平成 30 年度

修士論文

鍵の部分情報の漏洩に対する RSA 暗号の安全性解析

47176112　鈴木海地

指導教員　國廣昇

2019 年 3 月 6 日

東京大学大学院新領域創成科学研究科

複雑理工学専攻

概要

これまで RSA 暗号および一般化 RSA 暗号に対して，復号指数 d の上位ビットもしくは下位ビットが得られたときの多項式時間攻撃アルゴリズムが，Coppersmith の手法を用いて活発に研究されてきた．この攻撃設定において，RSA 暗号に対しては Ernst らの攻撃 (Eurocrypt'05) と Takayasu と Kunihiro の攻撃 (SAC'14) が，一般化 RSA 暗号に対しては Zheng らの攻撃（Africacrypt'18）が現在知られている最も良い攻撃である．特に，Takayasu と Kunihiro の攻撃は，d が小さいほど有効であり，上位ビットが得られる場合は $d < N^{0.5625}$ のとき，下位ビットが得られる場合は $d < N^{0.368}$ のときに，Ernst らの攻撃よりもより少ない部分情報で攻撃できる．ただし，Ernst らは，上位ビットと下位ビットが同時に得られた設定においても，攻撃を提案している．Zheng らは，Ernst らの RSA 暗号に対する攻撃を一般化 RSA 暗号に適用した攻撃を提案した．本論文で，我々は，$d < N$ を満たすようなより大きな復号指数に対して，その上位ビットと下位ビットが同時に得られたときに，Ernst らの攻撃を改良する．また，我々の提案攻撃を一般化 RSA 暗号に適用することで，Zheng らの攻撃をも改良する．提案攻撃は，Takayasu と Kunihiro の攻撃を拡張したものとなっているが，Ernst らの拡張とは違い，その構成は非自明である．Ernst らの攻撃は，単純な多項式の選択によって得られるのに対し，Takayasu-Kunihiro の攻撃は，上位もしくは下位ビットが得られたときそれぞれに応じて，複雑かつ異なる変数変換を用いて多項式を構成することによって得られる．我々は，これら二つを特別な場合として含む，より統一的な変数変換を導入することで，Takayasu-Kunihiro の攻撃を拡張する．

キーワード　RSA 暗号，部分鍵導出攻撃，Coppersmith の手法，格子理論

目次

第 1 章

はじめに

1.1 研究背景

1.1.1 RSA 暗号

RSA 暗号は 1978 年に Rivest らによって考案された，現在最も広く使われている公開鍵暗号方式のひとつである [15]．RSA 暗号は，2 つの大きな異なる素数 p, q の積 N を素因数分解することが計算量的に困難という事実を安全性の根拠とした暗号方式である．RSA 暗号では，自然数 e, d を，$ed = 1 \pmod{(p-1)(q-1)}$ を満たすものとおき，(N, e) を公開鍵，d を秘密鍵とする．

これに対して，一般化 RSA 暗号 (RSA Variant with Euler Quotient) は 1995 年に Kuwakado らによって考案された，RSA 暗号をもとにした公開鍵暗号方式である [6, 11]．彼らは，N の Euler Quotient を用いることで，先述の RSA 暗号をより一般化した暗号方式を構成した．本論文では，RSA 暗号と一般化 RSA 暗号の安全性について議論する．

1.1.2 RSA 暗号に対する部分鍵導出攻撃

これまで RSA 暗号および一般化 RSA 暗号において，秘密鍵の上位ビットもしくは下位ビットが得られたときに鍵全体を復元するアルゴリズムが，Coppersmith の手法を用いて活発に研究されてきた [1, 2, 7, 9, 16, 18, 19]．一連の研究は，より少ない部分情報で RSA 暗号を破る多項式時間攻撃アルゴリズムを構成することを目標としてきた．このうち RSA 暗号に対しては，Ernst らの攻撃 [7] と Takaysu と Kunihiro の攻撃 [18] が，現在知られている中で，最も少ない部分情報で秘密鍵を復元できる．また一般化 RSA 暗号に対しては，Zheng らの攻撃 [19] が，現在知られている中で最も良い攻撃である．本論文ではこれ以降，Ernst らの攻撃，Takayasu と Kunihiro の攻撃，Zheng らの攻撃をそれぞれ EJMW 攻撃，TK 攻撃，ZKH 攻撃とよぶ．

RSA 暗号に対する EJMW 攻撃と TK 攻撃は，どちらも Coppersmith の手法を用いて構成されている．TK 攻撃は，Coppersmith の手法における多項式の選択をより詳細に解析することで，EJMW 攻撃を改良したものである．TK 攻撃は，秘密鍵の上位ビットま

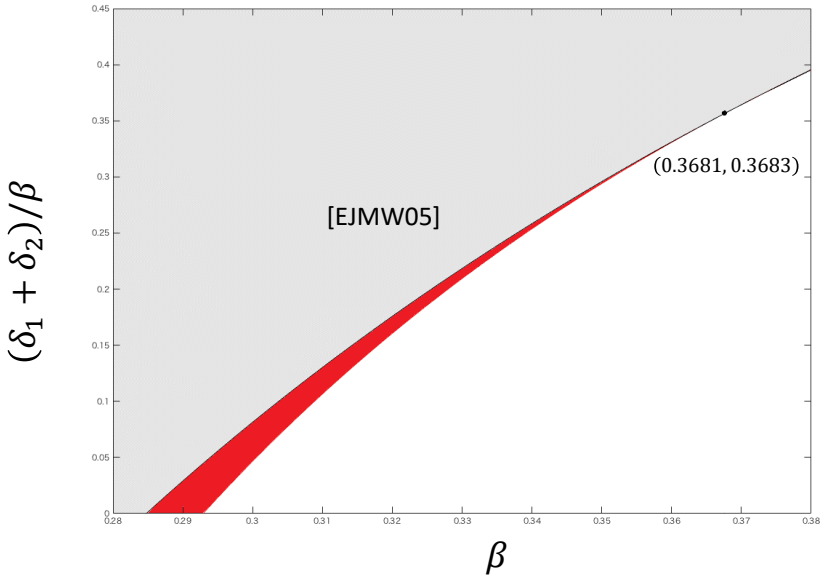

図 1.1. $N^{0.28} < d < N^{0.38}$ のときの RSA 暗号に対する既存攻撃と提案攻撃の適用範囲の比較

たは下位ビットから全体を復元するものでは，それぞれ $d < N^{9/16} = N^{0.5625}$ のとき，$d < N^{(9-\sqrt{21})/12} = N^{0.368\cdots}$ のとき，EJMW 攻撃より少ない部分情報で秘密鍵を復元できる．

ただし，Ernst らは，秘密鍵の上位ビットと下位ビット両方の部分情報が得られたときに鍵を復元する攻撃を提案した [7]．本論文ではこれ以降，この設定での Ernst らの攻撃を，Ernst らの拡張攻撃とよぶ．これに対して，Takayasu と Kunihiro は，この設定での攻撃は提案していない．しかし，上位ビットが得られたときの TK 攻撃は，$d < N^{0.5625}$ のときにも EJMW 攻撃より良い攻撃となっているため，上位および下位ビットが両方得られたとき，少なくとも $d < N^{0.5625}$ の範囲において Ernst らの拡張攻撃は改良できると考えられる．よって，本論文では，TK 攻撃を適切に拡張することで，Ernst らの拡張攻撃の改良を目指す．

1.2　成果

我々は本論文で，RSA 暗号および一般化 RSA 暗号に対して，秘密鍵の上位ビットと下位ビット両方の部分情報から鍵全体を復元する攻撃を構成する．その上で，既存攻撃と提案攻撃を比較するための数値実験を行う．提案攻撃は，上位ビットまたは下位ビットが与えられたときの TK 攻撃を拡張することで得られたものである．RSA 暗号に対する提案攻撃は，$N^{0.284} < d < N$ のときに，Ernst らの拡張攻撃より少ない部分情報で秘密鍵を復元できる．TK 攻撃による改良は，$N^{0.284} < d < N^{0.5625}$ を満たすような小さい秘密鍵に対してのみ EJMW 攻撃を改良するものだったのに対し，提案攻撃は，より大きい秘密鍵でも改良できる．提案攻撃は，大きな秘密鍵において EJMW 攻撃を改良する初めてのものである．

図 1.1 は，$N^{0.28} < d < N^{0.38}$ のときの，既存攻撃と提案攻撃の適用範囲の比較を表したものである．図は，$\beta \log N$ ビットの秘密鍵のうち，上位 $\delta_1 \log N$ ビットと下位 $\delta_2 \log N$ ビット

