-Sébastien Coron and Alexander May. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *J. Cryptology*, 20(1):39–50, 2007.

[CMNT11] Jean-Sébastien Coron, Avradip Mandal, David Naccache, and Mehdi Tibouchi. Fully homomorphic encryption over the integers with shorter public keys. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference*, volume 6841 of *Lecture Notes in Computer Science*, pages 487–504. Springer, 2011.

[CN11] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.

[CNT10] Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi. Fault attacks against emv signatures. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010*, volume 5985 of *Lecture Notes in Computer Science*, pages 208–220. Springer, 2010.

[CNT12] Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi. Public key compression and modulus switching for fully homomorphic encryption over the integers. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7237 of *Lecture Notes in Computer Science*, pages 446–464. Springer, 2012.

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer, 2001.

[Cop96a] Don Coppersmith. Finding a small root of a bivariate integer equation;

factoring with high bits known. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1070 of *Lecture Notes in Computer Science*, pages 178–189. Springer, 1996.

[Cop96b] Don Coppersmith. Finding a small root of a univariate modular equation. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques*, volume 1070 of *Lecture Notes in Computer Science*, pages 155–165. Springer, 1996.

[Cop97] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. Cryptology*, 10(4):233–260, 1997.

[Cop01] Don Coppersmith. Finding small solutions to small degree polynomials. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 20–31. Springer, 2001.

[Cor04] Jean-Sébastien Coron. Finding small roots of bivariate integer polynomial equations revisited. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3027 of *Lecture Notes in Computer Science*, pages 492–505. Springer, 2004.

[Cor07] Jean-Sébastien Coron. Finding small roots of bivariate integer polynomial equations: A direct approach. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference*, volume 4622 of *Lecture Notes in Computer Science*, pages 379–394. Springer, 2007.

[CS15] Jung Hee Cheon and Damien Stehlé. Fully homomophic encryption over the integers revisited. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9056 of *Lecture Notes in Computer Science*, pages 513–536. Springer, 2015.

[CW13] Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8043 of *Lecture Notes in Computer Science*, pages 435–460.

Springer, 2013.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[DN00] Glenn Durfee and Phong Q. Nguyen. Cryptanalysis of the RSA schemes with short secret exponent from asiacrypt '99. In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security*, volume 1976 of *Lecture Notes in Computer Science*, pages 14–29. Springer, 2000.

[dW02] Benne de Weger. Cryptanalysis of rsa with small prime difference. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):17–28, 2002.

[EJMdW05] Matthias Ernst, Ellen Jochemsz, Alexander May, and Benne de Weger. Partial key exposure attacks on RSA up to full size exponents. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 371–386. Springer, 2005.

[FGL+13] Pierre-Alain Fouque, Nicolas Guillermin, Delphine Leresteux, Mehdi Tibouchi, and Jean-Christophe Zapalowicz. Attacking RSA-CRT signatures with faults on montgomery multiplication. *J. Cryptographic Engineering*, 3(1):59–72, 2013.

[FHPS13] Eduarda S. V. Freire, Dennis Hofheinz, Kenneth G. Paterson, and Christoph Striecks. Programmable hash functions in the multilinear setting. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8042 of *Lecture Notes in Computer Science*, pages 513–530. Springer, 2013.

[FK15] Masaharu Fukase and Kenji Kashiwabara. An accelerated algorithm for solving SVP based on statistical analysis. *JIP*, 23(1):67–80, 2015.

[FMR10] Jean-Charles Faugère, Raphaël Marinier, and Guénaël Renault. Implicit factoring with shared most significant and middle bits. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 70–87. Springer, 2010.

[FOPS04] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA-OAEP is secure under the RSA assumption. *J. Cryptology*, 17(2):81–104, 2004.

[FP85] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, April 1985.

[Gam85] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Information Theory*, 31(4):469–472, 1985.

[Gar14] Sanjam Garg. Program obfuscation via multilinear maps. In *Security and Cryptography for Networks - 9th International Conference, SCN 2014*, pages 91–94, 2014.

[Gen06] Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464. Springer, 2006.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 169–178. ACM, 2009.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference*, volume 1294 of *Lecture Notes in Computer Science*, pages 112–131. Springer, 1997.

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7881 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2013.

[GGH$^+$13b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013*, pages 40–49. IEEE

Computer Society, 2013.

[GGH^{+}13c] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8043 of *Lecture Notes in Computer Science*, pages 479–499. Springer, 2013.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015*, volume 9015 of *Lecture Notes in Computer Science*, pages 498–527. Springer, 2015.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 467–476. ACM, 2013.

[GHKN06] Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q. Nguyen. Rankin's constant and blockwise lattice reduction. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference*, volume 4117 of *Lecture Notes in Computer Science*, pages 112–130. Springer, 2006.

[GHM05] Steven D. Galbraith, Chris Heneghan, and James F. McKee. Tunable balancing of RSA. In Colin Boyd and Juan Manuel González Nieto, editors, *Information Security and Privacy, 10th Australasian Conference, ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, pages 280–292. Springer, 2005.