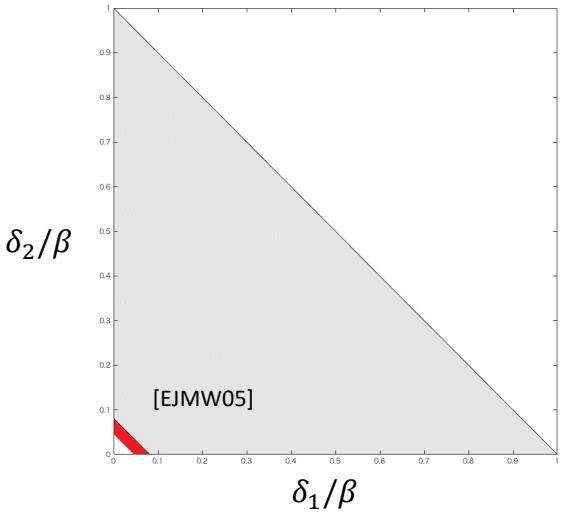

図 1.2. $d = N^{0.3}$ のときの既存攻撃と提案攻撃の適用範囲の比較

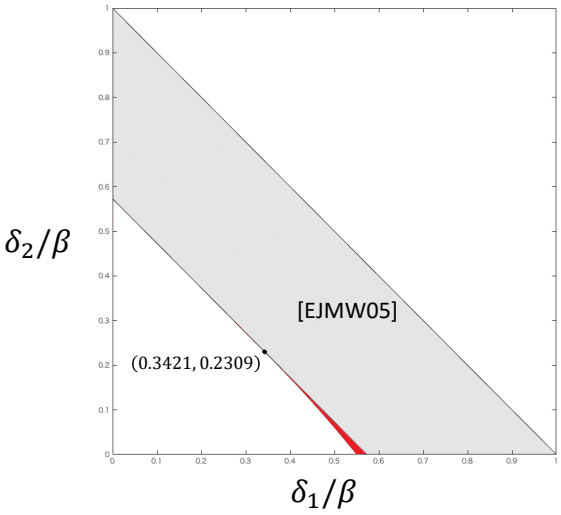

図 1.3. $d = N^{0.45}$ のときの既存攻撃と提案攻撃の適用範囲の比較

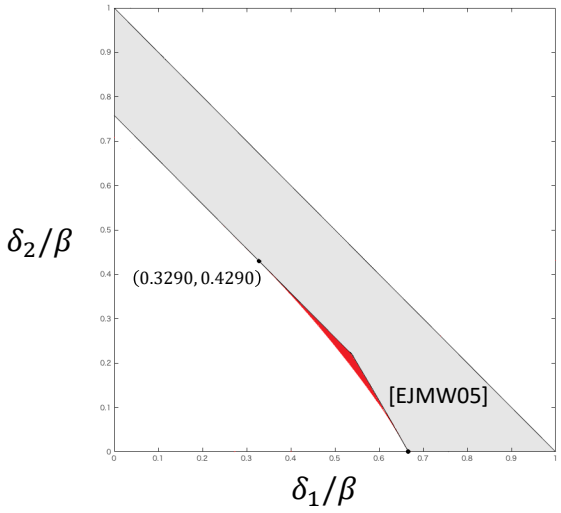

図 1.4. $d = N^{0.5625}$ のときの既存攻撃と提案攻撃の適用範囲の比較

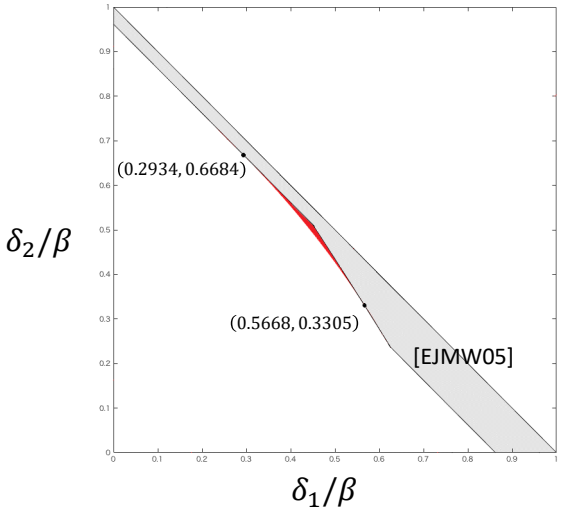

図 1.5. $d = N^{0.8}$ のときの既存攻撃と提案攻撃の適用範囲の比較

の部分情報が得られた状況における，攻撃可能な範囲を表している．横軸は秘密鍵の大きさ β を，縦軸は部分情報の割合の和 $(\delta_1 + \delta_2)/\beta$ を表している．灰色の部分は EJMW 攻撃の適用範囲で，赤い部分は提案攻撃の適用範囲である．この図から，提案攻撃は $d < N^{0.368}$ のとき，復元に必要な部分情報の和 $\delta_1 + \delta_2$ をより少なくしているという意味で，EJMW 攻撃を改良していることが分かる．

提案攻撃は，$N^{0.368} < d$ となるような d に対しても改良範囲をもつ．図 1.2–1.5 はそれぞれ，$\beta = 0.3, 0.45, 0.5625, 0.8$ のときの，既存攻撃と提案攻撃の適用範囲の比較を表したものである．これらの図において，横軸は上位ビットの割合 δ_1/β を，縦軸は下位ビットの割合

δ_2/β を表している．

また，一般化 RSA 暗号に対する提案攻撃については，$N^{0.569} < d < N^2$ のときに，ZKH 攻撃より少ない部分情報で秘密鍵を復元できる．$\beta = 0.6, 0.9, 1.125, 1.6$ のときの改良範囲は，それぞれ図 1.2–1.5 と同じものとなる．

1.3　本論文の構成

本論文ではまず，第 2 章で，RSA 暗号および Coppersmith の手法について説明する．次に，第 3 章で，既存研究を示す．第 4 章では，RSA 暗号に対する提案攻撃を示す．第 5 章では，一般化 RSA 暗号に対する提案攻撃を示す．最後に，結論を述べる．

第 2 章

準備

この章では，まず，RSA 暗号および，RSA を一般化した暗号方式を定義する．次に，格子理論を説明する．その後，Coppersmith の手法を紹介する．

2.1 RSA 暗号の定義

RSA 暗号および一般化 RSA 暗号の定義をする．

まず，RSA 暗号の定義を行う．ビット長が同じ 2 つの異なる素数 p, q に対して，$N = pq$ とおく．自然数 e, d を，

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

を満たすものとおく．RSA 暗号では (N, e) を公開鍵，d を秘密鍵とする．平文 m の暗号化は $c = m^e \pmod{N}$，暗号文 c の復号は $m = c^d \pmod{N}$ により行われる．本論文では，RSA 暗号を考えるとき，簡単のため，$e \approx N$ である状況を考える．

続いて，一般化 RSA 暗号の定義を行う．ビット長が同じ 2 つの異なる素数 p, q に対して，$N = pq$ とおく．自然数 e, d を，

$$ed = 1 \pmod{(p^2-1)(q^2-1)}$$

を満たすものとおく．一般化 RSA 暗号では (N, e) を公開鍵，d を秘密鍵とする．本論文では，一般化 RSA 暗号を考えるとき，簡単のため，$e \approx N^2$ である状況を考える．

2.2 格子

2.2.1 格子の定義

格子の定義を述べる．

正整数 k, n を $k \leq n$ となるようにおく．$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^k$ を互いに線形独立な行ベクトルとする．$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ の整数線形結合で張られる格子 $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ を

$$L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) := \left\{ \sum_{i=1}^{n} c_i \boldsymbol{b}_i | c_i \in \mathbb{Z} \right\}$$

と定義する．

$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{Z}^k$ のとき，格子 $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ を整数格子とよぶ．また，$n = k$ となるような格子を，フルランクな格子とよぶ．本論文で構成する格子は，特に指示がない限り，フルランクな整数格子のみを扱う．

2.2.2　LLL 格子基底簡約アルゴリズム

$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ を各行にもつような $n \times k$ 行列を $\boldsymbol{B}$ とする．LLL 格子基底簡約アルゴリズムは，行列 $\boldsymbol{B}$ を入力として，ノルムの小さい格子上のベクトル $\boldsymbol{v}_1, \boldsymbol{v}_2$ を多項式時間で出力する．

行列 $\boldsymbol{B}$ の張る格子の体積を $\mathrm{vol}(L(\boldsymbol{B}))$ で表す．格子の体積は，$\mathrm{vol}(L(\boldsymbol{B})) := \sqrt{\det \boldsymbol{B}\boldsymbol{B}^T}$ で計算される．特に，格子がフルランクなとき，$\mathrm{vol}(L(\boldsymbol{B})) = |\det \boldsymbol{B}|$ となる．LLL アルゴリズムの出力するベクトルのノルムの大きさについて，次の事実が知られている．

命題 2.1 (LLL 格子基底簡約アルゴリズム [12, 13])**.** $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ を線形独立な n 個の k 次元整数ベクトルとし，これらを各行にもつような $n \times k$ 行列を $\boldsymbol{B}$ とする．*LLL* 格子基底簡約アルゴリズムは，$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ が与えられたとき，$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n$ が張る格子上のベクトルで以下を満たすような *2* つの線形独立なベクトル $\boldsymbol{v}_1, \boldsymbol{v}_2$ を多項式時間で探す．

$$||\boldsymbol{v}_1|| \leq 2^{\frac{k-1}{4}} (\mathrm{vol}(L(\boldsymbol{B})))^{\frac{1}{n}}, \quad ||\boldsymbol{v}_2|| \leq 2^{\frac{k}{2}} (\mathrm{vol}(L(\boldsymbol{B})))^{\frac{1}{n-1}}.$$

2.3　Coppersmith の手法

Coppersmith の手法の概要

法付き方程式の小さい解を多項式時間で求める方法として，Coppersmith の手法を紹介する [4]．この手法は，本論文で紹介するすべての攻撃に共通して用いられている．

2 変数多項式 $h(x, y) = \sum h_{i,j} x^i y^j$ に対して，多項式のノルムを $\|h(x, y)\| := \sqrt{\sum h_{i,j}^2}$ とする．Howgrave-Graham は，以下の補題を示した [10].

補題 2.1 (Howgrave-Graham の補題 [10])**.** 最大 n 個の単項からなる多項式 $h(x, y)$ と正整数 W, X, Y に対して，

1. $h(\tilde{x}, \tilde{y}) = 0 \pmod{W}$ ただし，$|\tilde{x}| < X, |\tilde{y}| < Y$
2. $\|h(xX, yY)\| < \dfrac{W}{\sqrt{n}}$

を満たすとき，整数上で $h(\tilde{x}, \tilde{y}) = 0$ が成立する．

この補題を使って，法付き方程式を解く問題を整数方程式を解く問題に帰着させることを基本戦略とする．いま，法付き方程式の解と同じ値の根を持つような 2 つの法付き多項式を構成できたとする．この 2 つの法付き多項式のノルムが補題 2.1 の条件 2 を満たすほど小さければ，これらを整数方程式として考えて，元の法付き方程式の解を得ることができる．

Coppersmith の手法の法付き方程式を解く手順を説明する．求めたい解を $(\tilde{x}, \tilde{y})$ とし，X, Y を $|\tilde{x}| < X, |\tilde{y}| < Y$ を満たすような整数とする．m, r を正整数とする．W^m を法として $(x, y) = (\tilde{x}, \tilde{y})$ を根にもつような多項式 $g_1(x, y), \ldots, g_r(x, y)$ を，登場する単項の総数が r 個となるように作る．

いま，r 個の多項式 $g_1(xX, yY), \ldots, g_r(xX, yY)$ に対して，各項の係数をそれぞれ要素とするような r 個のベクトル $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_r$ を構成する．これらのベクトルを各行に持つような基底行列を $\boldsymbol{B}$ とする．$\boldsymbol{B}$ を LLL アルゴリズムに入力して得られる 2 つのベクトルの成分を，多項式 $h_1(xX, yY), h_2(xX, yY)$ の係数に対応させる．このとき，命題 2.1 より，多項式 $h_1(xX, yY), h_2(xX, yY)$ のノルムは $2^{r/2}|\det \boldsymbol{B}|^{1/(r-1)}$ より小さい．したがって補題 2.1 より，もし $2^{r/2}|\det \boldsymbol{B}|^{1/(r-1)} < W^m/\sqrt{r}$ ならば，$h_1(\tilde{x}, \tilde{y}) = 0, h_2(\tilde{x}, \tilde{y}) = 0$ となる．

解 $(\tilde{x}, \tilde{y})$ を求めるために，2 つの 2 変数整数方程式 $h_1(x, y) = 0, h_2(x, y) = 0$ の共通解を探す．いま，もし多項式 $h_1(x, y), h_2(x, y)$ が代数的に独立であるならば，2 つの多項式の終結式を求めることによって，共通解を探すことができる．本論文では，このようにして得られる多項式 $h_1(x, y), h_2(x, y)$ は必ず代数的に独立であると仮定して議論する．この仮定は必ず成り立つとは限らないが，攻撃を実装したときに成り立つケースが多いことが分かっている．以上より，整数方程式 $h_1(x, y) = 0, h_2(x, y) = 0$ の共通解はすべて効率的に求められる．このうちの 1 つが $f(x, y) = 0$ の法付き方程式の解 $(x, y) = (\tilde{x}, \tilde{y})$ である．

Helpful な多項式

本論文では，Coppersmith の手法に従って提案攻撃を構成する．攻撃を成立させるために必要な条件は，小さい項を無視すると $|\det \boldsymbol{B}|^{1/r} < W^m$ と書ける．m を固定したとき，法付き方程式の解の上限 X, Y が大きくなるほど $|\det \boldsymbol{B}|^{1/r}$ の値は大きくなる．ここで，この行列 $\boldsymbol{B}$ は，通常三角行列となるように構成される．いま，もし構成した行列 $\boldsymbol{B}$ が三角行列になると仮定すると，$|\det \boldsymbol{B}|^{1/r}$ の値は対角成分の相乗平均となる．すなわち，対角成分に対応する項がより小さい多項式を選んで行列を構成することができれば，法付き方程式のより大きな解を導出することができる．

May は，このような多項式を集めるために，行列 $\boldsymbol{B}$ の各行に対応する多項式に対して，多項式の対角成分に対応する項の大きさに関する 1 つの指標として，Helpful な多項式という概念を導入した [14]．Takayasu と Kunihiro は，多項式が Helpful であることを以下のように定義し直し，Helpful でない多項式をできるだけ使わないような行列の構成法を提案した [17, 18]．

定義 2.1. 法付き方程式 $f(x, y) = 0 \pmod{W}$ を解くための正方行列を $\boldsymbol{B}$ とし，$g(x, y) \pmod{W^m}$ を $\boldsymbol{B}$ の列ベクトルに対応する多項式とする．いま，$\boldsymbol{B}$ の構成に使われている $g(x, y)$ 以外のすべての多項式のみを使って，三角行列 $\boldsymbol{B}'$ を構成できたとする．このとき，多項式 $g(x, y)$ が *Helpful* であるとは，

$$\left|\frac{\det \boldsymbol{B}}{\det \boldsymbol{B}'}\right| \leq W^m$$

となることである．

本論文の提案攻撃では，Takayasu と Kunihiro の提案した構成法を応用することで，行列

を構成する.

第 3 章

既存研究

本章では，RSA 暗号および一般化 RSA 暗号に対する既存攻撃を紹介し，各攻撃の適用条件をまとめる．

3.1 RSA 暗号に対する既存の部分鍵導出攻撃

3.1.1 RSA 暗号に対する部分鍵導出攻撃の定式化

秘密鍵の上位ビットと下位ビットが得られた状況に対応する，法付き方程式問題を定式化する．N を RSA 暗号の合成数とし，公開鍵 e を $\log N$ ビットとする．全体で $\beta \log N$ ビットの秘密鍵 $d \approx N^{\beta}$ のうち，上位 $\delta_1 \log N$ ビットの値を $d_1 \approx N^{\delta_1}$，下位 $\delta_2 \log N$ ビットの値を $d_2 \approx N^{\delta_2}$ とする．このとき，

$$M_1 := 2^{(\beta-\delta_1)\log N}, \quad M_2 := 2^{\delta_2 \log N}$$

とすると，秘密鍵 d は

$$d = d_1 M_1 + d' M_2 + d_2$$

と表すことができる．いま攻撃者に，d_1, d_2 の値が与えられていて，d' の値が未知であるような状況を考える．このような d を RSA の鍵生成にあてはめると，

$$e(d_1 M_1 + d' M_2 + d_2) = 1 + \ell(p-1)(q-1)$$

となる．このとき，ℓ の近似を $\ell_0 := \lfloor (ed_1M_1 - 1)/N \rfloor$ とすると，ℓ の真の値との近似誤差は

$$\begin{aligned}
|\ell - \ell_0| &= \left| \frac{e(d_1M_1 + d'M_2 + d_2) - 1}{N - p - q + 1} - \left\lfloor \frac{ed_1M_1 - 1}{N} \right\rfloor \right| \\
&\leq \left| \frac{N(e(d'M_2 + d_2)) - (ed_1M_1 - 1)(-p - q + 1)}{N(N - p - q + 1)} \right| + 1 \\
&\leq \left| \frac{e(d'M_2 + d_2)}{N - p - q + 1} \right| + \left| \frac{(ed_1M_1 - 1)(p + q - 1)}{(N - p - q + 1)N} \right| + 1 \\
&\leq N^{\beta - \delta_1} + N^{\beta - \frac{1}{2}} + 1
\end{aligned}$$

となる．ここで，提案攻撃は $\delta_1 < 1/2$ のときにのみ EJMW 攻撃を改良するため，本論文では，特に断らない限りこの場合のみを扱う．$\delta_1 < 1/2$ のとき，近似誤差 $|\ell - \ell_0|$ は高々 $N^{\beta-\delta_1}$ の定数倍となる．

多項式 $f_{eM_2}(x,y), f_e(x,y)$ を，

$$f_{eM_2}(x,y) := 1 - ed_2 + (\ell_0 + x)(N + y) \pmod{eM_2}, \tag{3.1}$$
$$f_e(x,y) := 1 + (\ell_0 + x)(N + y) \pmod{e} \tag{3.2}$$

とおくと，$(\tilde{x}, \tilde{y}) := (\ell - \ell_0, -p - q + 1)$ は $f_{eM_2}(x,y), f_e(x,y)$ の根となる．$(\tilde{x}, \tilde{y})$ の絶対値は，それぞれ高々 $X := N^{\beta-\delta_1}, Y := N^{1/2}$ の定数倍である．したがって，法付き方程式 $f_{eM_2}(x,y) = 0, f_e(x,y) = 0$ においてこれより小さい解を求めることができれば，N の素因数分解ができる．

3.1.2　RSA 暗号に対する既存攻撃の概要

EJMW 攻撃

Ernst らは，Coppersmith の手法 [5] を使い，上位ビットと下位ビットが得られた状況における RSA 暗号に対する攻撃を提案した [7]．彼らの手法を用いると，この章で定式化した $\beta, \delta_1, \delta_2$ が以下の条件を満たすとき，攻撃が成功する [7]．

(a) $\beta \leq \dfrac{235 + 904\delta_2 + 1064\delta_2^2 + 416\delta_2^3 + 48\delta_2^4}{512(1+\delta_2)^2}$ のとき，

$$\delta_1 + \delta_2 > \beta - \frac{5}{6} + \frac{\sqrt{6\beta + 1}}{3},$$

(b) $\dfrac{235 + 904\delta_2 + 1064\delta_2^2 + 416\delta_2^3 + 48\delta_2^4}{512(1+\delta_2)^2} < \beta \leq \dfrac{11 + 20\delta_2 + 12\delta_2^2}{16(1+\delta_2)}$ のとき，

$$\delta_1 > \beta - \frac{3(1+2\delta_2)^2}{16(1+\delta_2)},$$

(c) $\dfrac{11 + 20\delta_2 + 12\delta_2^2}{16(1+\delta_2)} < \beta$ のとき，

$$\delta_1 + \delta_2 > \frac{1}{3}\left(2\beta - 1 + \sqrt{4\beta^2 + 2\beta - 2}\right)$$

条件 (b) は [7] で示されているものとは一致しないが，これは彼らの論文に誤りが含まれているため，上記のように訂正をした．この条件 (b) の導出方法は次章で述べる．

TK 攻撃

Takayasu と Kunihiro は，上位ビットのみまたは下位ビットのみが得られた 2 つの状況に限定して，EJMW 攻撃を改良した [18]．彼らは，3.1.1 章の攻撃設定において上位ビットのみが与えられたとき，すなわち $\delta_2 = 0, d_2 = 0$ であるような状況で，EJMW 攻撃の適用条件を以下のように改良できることを示した．

(A) $\beta \leq \frac{1}{2}$ のとき，

$$\delta_1 > \frac{1}{2}\left(-1+\beta+\sqrt{-3\beta^2+6\beta-1}\right),$$

(B) $\frac{1}{2} < \beta \leq \frac{9}{16}$ のとき，

$$6(\beta-\delta_1)\sigma - 3\sigma^2 + 2\sigma^3 < \frac{(\sigma-2\delta_1)^3}{2-2\beta-2\delta_1}, \quad \sigma = 1 - \frac{2\beta-1}{1-2\sqrt{1-\beta-\delta_1}}$$

また Takayasu と Kunihiro は，下位ビットのみが与えられたとき，すなわち $\delta_2 = 0, d_2 = 0$ であるような状況でも EJMW 攻撃の適用条件を以下のように改良できることを示した [18].

$$\beta < \frac{9-\sqrt{21}}{12} \quad and \quad \delta_2 > \frac{1}{2}\left(-1+\beta+\sqrt{-3\beta^2+6\beta-1}\right)$$

このとき，δ_2 の下限は (A) の左辺と同じである．ただし，β の範囲は (A) よりも狭く，彼らの攻撃は $\beta < (9-\sqrt{21})/12 = 0.368\cdots$ のときに成功する．

攻撃の構成を紹介する前に，TK 攻撃において行列を構成する際に用いる関数を定義する．下記の関数 $l_{k,\tau}^{MSBs}(\cdot)$ および $l_{k,\tau}^{LSBs}(\cdot)$ は，それぞれ TK 攻撃の上位ビット攻撃，下位ビット攻撃で使われている．