[GHS12a] Craig Gentry, Shai Halevi, and Nigel P. Smart. Fully homomorphic encryption with polylog overhead. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7237 of *Lecture Notes in Computer Science*, pages 465–482. Springer, 2012.

[GHS12b] Craig Gentry, Shai Halevi, and Nigel P. Smart. Homomorphic evaluation of the AES circuit. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference*, volume 7417 of *Lecture Notes in Computer Science*, pages 850–867. Springer, 2012.

[GLSW15] Craig Gentry, Allison Bishop Lewko, Amit Sahai, and Brent Waters. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. In Venkatesan Guruswami, editor, *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015*, pages 151–170. IEEE Computer Society, 2015.

[GMM$^+$16] Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry. Secure obfuscation in a weak multilinear map model. In Martin Hirt and Adam D. Smith, editors, *Theory of Cryptography - 14th International Conference, TCC 2016-B*, volume 9986 of *Lecture Notes in Computer Science*, pages 241–268, 2016.

[GN08] Nicolas Gama and Phong Q. Nguyen. Finding short lattice vectors within mordell's inequality. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 207–216. ACM, 2008.

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 6110 of *Lecture Notes in Computer Science*, pages 257–278. Springer, 2010.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 197–206. ACM, 2008.

[GST14] Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference*, volume 8616 of *Lecture Notes in Computer Science*, pages 444–461. Springer, 2014.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2013.

[GV15] Sergey Gorbunov and Dhinakaran Vinayagamurthy. Riding on asymmetry: Efficient ABE for branching programs. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, volume 9452 of *Lecture Notes in Computer Science*, pages 550–574. Springer, 2015.

[GVW15a] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. *J. ACM*, 62(6):45, 2015.

[GVW15b] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Predicate encryption for circuits from LWE. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference*, volume 9216 of *Lecture Notes in Computer Science*, pages 503–523. Springer, 2015.

[HDWH12] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In Tadayoshi Kohno, editor, *Proceedings of the 21th USENIX Security Symposium*, pages 205–220. USENIX Association, 2012.

[Hel85] Bettina Helfrich. Algorithms to construct minkowski reduced an hermite reduced lattice bases. *Theor. Comput. Sci.*, 41:125–139, 1985.

[HHX$^+$14] Zhangjie Huang, Lei Hu, Jun Xu, Liqiang Peng, and Yonghong Xie. Partial key exposure attacks on takagi's variant of RSA. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *Applied Cryptography and Network Security - 12th International Conference, ACNS 2014*, volume 8479 of *Lecture Notes in Computer Science*, pages 134–150. Springer, 2014.

[Hin08] M. Jason Hinek. On the security of multi-prime RSA. *J. Mathematical Cryptology*, 2(2):117–147, 2008.

[HJ16] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH map. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9665 of *Lecture Notes in Computer Science*, pages 537–565. Springer, 2016.

[HM08] Mathias Herrmann and Alexander May. Solving linear equations modulo divisors: On factoring given any bits. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security*, volume

5350 of *Lecture Notes in Computer Science*, pages 406–424. Springer, 2008.

[HM09] Mathias Herrmann and Alexander May. Attacking power generators using unravelled linearization: When do we output too much? In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security*, volume 5912 of *Lecture Notes in Computer Science*, pages 487–504. Springer, 2009.

[HM10] Mathias Herrmann and Alexander May. Maximizing small root bounds by linearization and applications to small secret exponent RSA. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 53–69. Springer, 2010.

[HMM10] Wilko Henecka, Alexander May, and Alexander Meurer. Correcting errors in RSA private keys. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference*, volume 6223 of *Lecture Notes in Computer Science*, pages 351–369. Springer, 2010.

[How97] Nick Howgrave-Graham. Finding small roots of univariate modular equations revisited. In Michael Darnell, editor, *Cryptography and Coding, 6th IMA International Conference*, volume 1355 of *Lecture Notes in Computer Science*, pages 131–142. Springer, 1997.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference*, volume 6841 of *Lecture Notes in Computer Science*, pages 447–464. Springer, 2011.

[HS06] M. Jason Hinek and Douglas R. Stinson. An inequality about factors of multivariate polynomials. *CACR Technical Report CACR 2006-15, Centre for Applied Cryptographic Research, University of Waterloo*, 2006.

[HS07] Guillaume Hanrot and Damien Stehlé. Improved analysis of kannan's shortest lattice vector algorithm. In Alfred Menezes, editor, *Advances* *in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference*, volume 4622 of *Lecture Notes in Computer Science*, pages 170–186. Springer, 2007.

[HS09] Nadia Heninger and Hovav Shacham. Reconstructing RSA private keys from random key bits. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference*, volume 5677 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2009.

[HSH$^+$09] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM*, 52(5):91–98, 2009.

[HSW13] Susan Hohenberger, Amit Sahai, and Brent Waters. Full domain hash from (leveled) multilinear maps and identity-based aggregate signatures. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8042 of *Lecture Notes in Computer Science*, pages 494–512. Springer, 2013.