定義 3.1. k を正整数，τ を実数とする．実数に対して定義される整数値関数 $l_{k,\tau}^{MSBs}(\cdot)$ および $l_{k,\tau}^{LSBs}(\cdot)$ を以下で定義する．

$$l_{k,\tau}^{MSBs}(x) := \max\left\{0, \left\lceil \frac{x-k}{\tau+1} \right\rceil\right\}, \quad l_{k,\tau}^{LSBs}(x) := \max\left\{0, \left\lceil \frac{x-k}{\tau} \right\rceil\right\}$$

$l_{k,\tau}^{MSBs}(\cdot)$ は $-1 \leq \tau \leq 1$，$l_{k,\tau}^{LSBs}(\cdot)$ は $-1 \leq \tau \leq 0$ となるときのみ定義される．

以下，TK 攻撃の構成を紹介する．TK 攻撃は，多項式 (3.2) および (3.1) の根 $(\tilde{x}, \tilde{y}) = (\ell - \ell_0, -p-q+1)$ を，Coppersmith の手法を用いて探すことによって構成される．上位ビットのみが与えられたときは $d_2 = 0, M_2 = 1$ となり，$f_{eM_2}(x,y)$ と $f_e(x,y)$ は等価となる．上位ビットの攻撃では，m を正整数とし，以下のような多項式を攻撃構成に使った．

$$\begin{aligned} g_{[u,i]}^{(x)}(x,y) &= x^{u-i} f_e(x,y)^i e^{m-i}, \\ g_{[u,j]}^{(y)}(x,y) &= y^j f_e(x,y)^u e^{m-u} \end{aligned}$$

また，下位ビットのみが与えられたときは $d_1 = 0$ となり，$\ell_0 = 0$ となる．$f_{eM_2}(x,y), f_e(x,y)$ に新たな変数 $w = \ell_0 + x$ を導入することで，$f_{eM_2}^{LSBs}(w,y), f_e^{LSBs}(w,y)$ を以下のように定義する．

$$\begin{aligned} f_{eM_2}^{LSBs}(w,y) &:= 1 - ed_2 + w(N+y) \pmod{eM_2}, \\ f_e^{LSBs}(w,y) &:= 1 + w(N+y) \pmod{e} \end{aligned}$$

下位ビットの攻撃では，以下のような多項式を攻撃構成に使った．

$$\begin{aligned} g^{(w)}_{[u,i]}(w,y) =& x^{u-i} f_{eM_2}(w,y)^i (eM_2)^{m-i}, \\ g^{(y)}_{[u,j]}(w,y) =& y^j f_{eM_2}(w,y)^{u-l^{LSBs}_{k,\tau}(j)} f_e(w,y)^{l^{LSBs}_{k,\tau}(j)} e^{m-u} M_2^{m-(u-l^{LSBs}_{k,\tau}(j))} \end{aligned}$$

次に，k, s を正整数，τ を実数とする．$(u,i),(u,j)$ のインデックスの集合 $\mathcal{I}_{x1}, \mathcal{I}_{y1}$ をそれぞれ

$$\begin{cases} \mathcal{I}_{x1} := \{u = 0,1,\ldots,m; i = 0,1,\ldots,u\}, \\ \mathcal{I}_{y1} := \{u = 0,1,\ldots,m; j = 1,2,\ldots,k + \lfloor \tau u \rfloor\} \end{cases} \tag{3.3}$$

と定め，$\mathcal{I}_{x2}, \mathcal{I}_{y2}$ を

$$\begin{cases} \mathcal{I}_{x2} := \{u = 0,1,\ldots,m; i = 0,1,\ldots,u\}, \\ \mathcal{I}_{y2} := \{u = 0,1,\ldots,m; j = 1,2,\ldots,\min\{s-u, k + \lfloor \tau u \rfloor\}\} \end{cases} \tag{3.4}$$

と定める．上位ビット攻撃の行列は，(3.3) と (3.4) の両方を使って構成され，下位ビット攻撃は，(3.3) のみを使って構成された．Takayasu と Kunihiro は，このように構成された行列にとって，できるだけ Helpful な多項式が使われるように k, s, τ の値を調整した．

3.2　一般化 RSA 暗号に対する既存の部分鍵導出攻撃

3.2.1　一般 RSA 暗号に対する部分鍵導出攻撃の定式化

3.1.1 節と同様に $N, e, d, d_1, d', d_2, M_1, M_2$ を $e = N^2$ となるように定める．これらを一般化 RSA の鍵生成にあてはめると，

$$e(d_1 M_1 + d' M_2 + d_2) = 1 + \ell(p^2 - 1)(q^2 - 1)$$

となる．このとき，ℓ の近似 ℓ_0 を $\ell_0 = \lfloor (ed_1 M_1 - 1)/N^2 \rfloor$ とすると，ℓ の真の値との近似誤差は

$$\begin{aligned} |\ell - \ell_0| =& \left| \frac{e(d_1 M_1 + d' M_2 + d_2) - 1}{N^2 - p^2 - q^2 + 1} - \left\lfloor \frac{ed_1 M_1 - 1}{N^2} \right\rfloor \right| \\ \leq& \left| \frac{N^2(e(d' M_2 + d_2)) - (ed_1 M_1 - 1)(-p^2 - q^2 + 1)}{N(N^2 - p^2 - q^2 + 1)} \right| + 1 \\ \leq& \left| \frac{e(d' M_2 + d_2)}{N^2 - p^2 - q^2 + 1} \right| + \left| \frac{(ed_1 M_1 - 1)(p^2 + q^2 - 1)}{(N^2 - p^2 - q^2 + 1)N} \right| + 1 \\ \leq& N^{\beta - \delta_1} + N^{\beta - 1} + 1 \end{aligned}$$

となる．$\delta_1 < 1$ のとき，$|\ell - \ell_0|$ は高々 $N^{\beta-\delta_1}$ の定数倍となり，$1 < \delta_1$ のとき，$|\ell - \ell_0|$ は高々 $N^{\beta-1}$ の定数倍となる．

多項式 $f_{eM_2}(x,y), f_e(x,y)$ を，

$$f_{eM_2}(x,y) := 1 - ed_2 + (\ell_0 + x)(N^2 + y) \pmod{eM_2}, \tag{3.5}$$

$$f_e(x,y) := 1 + (\ell_0 + x)(N^2 + y) \pmod{e} \tag{3.6}$$

とおくと，$(\tilde{x}, \tilde{y}) := (\ell - \ell_0, -p^2 - q^2 + 1)$ は $f_{eM_2}(x,y), f_e(x,y)$ の根となる．$(\tilde{x}, \tilde{y})$ の絶対値は，それぞれ高々 $X := N^{\beta-\delta_1}, Y := N$ の定数倍である．したがって，法付き方程式 $f_{eM_2}(x,y) = 0, f_e(x,y) = 0$ においてこれより小さい解を求めることができれば，N の素因数分解ができる．

3.2.2　一般化 RSA 暗号に対する既存攻撃の概要

Zheng らは，上位ビットと下位ビットが得られた状況における一般化 RSA 暗号に対する攻撃を提案した [19]．彼らの提案攻撃を用いると，前章で定式化した $\beta, \delta_1, \delta_2$ が以下の条件を満たすとき，攻撃が成功する．

$$\delta_1 + \delta_2 > \beta - \frac{5}{3} + \frac{2}{3}\sqrt{3\beta + 1} \tag{3.7}$$

彼らの攻撃の構成は，3.1.2 節で述べた EJMW 攻撃 [7] と同じ構成である．

第 4 章

RSA 暗号に対する提案攻撃

本章では，前章で述べた RSA 暗号に対する既存攻撃の，改良攻撃を提案する．本章ではまず，3.1.1 節で定式化した攻撃設定に対して，Sarkar らの攻撃 [16] を素朴に応用した攻撃を示す．この攻撃の成功条件は EJMW 攻撃が示した 3 章の (b) と同じで，改良攻撃とはなっていない．しかし，EJMW 攻撃では計算の誤りがあったため，(b) とは違う条件が示されていた．我々は Sarkar らの攻撃を応用することでこれを適切に修正することができた．

よって，本章ではまず，Sarkar らの攻撃の自明な拡張を構成し，条件 (b) を導出する．その後，我々の改良攻撃について説明する．最後に，数値実験により，既存攻撃と提案攻撃の比較を示す．

4.1 Sarkar らの手法の自明な拡張

2.3 章で紹介した Coppersmith の手法を用いて攻撃を構成する．多項式 $f_{eM_2}(x,y)$ を，3.1.1 章の式 (3.1) で定めたものとし，法付き方程式 $f_{eM_2}(x,y) = 0 \pmod{eM_2}$ の解 $(\tilde{x},\tilde{y}) = (\ell - \ell_0, -p-q+1)$ を探す．

m, s を正整数とおく．攻撃で用いる多項式 $g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ を以下のように定義する．

$$\begin{aligned} g^{(x)}_{[u,i]}(x,y) :=& x^{u-i} f_{eM_2}(x,y)^i (eM_2)^{m-i}, \\ g^{(y)}_{[u,j]}(x,y) :=& y^j f_{eM_2}(x,y)^u (eM_2)^{m-u} \end{aligned} \tag{4.1}$$

すべての $u = 0, 1, \ldots, m$ と非負整数 i, j に対して，$g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ は，$(x,y) = (\ell - \ell_0, -p-q+1)$ を代入したとき，$(eM_2)^m$ を法として 0 となる．また，$(u,i), (u,j)$ のインデックスの集合 $\mathcal{I}_{x3}, \mathcal{I}_{y3}$ をそれぞれ

$$\begin{cases} \mathcal{I}_{x3} := \{u = 0, 1, \ldots, m; i = 0, 1, \ldots, \min\{s, u\}\}, \\ \mathcal{I}_{y3} := \{u = 0, 1, \ldots, k-1; j = 1, 2, \ldots, s-u\} \end{cases} \tag{4.2}$$

と定め，$(u,i) \in \mathcal{I}_{x3}$ に対して多項式 $g^{(x)}_{[u,i]}(x,y)$ を，$(u,j) \in \mathcal{I}_{y3}$ に対して多項式 $g^{(y)}_{[u,j]}(x,y)$ を使う．

表 4.1. Sarkar らの手法の自明な拡張における $m = 2$ のときの基底行列の例

	1	y	y^2	x	xy	xy^2	x^2	x^2y	x^2y^2
$g^{(x)}_{[0,0]}$	$(eM_2)^2$								
$g^{(y)}_{[0,1]}$		$Y(eM_2)^2$							
$g^{(y)}_{[0,2]}$			$Y(eM_2)^2$						
$g^{(x)}_{[1,0]}$				$X(eM_2)^2$					
$g^{(x)}_{[1,1]}$	$*$	$*$		$*$	$XYeM_2$				
$g^{(y)}_{[1,1]}$		$*$	$*$		$*$	XY^2eM_2			
$g^{(x)}_{[2,0]}$							$X^2(eM_2)^2$		
$g^{(x)}_{[2,1]}$				$*$	$*$		$*$	X^2YeM_2	
$g^{(x)}_{[2,2]}$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	X^2YeM_2