[IKK08] Kouichi Itoh, Noboru Kunihiro, and Kaoru Kurosawa. Small secret key attack on a variant of RSA (due to takagi). In Tal Malkin, editor, *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008*, volume 4964 of *Lecture Notes in Computer Science*, pages 387–406. Springer, 2008.

[IKK09] Kouichi Itoh, Noboru Kunihiro, and Kaoru Kurosawa. Small secret key attack on a takagi's variant of RSA. *IEICE Transactions*, 92-A(1):33–41, 2009.

[JL12] Marc Joye and Tancrède Lepoint. Partial key exposure on RSA with private exponents larger than N. In Mark Dermot Ryan, Ben Smyth, and Guilin Wang, editors, *Information Security Practice and Experience - 8th International Conference, ISPEC 2012*, volume 7232 of *Lecture Notes in Computer Science*, pages 369–380. Springer, 2012.

[JM06] Ellen Jochemsz and Alexander May. A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security*, volume 4284 of *Lecture Notes in Computer Science*, pages 267–282. Springer, 2006.

[JM07] Ellen Jochemsz and Alexander May. A polynomial time attack on RSA with private crt-exponents smaller than $N^{0.073}$. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference*, volume 4622 of *Lecture Notes in Computer Science*, pages 395–411. Springer, 2007.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In Wieb Bosma, editor, *Algorithmic Number Theory, 4th International Symposium, ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–394. Springer, 2000.

[JR13] Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security*, volume 8269 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2013.

[Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In David S. Johnson, Ronald Fagin, Michael L. Fredman, David Harel, Richard M. Karp, Nancy A. Lynch, Christos H. Papadimitriou, Ronald L. Rivest, Walter L. Ruzzo, and Joel I. Seiferas, editors, *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, pages 193–206. ACM, 1983.

[KH14] Noboru Kunihiro and Junya Honda. RSA meets DPA: recovering RSA secret keys from noisy analog data. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop*, volume 8731 of *Lecture Notes in Computer Science*, pages 261–278. Springer, 2014.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

[Koc96] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1996.

[KOS10] Eike Kiltz, Adam O'Neill, and Adam D. Smith. Instantiability of RSA-OAEP under chosen-plaintext attack. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference*, volume 6223 of *Lecture Notes in Computer Science*, pages 295–313. Springer, 2010.

[KS01] Henrik Koy and Claus-Peter Schnorr. Segment LLL-reduction of lattice bases. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 67–80. Springer, 2001.

[KSI13] Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu. Recovering RSA secret keys from noisy key bits with erasures and errors. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 180–197. Springer, 2013.

[KSI14] Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu. A unified framework for small secret exponent attack on RSA. *IEICE Transactions*, 97-A(6):1285–1295, 2014.

[KSW13] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *J. Cryptology*, 26(2):191–224, 2013.

[Kun11] Noboru Kunihiro. Solving generalized small inverse problems. *IEICE Transactions*, 94-A(6):1274–1284, 2011.

[Kun12] Noboru Kunihiro. On optimal bounds of small inverse problems and approximate GCD problems with higher degree. In Dieter Gollmann and Felix C. Freiling, editors, *Information Security - 15th International Conference, ISC 2012*, volume 7483 of *Lecture Notes in Computer Science*, pages 55–69. Springer, 2012.

[Kun15] Noboru Kunihiro. An improved attack for recovering noisy RSA secret keys and its countermeasure. In Man Ho Au and Atsuko Miyaji, editors, *Provable Security - 9th International Conference, ProvSec 2015*, volume 9451 of *Lecture Notes in Computer Science*, pages 61–81. Springer, 2015.

[KY16] Shuichi Katsumata and Shota Yamada. Partitioning via non-linear polynomial functions: More compact ibes from ideal lattices and bilinear maps. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the*

Theory and Application of Cryptology and Information Security, volume 10032 of *Lecture Notes in Computer Science*, pages 682–712, 2016.

[Laa15] Thijs Laarhoven. Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference*, volume 9215 of *Lecture Notes in Computer Science*, pages 3–22. Springer, 2015.

[Len87] Hendrik W. Lenstra. Factoring integers with elliptic curves. *The Annals of Mathematics*, 126(3):649–673, November 1987.

[Lew12] Allison B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7237 of *Lecture Notes in Computer Science*, pages 318–335. Springer, 2012.

[LHA$^+$12] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Public keys. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference*, volume 7417 of *Lecture Notes in Computer Science*, pages 626–642. Springer, 2012.

[LJMP90] Arjen K. Lenstra, Hendrik W. Lenstra Jr., Mark S. Manasse, and John M. Pollard. The number field sieve. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 564–572, 1990.

[LLL82] A.K. Lenstra, H.W.jun. Lenstra, and Lászlo Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[LO85] J. C. Lagarias and Andrew M. Odlyzko. Solving low-density subset sum problems. *J. ACM*, 32(1):229–246, 1985.