次に，これらの多項式に $(x, y) = (xX, yY)$ を代入し，各項の係数をそれぞれ要素となるようなベクトルを，各行に対応させた基底行列 $\boldsymbol{B}_0$ を構成する．表 4.1 は，$m = 2$ としたときの行列の構成例である．表中の * は，非ゼロ成分を表す．この表から，基底行列は三角行列となるように構成できることがわかる．

行列の対角成分のうち，多項式 $g^{(x)}_{[u,i]}(x, y)$ に対応するものは，

$$X^u Y^i (eM_2)^{m-i}$$

となり，多項式 $g^{(y)}_{[u,j]}(x, y)$ に対応するものは，

$$X^u Y^{u+j} (eM_2)^{m-u}$$

となる．

$\sigma := s/m$ とする．行列 $\boldsymbol{B}_0$ の次元 r は，

$$r = \sum_{(u,i)\in\mathcal{I}_{x3}} 1 + \sum_{(u,j)\in\mathcal{I}_{y3}} 1 = \sigma m^2 + o(m^2)$$

となる．行列式の値を $\det(\boldsymbol{B}_0) = X^{s_X} Y^{s_Y} (eM_2)^{s_{eM_2}}$ と表すと，これらはそれぞれ，

$$\begin{aligned}
s_X &= \sum_{u=0}^{m}\sum_{i=0}^{s} u = \frac{1}{2}\sigma m^3 + o(m^3), \\
s_Y &= \sum_{u=0}^{m}\sum_{i=0}^{s} j = \frac{1}{2}\sigma^2 m^3 + o(m^3), \\
s_{eM_2} &= \sum_{u=0}^{s}\sum_{i=0}^{u}(m-i) + \sum_{u=s}^{m}\sum_{i=0}^{s}(m-i) + \sum_{u=0}^{s-1}\sum_{j=1}^{s-u}(m-u) \\
&= \left(\sigma - \frac{1}{2}\sigma^2 + \frac{1}{6}\sigma^3\right) m^3 + o(m^3)
\end{aligned}$$

となる．このとき，条件 $|\det \boldsymbol{B}|^{1/r} < (eM_2)^m$ を満たせば攻撃が成功する．条件を整理すると，

$$\frac{1}{6}(1+\delta_2)\sigma^2 + \left(-\frac{1}{4} - \frac{1}{2}\delta_2\right)\sigma + \frac{1}{2}\beta - \frac{1}{2}\delta_1 < 0$$

となる．この不等式の左辺を最小化するような σ は，

$$\sigma = \frac{\dfrac{1}{4} + \dfrac{1}{2}\delta_2}{2 \cdot \dfrac{1}{6}(1+\delta_2)}$$

である．これを代入してしてさらに整理すると，

$$\delta_1 > \beta - \frac{3(1+2\delta_2)^2}{16(1+\delta_2)}$$

を得る．$\delta_1 \leq 1/2$ より，β の範囲は

$$\beta < \delta_1 + \frac{3(1+2\delta_2)^2}{16(1+\delta_2)} \leq \frac{11 + 20\delta_2 + 12\delta_2^2}{16 + 16\delta_2}$$

となる．□

4.2　改良攻撃

この章では，上位ビットのみが与えられたときの TK 攻撃の構成を，下位ビットが与えられたときの構成より有効に活用して，両方が同時に得られた状況に対する攻撃として拡張した攻撃を提案する．

定理 4.1. (N, e) を公開鍵，d を秘密鍵とする *RSA* 暗号を考える．$e \approx N, d \approx N^{\beta}, \beta < 1$ とする．秘密鍵 d のうち，上位 $\delta_1 \log N$ ビットの値 $d_1 \approx N^{\delta_1}$ および下位 $\delta_2 \log N$ ビットの値 $d_2 \approx N^{\delta_2}$ が与えられたとする．N が十分大きいとき，以下を満たすならば N を $\log N$ の多項式時間で素因数分解するアルゴリズムが存在する．

1. $\beta < \dfrac{9 - \sqrt{21}}{12}$ のとき，

$$\delta_1 + \delta_2 > \frac{1}{2}\left(-1 + \beta + \sqrt{-3(1-\beta)^2 + 2}\right),$$

2. $\dfrac{1}{2} - \delta_1 + \delta_2 \leq \beta \leq \dfrac{1}{2} + \delta_2$ のとき，

$$\delta_1 > \frac{1}{2}\left(-1 + \beta - \delta_2 + \sqrt{-3(1-\beta+\delta_2)^2 + 2(1+\delta_2)}\right),$$

3. $\frac{1}{2}+\delta_2 \le \beta \le \delta_1(4(1+\delta_2)(1-\delta_1)-1)$ のとき，

$$6(\beta-\delta_1)\sigma - 3(1+2\delta_2)\sigma^2 + 2(1+\delta_2)\sigma^3 < \frac{(\sigma-2\delta_1)^3}{2-2\beta-2\delta_1+2\delta_2},$$

$$\sigma = 1 - \frac{2\beta-2\delta_2-1}{1-2\sqrt{(1+\delta_2)(1-\beta-\delta_1+\delta_2)}}$$

秘密鍵 d の大きさが $N^{1-1/\sqrt{2}} < d < N$ にあるとき，提案攻撃は，既存攻撃が適用できない条件で攻撃可能である．この提案攻撃は，3.1.2 節で紹介した TK 攻撃を拡張したものである．定理 4.1 は，$\delta_1 = 0$ としたとき，上位ビットのみが得られたときの TK 攻撃の適用条件 (A) および (B) を含む．また，$\delta_2 = 0$ としたとき，下位ビットのみが得られたときの TK 攻撃の適用条件と一致する．この提案攻撃は，TK 攻撃を特別な場合として含むという意味で，TK 攻撃の拡張を達成したものである．

定理 4.1 の条件 1 のときの攻撃を RSA に対する攻撃 1，条件 2 のときの攻撃を RSA に対する攻撃 2，条件 3 のときの攻撃を RSA に対する攻撃 3 とする．4.2.1 節で RSA に対する攻撃 1，4.2.2 節で RSA に対する攻撃 2，4.2.3 節で RSA に対する攻撃 3 を構成する．それぞれの攻撃における多項式と行列の構成には，TK 攻撃で使われた関数 $l^{MSBs}_{k,\tau}(\cdot)$ および $l^{LSBs}_{k,\tau}(\cdot)$ が用いられている．詳細は定義 3.1 を参照のこと．

4.2.1 RSA に対する攻撃 1

多項式 $f_{eM_2}(x,y), f_e(x,y)$ をそれぞれ，3.1.1 章の式 (3.1) および (3.2) で定めたものとし，法付き方程式 $f_{eM_2}(x,y) = 0 \pmod{eM_2}$ および $f_e(x,y) = 0 \pmod{e}$ の解 $(\tilde{x},\tilde{y}) = (\ell-\ell_0, -p-q+1)$ を探す．

m,k を正整数，τ を実数とおく．$(eM_2)^m$ を法として $(\tilde{x},\tilde{y}) = (\ell-\ell_0,-p-q+1)$ を根に持つ複数の多項式を，$f_{eM_2}(x,y), f_e(x,y)$ を使って構成する．攻撃で用いる多項式 $g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ を以下のように定義する．

$$\begin{aligned} g^{(x)}_{[u,i]}(x,y) :=& x^{u-i} f_{eM_2}(x,y)^i (eM_2)^{m-i}, \\ g^{(y)}_{[u,j]}(x,y) :=& y^j f_{eM_2}(x,y)^{u-l^{LSBs}_{k,\tau}(j)} f_e(x,y)^{l^{LSBs}_{k,\tau}(j)} e^{m-u} M_2^{m-(u-l^{LSBs}_{k,\tau}(j))} \end{aligned} \tag{4.3}$$

すべての $u = 0,1,\ldots,m$ と非負整数 i,j に対して，これらの多項式 $g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ は，$(x,y) = (\ell-\ell_0,-p-q+1)$ を代入したとき，$(eM_2)^m$ を法として 0 となる．$(u,i),(u,j)$ のインデックスの集合 $\mathcal{I}_{x1},\mathcal{I}_{y1}$ をそれぞれ式 (3.4) のように定める．$(u,i) \in \mathcal{I}_{x1}$ に対して多項式 $g^{(x)}_{[u,i]}(x,y)$ を，$(u,j) \in \mathcal{I}_{y2}$ に対して多項式 $g^{(y)}_{[u,j]}(x,y)$ を使う．

次に，これらの多項式に $(x,y) = (xX, yY)$ を代入し，各項の係数をそれぞれ要素とするようなベクトルを，各行に対応させた行列 $\boldsymbol{B}_1$ を構成する．表 4.2 は $m = 2$ としたときの素朴な基底行列の構成例である．

表 4.2. RSA に対する攻撃 1 の $m = 2$ のときの基底行列の例

	1	x	y	xy	y^2	xy^2	x^2	x^2y	x^2y^2	y^3	xy^3	x^2y^3	y^4	xy^4	x^2y^4
$g^{(x)}_{[0,0]}$	$(eM_2)^2$														
$g^{(x)}_{[1,0]}$		$X(eM_2)^2$													
$g^{(x)}_{[1,1]}$	$*$	$*$	$Y\ell_0eM_2$	$XYeM_2$											
$g^{(y)}_{[1,1]}$			$*$	$*$	$Y^2\ell_0eM_2^2$	$XY^2eM_2^2$									
$g^{(x)}_{[2,0]}$							$X^2(eM_2)^2$								
$g^{(x)}_{[2,1]}$		$*$		$*$			$*$	X^2YeM_2							
$g^{(x)}_{[2,2]}$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	X^2Y^2						
$g^{(y)}_{[2,1]}$			$*$	$*$	$*$	$*$		$*$	$*$	$Y^3\ell_0^2M_2$	$2XY^3\ell_0M_2$	$X^2Y^3M_2$			
$g^{(y)}_{[2,2]}$					$*$	$*$			$*$	$*$	$*$	$*$	$Y^4\ell_0^2M_2$	$2XY^4\ell_0M_2$	$X^2Y^4M_2^2$