[LOS$^+$10] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2010.

[LPZ$^+$15] Yao Lu, Liqiang Peng, Rui Zhang, Lei Hu, and Dongdai Lin. Towards optimal bounds for implicit factorization problem. In Orr Dunkelman and Liam Keliher, editors, *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference*, volume 9566 of *Lecture Notes in Computer Science*, pages 462–476. Springer, 2015.

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 8441 of *Lecture Notes in Computer Science*, pages 239–256. Springer, 2014.

[LW10] Allison B. Lewko and Brent Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In Daniele Micciancio, editor, *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010*, volume 5978 of *Lecture Notes in Computer Science*, pages 455–479. Springer, 2010.

[LW11] Allison B. Lewko and Brent Waters. Unbounded HIBE and attribute-based encryption. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 6632 of *Lecture Notes in Computer Science*, pages 547–567. Springer, 2011.

[LZL14] Yao Lu, Rui Zhang, and Dongdai Lin. New partial key exposure attacks on CRT-RSA with large public exponents. In Ioana Boureanu, Philippe Owesarski, and Serge Vaudenay, editors, *Applied Cryptography and Network Security - 12th International Conference, ACNS 2014*, volume 8479 of *Lecture Notes in Computer Science*, pages 151–162. Springer, 2014.

[LZPL15] Yao Lu, Rui Zhang, Liqiang Peng, and Dongdai Lin. Solving linear equations modulo unknown divisors: Revisited. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security*, volume 9452 of *Lecture Notes in Computer Science*, pages 189–213. Springer, 2015.

[Mau95] Ueli M. Maurer. On the oracle complexity of factoring integers. *Computational Complexity*, 5(3/4):237–247, 1995.

[May02] Alexander May. Cryptanalysis of unbalanced RSA with small crt-exponent. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference*, volume 2442 of *Lecture Notes in Computer Science*, pages 242–256. Springer, 2002.

[May03] Alexander May. *New RSA vulnerabilities using lattice reduction methods.* PhD thesis, University of Paderborn, 2003.

[May04a] Alexander May. Computing the RSA secret key is deterministic polynomial time equivalent to factoring. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference*, volume 3152 of *Lecture Notes in Computer Science*, pages 213–219. Springer, 2004.

[May04b] Alexander May. Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 218–230. Springer, 2004.

[May10] Alexander May. Using LLL-reduction for solving RSA and factorization problems. In Nguyen and Vallée [NV10], pages 315–348.

[MH78] Ralph C. Merkle and Martin E. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Information Theory*, 24(5):525–530, 1978.

[Mil75] Gary L. Miller. Riemann's hypothesis and tests for primality. In William C. Rounds, Nancy Martin, Jack W. Carlyle, and Michael A. Harrison, editors, *Proceedings of the 7th Annual ACM Symposium on Theory of Computing*, pages 234–239. ACM, 1975.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer, 2012.

[MR09] Alexander May and Maike Ritzenhofen. Implicit factoring: On polynomial time factoring given only an implicit hint. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 2009.

[MSZ16] Eric Miles, Amit Sahai, and Mark Zhandry. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13. In Matthew Robshaw and Jonathan Katz, editors, *Advances* *in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference*, volume 9815 of *Lecture Notes in Computer Science*, pages 629–658. Springer, 2016.

[MV10a] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. In Leonard J. Schulman, editor, *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010*, pages 351–358. ACM, 2010.

[MV10b] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In Moses Charikar, editor, *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2010*, pages 1468–1480. SIAM, 2010.

[MW96] Ueli M. Maurer and Stefan Wolf. Diffie-hellman oracles. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference*, volume 1109 of *Lecture Notes in Computer Science*, pages 268–282. Springer, 1996.

[MW15] Daniele Micciancio and Michael Walter. Fast lattice point enumeration with minimal overhead. In Piotr Indyk, editor, *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015*, pages 276–294. SIAM, 2015.

[MW16] Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9665 of *Lecture Notes in Computer Science*, pages 820–849. Springer, 2016.

[Ngu10] Phong Q. Nguyen. Hermite's constant and lattice algorithms. In Nguyen and Vallée [NV10], pages 19–69.

[NIK15] Koji Nuida, Naoto Itakura, and Kaoru Kurosawa. A simple and improved algorithm for integer factorization with implicit hints. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015*, volume 9048 of *Lecture Notes in Computer Science*, pages 258–269. Springer, 2015.

[NK15] Koji Nuida and Kaoru Kurosawa. (Batch) Fully homomorphic encryption over integers for non-binary message spaces. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT*

2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, volume 9056 of *Lecture Notes in Computer Science*, pages 537–555. Springer, 2015.

[NS01] Phong Q. Nguyen and Jacques Stern. The two faces of lattices in cryptology. In Joseph H. Silverman, editor, *Cryptography and Lattices, International Conference, CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 146–180. Springer, 2001.

[NS05] Phong Q. Nguyen and Damien Stehlé. Floating-point LLL revisited. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 215–233. Springer, 2005.