表 4.3. RSA に対する攻撃 1 の $m = 2$ のときの変数変換後の基底行列の例

	1	x	z	yz	x^2	xz	xyz	yz^2	y^2z^2
$g^{(x)}_{[0,0]}$	$(eM_2)^2$								
$g^{(x)}_{[1,0]}$		$X(eM_2)^2$							
$g^{(x)}_{[1,1]}$	$*$	$*$	ZeM_2						
$g^{(y)}_{[1,1]}$			$*$	$YZeM_2^2$					
$g^{(x)}_{[2,0]}$					$X^2(eM_2)^2$				
$g^{(x)}_{[2,1]}$		$*$		$*$		$XZeM_2$			
$g^{(x)}_{[2,2]}$	$*$	$*$	$*$	$*$	$*$	$*$	XYZ		
$g^{(y)}_{[2,1]}$	$*$	$*$	$*$	$*$		$*$	$*$	YZ^2M_2	
$g^{(y)}_{[2,2]}$	$*$		$*$	$*$			$*$	$*$	$Y^2Z^2M_2^2$

この行列 $\boldsymbol{B}_1$ は三角行列となっていないが，新たな変数

$$z := (\ell_0 + x)y + 1$$

を導入することで，三角行列となるように構成することができる．$\tilde{z} := (\ell_0 + \tilde{x})\tilde{y} + 1$ の絶対値は，高々 $Z := N^{1/2+\beta}$ の定数倍である．表 4.3 は，表 4.2 の行列に新たな変数 z を導入した行列である．これらの表から，変数変換を施すことで，基底行列を三角行列となるように構成できることがわかる．このことを，次の補題によって示す．

補題 4.1 ($g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ が三角行列をなすこと)．$g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ を式 *(4.3)* で定めたものとする．$\mathcal{I}_{x1}, \mathcal{I}_{y1}$ を式 *(3.3)* で定めた $(u,i), (u,j)$ の組の集合とする．$(u,i) \in \mathcal{I}_{x1}$ に対して多項式 $g^{(x)}_{[u,i]}(x,y)$ を，$(u,j) \in \mathcal{I}_{y1}$ に対して多項式 $g^{(y)}_{[u,j]}(x,y)$ を使う．$\boldsymbol{B}$ を $g^{(x)}_{[u,i]}(xX,yY), g^{(y)}_{[u,j]}(xX,yY)$ の各項の係数をそれぞれ要素とするようなベクトルを，各行対応させた行列とする．これらの多項式に対して多項式順序を以下のように定める．

- $u' < u$ のとき，

$$g^{(x)}_{[u',i']}(xX,yY), g^{(y)}_{[u',j']}(xX,yY) \prec g^{(x)}_{[u,i]}(xX,yY),\ g^{(y)}_{[u,j]}(xX,yY),$$

- $u' = u, i' < i, j' < j$ のとき，

$$\begin{aligned} g^{(x)}_{[u,i]}(xX,yY) &\prec g^{(y)}_{[u,j]}(xX,yY), \\ g^{(x)}_{[u',i']}(xX,yY) &\prec g^{(x)}_{[u,i]}(xX,yY), \\ g^{(y)}_{[u',j']}(xX,yY) &\prec g^{(y)}_{[u,j]}(xX,yY) \end{aligned}$$

この順序に従って行列を構成すると，行列 $\boldsymbol{B}$ は三角行列となる．行列の対角成分のうち，多項式 $g^{(x)}_{[u,i]}(x,y)$ に対応するものは，

$$X^{u-l^{MSBs}_{k,\tau}(i)} Y^{i-l^{MSBs}_{k,\tau}(i)} Z^{l^{MSBs}_{k,\tau}(i)} (eM_2)^{m-i}$$

となり，多項式 $g^{(y)}_{[u,j]}(x,y)$ に対応するものは，

$$X^{u-l^{MSBs}_{k,\tau}(u+j)} Y^{u+j-l^{MSBs}_{k,\tau}(u+j)} Z^{l^{MSBs}_{k,\tau}(u+j)} e^{m-u} M_2^{m-(u-l^{LSBs}_{k,\tau}(j))} \tag{4.4}$$

となる．

補題 4.1 の証明.

最初に，多項式 $g^{(y)}_{[u,j]}(x,y)$ について，行列の対角成分にあたる変数以外はすべて，先に定めた順序で先行する多項式に登場する変数で表すことができることを示す．その後，対角成分のうち $g^{(y)}_{[u,j]}(x,y)$ にあたるものが，補題 4.1 の対角成分 (4.4) となるようにできることを示す．式 (4.3) で定められる多項式 $g^{(y)}_{[u,j]}(x,y)$ は，係数を無視すると

$$y^j f_{eM_2}(x,y)^{u-l^{LSBs}_{k,\tau}(j)} f_e(x,y)^{l^{LSBs}_{k,\tau}(j)} \tag{4.5}$$

となる．以下，この多項式を，先に定めた順序で先行する多項式に登場する変数で表すことを考える．多項式 (4.5) に登場する x, y の指数の組 (i_x, i_y) の集合は以下のようになる．

$$\mathcal{I}_{LSBs}^{(u,j)} := \left\{ \begin{array}{l} i_y = j, j+1, \ldots, u+j; \\ i_x = l_{k,\tau}^{LSBs}(i_y), l_{k,\tau}^{LSBs}(i_y)+1, \ldots, u \end{array} \right\}$$

いま，多項式 (4.5) に対して，変数変換

$$z = (\ell_0 + x)y + 1$$

を適用する．このとき，多項式 (4.5) は，$(i_x, i_y) \in \mathcal{I}_{LSBs}^{(u,j)}$ の各元に対してそれぞれある整数 $c_{i_x,i_y}^{(u,j)}$ が存在して，

$$\sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u,j)}} c_{i_x,i_y}^{(u,j)} x^{i_x - l_{k,\tau}^{MSBs}(i_y)} y^{i_y - l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)} \tag{4.6}$$

で表すことができることを示す．

いま，$(u,j) \in \mathcal{I}_{y1}$ を $u \geq 1, j \geq 2$ とすると，$\mathcal{I}_{y1}$ の定め方 (3.3) より，$(u, j-1), (u-1, j-1) \in \mathcal{I}_{y1}$ となる．これらに対応する 2 つの多項式 $g_{[u,j-1]}^{(y)}(x,y), g_{[u-1,j-1]}^{(y)}(x,y)$ および $g_{[u-1,j]}^{(y)}(x,y)$ は，補題 4.1 での多項式順序の定め方から，$g_{[u,j]}^{(y)}(x,y)$ より先行している．

(i) $(u-1, j) \in \mathcal{I}_{y1}$ のとき
$g_{[u-1,j]}^{(y)}(x,y)$ が $\mathcal{I}_{LSBs}^{(u-1,j)}$ に対して (4.6) と同様の表し方ができると仮定する．多項式 (4.5) は，

$$\begin{aligned}
&y^j f_{eM_2}(x,y)^{u - l_{k,\tau}^{LSBs}(j)} f_e(x,y)^{l_{k,\tau}^{LSBs}(j)} \\
=&y^j f_{eM_2}(x,y)^{u-1 - l_{k,\tau}^{LSBs}(j)} f_e(x,y)^{l_{k,\tau}^{LSBs}(j)} ((\ell_0+x)(N+y) + 1 - ed') \\
=& \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u-1,j)}} c_{i_x,i_y}^{(u-1,j)} x^{i_x - l_{k,\tau}^{MSBs}(i_y)} y^{i_y - l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)} \cdot (z + N(\ell_0+x) + 1 - ed') \\
=& \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u-1,j)}} d_{i_x,i_y}^{(u-1,j-1)} x^{i_x - l_{k,\tau}^{MSBs}(i_y)} y^{i_y - l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)} \\
&+ \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u,j-1)}} e_{i_x,i_y}^{(u,j-1)} x^{i_x - l_{k,\tau}^{MSBs}(i_y)} y^{i_y - l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)} \\
&+ c_{u-1,u-1+j}^{(u-1,j)} x^{u - l_{k,\tau}^{MSBs}(u+j)} y^{u+j - l_{k,\tau}^{MSBs}(u+j)} z^{l_{k,\tau}^{MSBs}(u+j)}
\end{aligned}$$

と表すことができる．

(ii) $(u-1, j) \notin \mathcal{I}_{y1}$ のとき
$g_{[u,j-1]}^{(y)}(x,y), g_{[u-1,j-1]}^{(y)}(x,y)$ が，それぞれ $\mathcal{I}_{LSBs}^{(u-1,j)}, \mathcal{I}_{LSBs}^{(u,j-1)}$ に対して (4.6) と同様の表し方ができると仮定する．$\mathcal{I}_{y1}$ の定め方 (3.3) より，$k + \lfloor \tau(u-1) \rfloor < j \leq k + \lfloor \tau u \rfloor$ となるので，

$$j = k + \lfloor \tau u \rfloor$$

となる．このとき，$l_{k,\tau}^{MSBs}(u+j) = l_{k,\tau}^{LSBs}(j) = u$ となっていることに注意する．多項式 (4.5) は，

$$y^j f_{eM_2}(x,y)^{u - l_{k,\tau}^{LSBs}(j)} f_e(x,y)^{l_{k,\tau}^{LSBs}(j)}$$

$$
\begin{aligned}
&= y^j(z+N(\ell_0+x))^u \\
&= y^{j-1}(z+N(\ell_0+x))^{u-1}(zy+N(z-1)) \\
&= \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u-1,j-1)}} c_{i_x,i_y}^{(u-1,j-1)} x^{i_x-l_{k,\tau}^{MSBs}(i_y)} y^{i_y-l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)}(zy+N(z-1)) \\
&= \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u-1,j-1)}} d_{i_x,i_y}^{(u-1,j-1)} x^{i_x-l_{k,\tau}^{MSBs}(i_y)} y^{i_y-l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)} \\
&\quad + \sum_{(i_x,i_y)\in\mathcal{I}_{LSBs}^{(u,j-1)}} e_{i_x,i_y}^{(u,j-1)} x^{i_x-l_{k,\tau}^{MSBs}(i_y)} y^{i_y-l_{k,\tau}^{MSBs}(i_y)} z^{l_{k,\tau}^{MSBs}(i_y)} \\
&\quad + c_{u-1,u-1+j-1}^{(u-1,j-1)} x^{u-l_{k,\tau}^{MSBs}(u+j)} y^{u+j-l_{k,\tau}^{MSBs}(u+j)} z^{l_{k,\tau}^{MSBs}(u+j)}
\end{aligned}
$$

と表すことができる．

(i),(ii) より，多項式 $g_{[u,j]}^{(y)}(x,y)$ の行列の対角成分にあたる変数以外はすべて，先に定めた順序で先行する多項式 $g_{[u-1,j]}^{(y)}(x,y), g_{[u,j-1]}^{(y)}(x,y), g_{[u-1,j-1]}^{(y)}(x,y)$ に登場する変数で表すことができる．

また，多項式 $g_{[0,1]}^{(y)}(x,y)$ について，$g_{[0,1]}^{(y)}(x,y)=y(eM_2)^m$ より，$c_{(0,1)}^{0,1}=1$ である．先の議論から，$c_{u,u+j}^{(u,j)}=c_{u-1,u-1+j}^{(u-1,j)}$ または $c_{u,u+j}^{(u,j)}=c_{u-1,u-1+j-1}^{(u-1,j-1)}$ であるので，すべての $u,j\in\mathcal{I}_{y1}$ に対して，$c_{u,u+j}^{(u,j)}=1$ である．

以上のことから，行列の対角成分のうち，多項式 $g_{[u,j]}^{(y)}(x,y)$ に対応するものは，

$$X^{u-l_{k,\tau}^{MSBs}(u+j)} Y^{u+j-l_{k,\tau}^{MSBs}(u+j)} Z^{l_{k,\tau}^{MSBs}(u+j)} e^{m-u} M_2^{m-(u-l_{k,\tau}^{LSBs}(j))}$$

となる． □

補題 4.1 は，正整数 k，実数 τ が $k\geq 1, 0\leq\tau\leq 1$ を満たすときに三角行列 $\boldsymbol{B}$ を構成できることを保証している．正整数 k，実数 τ を，

$$k=\lfloor 2(\delta_1+\delta_2)m\rfloor, \quad \tau=1-2\beta-2\delta_1-2\delta_2 \tag{4.7}$$

となるようにとる．このとき，τ は β,δ_1,δ_2 の値によるため，$0\leq\tau\leq 1$ を満たしているかどうかは自明ではない．そこで，式 (4.7) のように定めた τ が $0\leq\tau\leq 1$ を満たしていると仮定して議論を進め，攻撃が成功するような β,δ_1,δ_2 の条件をまず導出する．そして，そのような β,δ_1,δ_2 に対して定められる τ が $0\leq\tau\leq 1$ を満たしているかどうかを最後に検証する．

我々は，2.3 章で定義した Helpful な多項式のみを使って行列を構成することを目標として攻撃を構成した．正整数 k，実数 τ の値 (4.7) は，以下の補題によって定めた．

補題 4.2. 補題 *4.1* の行列 $\boldsymbol{B}$ に対して，多項式 $g_{[u,j]}^{(y)}(x,y)$ は，以下を満たすとき，*Helpful* である．

$$j\leq 2(\delta_1+\delta_2)m+(1-2\beta-2\delta_1-2\delta_2)u$$

補題 4.2 の証明.

補題 4.1 のような三角行列 $\boldsymbol{B}$ が構成できたとする．いま，あるインデックスの組 (u',j') を，$u'=l_{k,\tau}^{LSBs}(j')$ となるようにおく．行列 $\boldsymbol{B}$ のインデックスの定め方 (3.3) より，行列 $\boldsymbol{B}$ のあ

るひとつの列は，多項式 $g^{(y)}_{[u',j']}(x,y)$ に対応するものである．またこのとき，定義 3.1 より，

$$l^{MSBs}_{k,\tau}(u'+j') = u' \tag{4.8}$$

となる．

このような行列 $\boldsymbol{B}$ に対して，多項式 $g^{(y)}_{[u',j']}(x,y)$ に対応する列を使わないような新たな行列を $\boldsymbol{B'}$ とする．このとき，新たな $\boldsymbol{B'}$ も補題 4.1 を満たしていると仮定する．いま，多項式 $g^{(y)}_{[u',j']}(x,y)$ が，行列 $\boldsymbol{B},\boldsymbol{B'}$ に対して Helpful であるかどうかを考える．

$\boldsymbol{B}$ の対角成分のうち，$g^{(y)}_{[u',j']}(x,y)$ に対応するものは，補題 4.1 および式 (4.8) より，

$$Y^{j'}Z^{u'}e^{m-u'}{M_2}^m$$

となる．いま，多項式

$$g^{(y)}_{[u'+1,j'-1]}(x,y), g^{(y)}_{[u'+2,j'-2]}(x,y), \ldots, g^{(y)}_{[u'+j'-1,1]}(x,y),$$

および

$$g^{(x)}_{[u'+j',u'+j']}(x,y), g^{(x)}_{[u'+j'+1,u'+j']}(x,y), \ldots, g^{(x)}_{[m,u'+j']}(x,y),$$

および

$$g^{(y)}_{[u'+1,j']}(x,y), g^{(y)}_{[u'+2,j']}(x,y), \ldots, g^{(y)}_{[m,j']}(x,y)$$

は行列 $\boldsymbol{B},\boldsymbol{B'}$ に含まれる．$\boldsymbol{B}$ の対角成分のうち，これらに対応するものはそれぞれ

$$XY^{j'}Z^{u'}e^{m-(u'+1)}{M_2}^{m-(u'+1-l^{LSBs}_{k,\tau}(j'+1))}, X^2Y^{j'}Z^{u'}e^{m-(u'+2)}{M_2}^{m-(u'+2-l^{LSBs}_{k,\tau}(j'+2))}, \ldots,$$
$$X^{j'-1}Y^{j'}Z^{u'}e^{m-(u'+j'-1)}{M_2}^{m-(u'+j'-1-l^{LSBs}_{k,\tau}(u'+j'-1))},$$

および

$$X^{j'}Y^{j'}Z^{u'}(eM_2)^{m-(u'+j')}, X^{j'+1}Y^{j'}Z^{u'}(eM_2)^{m-(u'+j')}, \ldots, X^{m-u'}Y^{j'}Z^{u'}(eM_2)^{m-(u'+j')},$$

および

$$X^{u'+1-l^{MSBs}_{k,\tau}(u'+j'+1)}Y^{u'+j'+1-l^{MSBs}_{k,\tau}(u'+j'+1)}Z^{l^{MSBs}_{k,\tau}(u'+j'+1)}e^{m-(u'+1)}{M_2}^{m-1},$$
$$X^{u'+2-l^{MSBs}_{k,\tau}(u'+j'+2)}Y^{u'+j'+2-l^{MSBs}_{k,\tau}(u'+j'+2)}Z^{l^{MSBs}_{k,\tau}(u'+j'+2)}e^{m-(u'+2)}{M_2}^{m-2},$$
$$\vdots$$
$$X^{m-l^{MSBs}_{k,\tau}(m+j')}Y^{m+j'-l^{MSBs}_{k,\tau}(m+j')}Z^{l^{MSBs}_{k,\tau}(m+j')}{M_2}^{u'}$$

である．また，$\boldsymbol{B'}$ の対角成分のうち，これらに対応するものはそれぞれ

$$Y^{j'-1}Z^{u'+1}e^{m-(u'+1)}{M_2}^{m-(u'+1-l^{LSBs}_{k,\tau}(j'+1))},$$
$$XY^{j'-1}Z^{u'+1}e^{m-(u'+2)}{M_2}^{m-(u'+2-l^{LSBs}_{k,\tau}(j'+2))},$$
$$\vdots$$

$$X^{j'-2}Y^{j'-1}Z^{u'+1}e^{m-(u'+j'-1)}{M_2}^{m-(u'+j'-1-l_{k,\tau}^{LSBs}(u'+j'-1))},$$

および

$$X^{j'-1}Y^{j'-1}Z^{u'+1}(eM_2)^{m-(u'+j')}, X^{j'}Y^{j'-1}Z^{u'+1}(eM_2)^{m-(u'+j')}, \ldots,$$
$$X^{m-u'-1}Y^{j'-1}Z^{u'+1}(eM_2)^{m-(u'+j')},$$

および

$$X^{u'+1-l_{k,\tau}^{MSBs}(u'+j'+1)}Y^{u'+j'+1-l_{k,\tau}^{MSBs}(u'+j'+1)}Z^{l_{k,\tau}^{MSBs}(u'+j'+1)}e^{m-(u'+1)}{M_2}^{m},$$
$$X^{u'+2-l_{k,\tau}^{MSBs}(u'+j'+2)}Y^{u'+j'+2-l_{k,\tau}^{MSBs}(u'+j'+2)}Z^{l_{k,\tau}^{MSBs}(u'+j'+2)}e^{m-(u'+2)}{M_2}^{m-1},$$
$$\vdots$$
$$X^{m-l_{k,\tau}^{MSBs}(m+j')}Y^{m+j'-l_{k,\tau}^{MSBs}(m+j')}Z^{l_{k,\tau}^{MSBs}(m+j')}{M_2}^{u'+1}$$

である．他の対角成分は同じなので，

$$\left|\frac{\det \boldsymbol{B}}{\det \boldsymbol{B}'}\right| = (eM_2)^{m-u'}(ZM_2)^{u'}Y^{j'}\left(\frac{XY}{ZM_2}\right)^{m-u'}$$

となる．この値が $(eM_2)^m$ より小さいことの必要十分条件は，

$$(eM_2)^{m-u'}(ZM_2)^{u'}Y^{j'}\left(\frac{XY}{ZM_2}\right)^{m-u'} \leq (eM_2)^m$$
$$X^{m-u'}Y^{m-u'+j'}Z^{-m+2u'} \leq e^{u'}{M_2}^{m-u'}$$

である．よって，$X = N^{\beta-\delta_1}, Y = N^{1/2}, W = N^{\beta}, e \approx N, M_2 = 2^{\delta_2 \log N}$ を代入すると，条件

$$(\beta-\delta_1)(m-u') + \frac{1}{2}(m-u'+j') + \left(\frac{1}{2}+\beta\right)(-m+2u') \leq u' + \delta_2(m-u')$$

を得る．これを整理すると，

$$j' \leq 2(\delta_1+\delta_2)m + (1-2\beta-2\delta_1-2\delta_2)u'$$

となる． □

式 (4.7) で決められた k, τ の値によって構成される行列 $\boldsymbol{B}$ の次元 r は，

$$r = \sum_{(u,i)\in\mathcal{I}_{x1}} 1 + \sum_{(u,j)\in\mathcal{I}_{y1}} 1 = \left(\frac{1}{2} + 2(\delta_1+\delta_2) + \frac{1}{2}(1-2\beta-2\delta_1-2\delta_2)\right)m^2 + o(m^2)$$