[NS09] Phong Q. Nguyen and Damien Stehlé. An LLL algorithm with quadratic complexity. *SIAM J. Comput.*, 39(3):874–903, 2009.

[NS16] Arnold Neumaier and Damien Stehlé. Faster LLL-type reduction of lattice bases. In Sergei A. Abramov, Eugene V. Zima, and Xiao-Shan Gao, editors, *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016*, pages 373–380. ACM, 2016.

[NSV11] Andrew Novocin, Damien Stehlé, and Gilles Villard. An LLL-reduction algorithm with quasi-linear time complexity: extended abstract. In Lance Fortnow and Salil P. Vadhan, editors, *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011*, pages 403–412. ACM, 2011.

[Nui14] Koji Nuida. A simple framework for noise-free construction of fully homomorphic encryption from a special class of non-commutative groups. *IACR Cryptology ePrint Archive*, 2014:97, 2014.

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *J. Mathematical Cryptology*, 2(2):181–207, 2008.

[NV10] Phong Q. Nguyen and Brigitte Vallée, editors. *The LLL Algorithm - Survey and Applications.* Information Security and Cryptography. Springer, 2010.

[OT09] Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the*

Theory and Application of Cryptology and Information Security, volume 5912 of *Lecture Notes in Computer Science*, pages 214–231. Springer, 2009.

[OT10] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference*, volume 6223 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2010.

[OT12a] Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 7237 of *Lecture Notes in Computer Science*, pages 591–608. Springer, 2012.

[OT12b] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure unbounded inner-product and attribute-based encryption. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security*, volume 7658 of *Lecture Notes in Computer Science*, pages 349–366. Springer, 2012.

[OT15] Tatsuaki Okamoto and Katsuyuki Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. *Des. Codes Cryptography*, 77(2-3):725–771, 2015.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 333–342. ACM, 2009.

[PHL$^+$15] Liqiang Peng, Lei Hu, Yao Lu, Santanu Sarkar, Jun Xu, and Zhangjie Huang. Cryptanalysis of variants of RSA with multiple small secret exponents. In Alex Biryukov and Vipul Goyal, editors, *Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India*, volume 9462 of *Lecture Notes in Computer Science*, pages 105–123. Springer, 2015.

[Pom84] Carl Pomerance. The quadratic sieve factoring algorithm. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology: Proceedings of EUROCRYPT 84, A Workshop on the The-*

ory and Application of of Cryptographic Techniques, volume 209 of *Lecture Notes in Computer Science*, pages 169–182. Springer, 1984.

[PPS12] Kenneth G. Paterson, Antigoni Polychroniadou, and Dale L. Sibborn. A coding-theoretic approach to recovering noisy RSA keys. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security*, volume 7658 of *Lecture Notes in Computer Science*, pages 386–403. Springer, 2012.

[QC82] J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for rsa public-key cryptosystem. *Electronics Letters*, 18:905–907(2), October 1982.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[RS85] Ronald L. Rivest and Adi Shamir. Efficient factoring based on partial information. In Franz Pichler, editor, *Advances in Cryptology - EUROCRYPT '85, Workshop on the Theory and Application of of Cryptographic Techniques*, volume 219 of *Lecture Notes in Computer Science*, pages 31–34. Springer, 1985.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[Sar14] Santanu Sarkar. Small secret exponent attack on RSA variant with modulus $N = p^r q$. *Des. Codes Cryptography*, 73(2):383–392, 2014.

[Sar16] Santanu Sarkar. Revisiting prime power RSA. *Discrete Applied Mathematics*, 203:127–133, 2016.

[Sch87] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53:201–224, 1987.

[Sch88] Claus-Peter Schnorr. A more efficient algorithm for lattice basis reduction. *J. Algorithms*, 9(1):47–62, 1988.

[Sch03] Claus-Peter Schnorr. Lattice reduction by random sampling and birthday methods. In Helmut Alt and Michel Habib, editors, *STACS 2003, 20th Annual Symposium on Theoretical Aspects of Computer Science*, volume 2607 of *Lecture Notes in Computer Science*, pages 145–156. Springer, 2003.

[Sch06] Claus-Peter Schnorr. Fast LLL-type lattice reduction. *Inf. Comput.*, 204(1):1–25, 2006.

[SE94] Claus-Peter Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

[Sha82] Adi Shamir. A polynomial time algorithm for breaking the basic merkle-hellman cryptosystem. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of CRYPTO '82*, pages 279–288. Plenum Press, New York, 1982.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, 1997.

[Sho02] Victor Shoup. OAEP reconsidered. *J. Cryptology*, 15(4):223–249, 2002.

[SM08] Santanu Sarkar and Subhamoy Maitra. Improved partial key exposure attacks on RSA by guessing a few bits of one of the prime factors. In Pil Joong Lee and Jung Hee Cheon, editors, *Information Security and Cryptology - ICISC 2008*, volume 5461 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 2008.

[SM09a] Santanu Sarkar and Subhamoy Maitra. Further results on implicit factoring in polynomial time. *Adv. in Math. of Comm.*, 3(2):205–217, 2009.

[SM09b] Santanu Sarkar and Subhamoy Maitra. Partial key exposure attack on CRT-RSA. In Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud, editors, *Applied Cryptography and Network Security, 7th International Conference, ACNS 2009*, volume 5536 of *Lecture Notes in Computer Science*, pages 473–484, 2009.

[SM10] Santanu Sarkar and Subhamoy Maitra. Some applications of lattice based root finding techniques. *Adv. in Math. of Comm.*, 4(4):519–531, 2010.

[SM11] Santanu Sarkar and Subhamoy Maitra. Approximate integer common divisor problem relates to implicit factorization. *IEEE Trans. Information Theory*, 57(6):4002–4013, 2011.

[SMS08] Santanu Sarkar, Subhamoy Maitra, and Sumanta Sarkar. RSA cryptanalysis with increased bounds on the secret exponent using less lattice dimension. *IACR Cryptology ePrint Archive*, 2008:315, 2008.

[SMSV14] Saruchi, Ivan Morel, Damien Stehlé, and Gilles Villard. LLL reducing with the most significant bits. In Katsusuke Nabeshima, Kosaku Nagasaka, Franz Winkler, and Ágnes Szántó, editors, *International Symposium on Symbolic and Algebraic Computation, ISSAC '14*, pages 367–374. ACM, 2014.

[SSM10] Santanu Sarkar, Sourav Sengupta, and Subhamoy Maitra. Partial key exposure attack on RSA - improvements for limited lattice dimensions. In Guang Gong and Kishan Chand Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India*, volume 6498 of *Lecture Notes in Computer Science*, pages 2–16. Springer, 2010.

[SWS$^+$08] Hung-Min Sun, Mu-En Wu, Ron Steinfeld, Jian Guo, and Huaxiong Wang. Cryptanalysis of short exponent RSA with primes sharing least significant bits. In Matthew K. Franklin, Lucas Chi Kwong Hui, and Duncan S. Wong, editors, *Cryptology and Network Security, 7th International Conference, CANS 2008*, volume 5339 of *Lecture Notes in Computer Science*, pages 49–63. Springer, 2008.

[Tak98] Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo p^kq. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference*, volume 1462 of *Lecture Notes in Computer Science*, pages 318–326. Springer, 1998.

[Tak14] Katsuyuki Takashima. Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. In Michel Abdalla and Roberto De Prisco, editors, *Security and Cryptography for Networks - 9th International Conference, SCN 2014*, volume 8642 of *Lecture Notes in Computer Science*, pages 298–317. Springer, 2014.

[TK14a] Atsushi Takayasu and Noboru Kunihiro. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. *IEICE Transactions*, 97-A(6):1259–1272, 2014.

[TK14b] Atsushi Takayasu and Noboru Kunihiro. Cryptanalysis of RSA with multiple small secret exponents. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014*, volume 8544 of *Lecture Notes in Computer Science*, pages 176–191. Springer, 2014.

[TK14c] Atsushi Takayasu and Noboru Kunihiro. General bounds for small inverse problems and its applications to multi-prime RSA. In Jooyoung

Lee and Jongsung Kim, editors, *Information Security and Cryptology - ICISC 2014 - 17th International Conference*, volume 8949 of *Lecture Notes in Computer Science*, pages 3–17. Springer, 2014.

[TK14d] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA: achieving the boneh-durfee bound. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference*, volume 8781 of *Lecture Notes in Computer Science*, pages 345–362. Springer, 2014.

[TK15] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on CRT-RSA: better cryptanalysis to full size encryption exponents. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *Applied Cryptography and Network Security - 13th International Conference, ACNS 2015*, volume 9092 of *Lecture Notes in Computer Science*, pages 518–537. Springer, 2015.

[TK16a] Atsushi Takayasu and Noboru Kunihiro. How to generalize RSA cryptanalyses. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography*, volume 9615 of *Lecture Notes in Computer Science*, pages 67–97. Springer, 2016.

[TK16b] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on CRT-RSA: general improvement for the exposed least significant bits. In Matt Bishop and Anderson C. A. Nascimento, editors, *Information Security - 19th International Conference, ISC 2016*, volume 9866 of *Lecture Notes in Computer Science*, pages 35–47. Springer, 2016.

[TK16c] Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA with multiple exponent pairs. In Joseph K. Liu and Ron Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016*, volume 9723 of *Lecture Notes in Computer Science*, pages 243–257. Springer, 2016.

[TK17a] Atsushi Takayasu and Noboru Kunihiro. General bounds for small inverse problems and its applications to multi-prime RSA. *IEICE Transactions*, 100-A(1):50–61, 2017.

[TK17b] Atsushi Takayasu and Noboru Kunihiro. A tool kit for partial key exposure attacks on RSA. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017, The Cryptographers' Track at the RSA Conference*

2017, volume 10159 of *Lecture Notes in Computer Science*, pages 58–73. Springer, 2017.

[vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer, 2010.

[Wal15] Michael Walter. Lattice point enumeration on block reduced bases. In Anja Lehmann and Stefan Wolf, editors, *Information Theoretic Security - 8th International Conference, ICITS 2015*, volume 9063 of *Lecture Notes in Computer Science*, pages 269–282. Springer, 2015.

[Wat05] Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005.

[Wat09] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer, 2009.

[Wie90] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Information Theory*, 36(3):553–558, 1990.

[Xag13] Keita Xagawa. Improved (hierarchical) inner-product encryption from lattices. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 235–252. Springer, 2013.

[YAHK11] Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro. Generic constructions for chosen-ciphertext secure attribute based encryption. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 71–89. Springer, 2011.

[YAHK14] Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro. A framework and compact constructions for non-monotonic attribute-based encryption. In Hugo Krawczyk, editor, *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography*, volume 8383 of *Lecture Notes in Computer Science*, pages 275–292. Springer, 2014.

[Yam16] Shota Yamada. Adaptively secure identity-based encryption from lattices with asymptotically shorter public parameters. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 9666 of *Lecture Notes in Computer Science*, pages 32–62. Springer, 2016.

[YYHK14] Takashi Yamakawa, Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Self-bilinear map on unknown order groups from indistinguishability obfuscation and its applications. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference*, volume 8617 of *Lecture Notes in Computer Science*, pages 90–107. Springer, 2014.

[ZCZ16] Jiang Zhang, Yu Chen, and Zhenfeng Zhang. Programmable hash functions from lattices: Short signatures and ibes with small key sizes. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference*, volume 9816 of *Lecture Notes in Computer Science*, pages 303–332. Springer, 2016.

[ZT13] Hui Zhang and Tsuyoshi Takagi. Attacks on multi-prime RSA with small prime difference. In Colin Boyd and Leonie Simpson, editors, *Information Security and Privacy - 18th Australasian Conference, ACISP 2013*, volume 7959 of *Lecture Notes in Computer Science*, pages 41–56. Springer, 2013.

[ZT14] Hui Zhang and Tsuyoshi Takagi. Improved attacks on multi-prime RSA with small prime difference. *IEICE Transactions*, 97-A(7):1533–1541, 2014.

業績リスト

国際論文誌（査読付き）

1. Atsushi Takayasu and Noboru Kunihiro. General bounds for small inverse problems and its applications to multi-prime RSA. *IEICE Transactions*, 100-A(1):50–61, 2017.
2. Atsushi Takayasu and Noboru Kunihiro. Better lattice constructions for solving multivariate linear equations modulo unknown divisors. *IEICE Transactions*, 97-A(6):1259–1272, 2014.

国際会議（査読付き）

1. Atsushi Takayasu, Yao Lu, and Liqiang Peng. Small CRT-exponent RSA revisited. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, *Lecture Notes in Computer Science*. Springer, 2017. （発表決定済み）
2. Atsushi Takayasu and Noboru Kunihiro. A tool kit for partial key exposure attacks on RSA. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017, The Cryptographers' Track at the RSA Conference 2017*, volume 10519 of *Lecture Notes in Computer Science*, pages 58–73. Springer, 2017.
3. Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA with multiple exponent pairs. In Joseph K. Liu and Ron Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016*, volume 9723 of *Lecture Notes in Computer Science*, pages 243–257. Springer, 2016.
4. Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on CRT-RSA: general improvement for the exposed least significant bits. In Matt Bishop and Anderson C. A. Nascimento, editors, *Information Security - 19th International Conference, ISC 2016*, volume 9866 of *Lecture Notes in Computer*

Science, pages 35–47. Springer, 2016.

5. Atsushi Takayasu and Noboru Kunihiro. Small secret exponent attacks on RSA with unbalanced prime factors. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2016*. IEEE, 2016.
6. Atsushi Takayasu and Noboru Kunihiro. How to generalize RSA cryptanalyses. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography*, volume 9615 of *Lecture Notes in Computer Science*, pages 67–97. Springer, 2016.
7. Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on CRT-RSA: better cryptanalysis to full size encryption exponents. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *Applied Cryptography and Network Security - 13th International Conference, ACNS 2015*, volume 9092 of *Lecture Notes in Computer Science*, pages 518–537. Springer, 2015.
8. Katsuyuki Takashima and Atsushi Takayasu. Tighter security for efficient lattice cryptography via the Rényi divergence of optimized orders. In Man Ho Au and Atsuko Miyaji, editors, *Provable Security - 9th International Conference, ProvSec 2015*, volume 9451 of *Lecture Notes in Computer Science*, pages 412–431. Springer, 2015.
9. Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA: achieving the boneh-durfee bound. In Antoine Joux and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference*, volume 8781 of *Lecture Notes in Computer Science*, pages 345–362. Springer, 2014.
10. Atsushi Takayasu and Noboru Kunihiro. General bounds for small inverse problems and its applications to multi-prime RSA. In Jooyoung Lee and Jongsung Kim, editors, *Information Security and Cryptology - ICISC 2014 - 17th International Conference*, volume 8949 of *Lecture Notes in Computer Science*, pages 3–17. Springer, 2014.
11. Atsushi Takayasu and Noboru Kunihiro. Cryptanalysis of RSA with multiple small secret exponents. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014*, volume 8544 of *Lecture Notes in Computer Science*, pages 176–191. Springer, 2014.

国際会議（招待講演）

1. Parameter selections for approximate GCD problems. In *The 11th International Workshop on Security, IWSEC 2016*, 2016.
2. Improved algorithms for partial key exposure attacks on RSA. In *The 9th International Workshop on Security, IWSEC 2014*, 2014.

国際会議ポスター発表（査読なし）

1. Atsushi Takayasu and Noboru Kunihiro. Faster LLL reduction to break the security of fully homomorphic encryption and multilinear map over the integers. In *The 10th International Workshop on Security, IWSEC 2015*, 2015.
2. Atsushi Takayasu and Noboru Kunihiro. Partial key exposure attacks on RSA when most significant bits of d known. In *9th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2014*. ACM, 2014.

受賞

1. 情報セキュリティ研究奨励賞, 情報セキュリティ研究会, 2017年1月.
   受賞論文: ブロック簡約基底に対する最短ベクトル探索の最悪時計算量評価
2. CSS学生論文賞, 情報処理学会 コンピュータセキュリティシンポジウム CSS 2016, 2016年10月.
   受賞論文: CRT-RSAを攻撃する格子の新たな構成法
3. Best Student Paper Award, ACISP 2016, 2016年7月.
   受賞論文: Partial key exposure attacks on RSA with multiple exponent pairs
4. 辻井重男セキュリティ論文優秀賞, 日本セキュリティ・マネジメント学会, 2016年3月.
   受賞論文: How to generalize RSA cryptanalyses
5. CSS優秀論文賞, 情報処理学会 コンピュータセキュリティシンポジウム CSS 2015, 2015年10月.
   受賞論文: 近似GCD問題のパラメータ解析
6. CSS学生論文賞, 情報処理学会 コンピュータセキュリティシンポジウム CSS 2015, 2015年10月.
   受賞論文: 低ノイズLPN問題におけるBKWアルゴリズムの解析

7. SCIS 論文賞, 電子情報通信学会 暗号と情報セキュリティシンポジウム SCIS 2014, 2015 年 1 月.
   受賞論文: RSA 暗号の部分鍵導出攻撃の改良

国内研究会・シンポジウム口頭発表（査読なし）

1. 高安敦, 國廣昇. Slide 簡約基底に対する最短ベクトル探索の最悪時計算量評価. **暗号と情報セキュリティシンポジウム**, *SCIS 2017*, 2B4-4, 2017.
2. 高安敦, 盧堯, 彭力強. CRT-RSA を攻撃する格子の新たな構成法. **コンピュータセキュリティシンポジウム**, *CSS 2016*, 3C4-1, 2016.
3. 高安敦, 國廣昇. ブロック簡約基底に対する最短ベクトル探索の最悪時計算量評価. **情報セキュリティ研究会**, *ISEC*, 2016.
4. 高安敦, 高島克幸. Rényi ダイバージェンスの次数を最適化した格子暗号のタイトな帰着. **暗号と情報セキュリティシンポジウム**, *SCIS 2016*, 1D1-2, 2016.
5. 宮崎結香, 谷垣友喜, 高安敦, 國廣昇. 使用可能領域を有効活用した Sieve アルゴリズムの高速化. **暗号と情報セキュリティシンポジウム**, *SCIS 2016*, 2D1-2, 2016.
6. 上中谷健, 國廣昇, 高安敦. 最小サンプルで LWE 問題を解くための BKW アルゴリズム. **暗号と情報セキュリティシンポジウム**, *SCIS 2016*, 2D4-5, 2016.
7. 高安敦, 國廣昇. 近似 GCD 問題のパラメータ解析. **コンピュータセキュリティシンポジウム**, *CSS 2015*, 3C2-3, 2015.
8. 上中谷健, 國廣昇, 高安敦. 低ノイズ LPN 問題における BKW アルゴリズムの解析. **コンピュータセキュリティシンポジウム**, *CSS 2015*, 3C2-4, 2015.
9. 高安敦, 高島克幸. 改善された安全性証明を持つ GGHLite パラメータ. **暗号と情報セキュリティシンポジウム**, *SCIS 2015*, 2D4-2, 2015.
10. 町野義貴, 青野良範, 高安敦, 國廣昇. 整数計画問題による binary-LWE 問題の求解アルゴリズム. **暗号と情報セキュリティシンポジウム**, *SCIS 2015*, 3D1-1, 2015.
11. 高安敦, 國廣昇. 複数の復号指数を持つ RSA 暗号の安全性解析. **情報セキュリティ研究会**, *ISEC*, 2014.