となる．行列式の値を $\det(\boldsymbol{B}) = X^{s_X}Y^{s_Y}Z^{s_Z}e^{s_e}{M_2}^{s_{M_2}}$ と表すと，これらはそれぞれ，

$$s_X = \sum_{(u,i)\in\mathcal{I}_{x1}} (u - l_{k,\tau}^{MSBs}(i)) + \sum_{(u,j)\in\mathcal{I}_{y1}} (u - l_{k,\tau}^{MSBs}(u+j))$$
$$\left(\frac{1}{6} + (\delta_1+\delta_2) + \frac{1}{6}(1-2\beta-2\delta_1-2\delta_2)\right)m^3 + o(m^3),$$

$$
\begin{aligned}
s_Y &= \sum_{(u,i)\in\mathcal{I}_{x1}} (i - l_{k,\tau}^{MSBs}(i)) + \sum_{(u,j)\in\mathcal{I}_{y1}} (u + j - l_{k,\tau}^{MSBs}(u+j)) \\
&= \Big((\delta_1+\delta_2) + 2(\delta_1+\delta_2)^2 + (\delta_1+\delta_2)(1-2\beta-2\delta_1-2\delta_2) + \frac{1}{6}(1-2\beta-2\delta_1-2\delta_2) \\
&\quad + \frac{1}{6}(1-2\beta-2\delta_1-2\delta_2)^2 \Big) m^3 + o(m^3), \\
s_Z &= \sum_{(u,i)\in\mathcal{I}_{x1}} (l_{k,\tau}^{MSBs}(i)) + \sum_{(u,j)\in\mathcal{I}_{y1}} l_{k,\tau}^{MSBs}(u+j) \\
&= \left(\frac{1}{6} + \frac{1}{6}(1-2\beta-2\delta_1-2\delta_2) \right) m^3 + o(m^3), \\
s_e &= \sum_{(u,i)\in\mathcal{I}_{x1}} (m-u) + \sum_{(u,j)\in\mathcal{I}_{y1}} (m-u) \\
&= \left(\frac{1}{3} + (\delta_1+\delta_2) + \frac{1}{6}(1-2\beta-2\delta_1-2\delta_2) \right) m^3 + o(m^3), \\
s_{M_2} &= \sum_{(u,i)\in\mathcal{I}_{x1}} (m-u) + \sum_{(u,j)\in\mathcal{I}_{y1}} (m - (u - l_{k,\tau}^{LSBs}(j))) \\
&= \left(\frac{1}{3} + (\delta_1+\delta_2) + \frac{1}{3}(1-2\beta-2\delta_1-2\delta_2) \right) m^3 + o(m^3)
\end{aligned}
$$

となる．このとき，条件 $|\det \boldsymbol{B}|^{1/r} < (eM_2)^m$ を満たせば攻撃が成功する．条件を整理すると，

$$2(\delta_1+\delta_2)^2 + 2(1-\beta)(\delta_1+\delta_2) + 2(1-\beta)^2 - 1 > 0$$

となる．この不等式を解くことによって，

$$\delta_1+\delta_2 > \frac{1}{2}\left(-1+\beta+\sqrt{-3(1-\beta)^2+2}\right)$$

を得る．式 (4.7) で定めた τ が

$$0 \le \tau \le 1$$

を満たすとき，この攻撃は成功する．τ についてこの制約を整理すると，

$$\beta \le \frac{9-\sqrt{21}}{12}$$

となる．　□

4.2.2　RSA に対する攻撃 2

4.2.1 章と同様に，Coppersmith の手法を用いて攻撃を構成する．RSA に対する攻撃 1 では多項式 $f_{eM_2}(x,y), f_e(x,y)$ を両方使ったが，本章で紹介する攻撃では多項式 $f_e(x,y)$ を使わず，多項式 $f_{eM_2}(x,y)$ のみを使う．また，RSA に対する攻撃 1 のうち多項式と行列の構成には関数 $l_{k,\tau}^{MSBs}(\cdot)$ および $l_{k,\tau}^{LSBs}(\cdot)$ が両方使われたが，本章では $l_{k,\tau}^{LSBs}(\cdot)$ は使わず，$l_{k,\tau}^{MSBs}(\cdot)$ のみを使う．

攻撃の構成を説明する．m,k を正整数，τ を実数とする．攻撃で用いる多項式 $g_{[u,i]}^{(x)}(x,y), g_{[u,j]}^{(y)}(x,y)$ には，式 (4.1) と同じものを使う．$(u,i),(u,j)$ のインデックスの集

合 $\mathcal{I}_{x1}, \mathcal{I}_{y1}$ には，式 (3.3) と同じものを使う．$(u,i) \in \mathcal{I}_{x1}$ に対して多項式 $g^{(x)}_{[u,i]}(x,y)$ を，$(u,j) \in \mathcal{I}_{y1}$ に対して多項式 $g^{(y)}_{[u,j]}(x,y)$ を用意する．

次に，これらの多項式に $(x,y) = (xX, yY)$ を代入し，各項の係数をそれぞれ要素とするようなベクトルを，各行に対応させた行列 $\boldsymbol{B}_2$ を構成する．表 4.4 は $m = 2, k = 1, \tau = 0$ としたときの素朴な基底行列の構成例である．

この行列 $\boldsymbol{B}_2$ は三角行列となっていないが，新たな変数

$$w := \ell_0 + x$$

を導入することで，三角行列となるように構成することができる．$\tilde{w} := \ell_0 + \tilde{x}$ の絶対値は，高々 $W := N^{\beta}$ の定数倍である．表 4.5 は，表 4.4 の行列に新たな変数 z を導入した行列である．これらの表から，変数変換を施すことで，基底行列を三角行列となるように構成できることがわかる．

次の補題 4.3 は，正整数 k，実数 τ に対して，$-1 \leq \tau \leq 0$ を満たすときに三角行列 $\boldsymbol{B}$ を構成できることを保証している．補題の証明は省略するが，この補題は，[18, **Lemma 7**] で Takayasu と Kunihiro が示したものを拡張したものである．

補題 4.3 ($g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ が三角行列をなすこと [18])**.** $g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ を式 *(4.1)* で定めた多項式とする．k を正整数，τ を $-1 \leq \tau \leq 0$ を満たすような実数とする．このような k, τ に対して，$(u,i), (u,j)$ の組の集合 $\mathcal{I}_{x1}, \mathcal{I}_{y1}$ を式 *(3.3)* のように定める．$(u,i) \in \mathcal{I}_{x1}$ を満たす多項式 $g^{(x)}_{[u,i]}(x,y)$ と，$(u,j) \in \mathcal{I}_{y1}$ を満たす多項式 $g^{(y)}_{[u,j]}(x,y)$ を使う．$\boldsymbol{B}$ を $g^{(x)}_{[u,i]}(xX,yY)$, $g^{(y)}_{[u,j]}(xX,yY)$ の各項の係数をそれぞれ要素とするようなベクトルを，各行対応させた行列とする．これらの多項式に対して多項式順序を以下のように定める．

- $u' < u$ のとき，

$$g^{(x)}_{[u',i']}(xX,yY),\, g^{(y)}_{[u',j']}(xX,yY) \prec g^{(x)}_{[u,i]}(xX,yY),\, g^{(y)}_{[u,j]}(xX,yY),$$

- $u' = u, i' < i, j' < j$ のとき，

$$\begin{aligned} g^{(x)}_{[u,i]}(xX,yY) &\prec g^{(y)}_{[u,j]}(xX,yY), \\ g^{(x)}_{[u',i']}(xX,yY) &\prec g^{(x)}_{[u,i]}(xX,yY), \\ g^{(y)}_{[u',j']}(xX,yY) &\prec g^{(y)}_{[u,j]}(xX,yY) \end{aligned}$$

この順序に従って行列を構成すると，行列 $\boldsymbol{B}$ は三角行列となる．行列の対角成分のうち，多項式 $g^{(x)}_{[u,i]}(x,y)$ に対応するものは，

$$W^{l_{k,\tau}(i)} X^{u - l_{k,\tau}(i)} Y^{i} (eM_2)^{m-i}$$

となり，多項式 $g^{(y)}_{[u,j]}(x,y)$ に対応するものは，

$$W^{l_{k,\tau}(u+j)} X^{u - l_{k,\tau}(u+j)} Y^{u+j} (eM_2)^{m-u}$$

となる．

表 4.4. RSA に対する攻撃 2 の $m = 2$ としたときの基底行列の例

	1	y	x	xy	y^2	xy^2	x^2	x^2y	x^2y^2	y^3	xy^3	x^2y^3
$g^{(x)}_{[0,0]}$	$(eM_2)^2$											
$g^{(y)}_{[0,1]}$		$Y(eM_2)^2$										
$g^{(x)}_{[1,0]}$			$X(eM_2)^2$									
$g^{(x)}_{[1,1]}$	$*$	$*$	$*$	$XYeM_2$								
$g^{(y)}_{[1,1]}$		$*$		$*$	$Y^2\ell_0eM_2$	XY^2eM_2						
$g^{(x)}_{[2,0]}$							$X^2(eM_2)^2$					
$g^{(x)}_{[2,1]}$			$*$	$*$		$*$		X^2YeM_2				
$g^{(x)}_{[2,2]}$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	X^2Y^2			
$g^{(y)}_{[2,1]}$		$*$		$*$	$*$		$*$	$*$	$*$	$Y^3\ell_0^2$	$2XY^3\ell_0$	X^2Y^3

表 4.5. RSA に対する攻撃 2 の $m = 2$ としたときの変数変換後の基底行列の例

	1	y	x	xy	wy^2	x^2	x^2y	wxy^2	w^2y^3
$g^{(x)}_{[0,0]}$	$(eM_2)^2$								
$g^{(y)}_{[0,1]}$		$Y(eM_2)^2$							
$g^{(x)}_{[1,0]}$			$X(eM_2)^2$						
$g^{(x)}_{[1,1]}$	$*$	$*$	$*$	$XYeM_2$					
$g^{(y)}_{[1,1]}$		$*$		$*$	WY^2eM_2				
$g^{(x)}_{[2,0]}$						$X^2(eM_2)^2$			
$g^{(x)}_{[2,1]}$			$*$	$*$		$*$	X^2YeM_2		
$g^{(x)}_{[2,2]}$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	WXY^2	
$g^{(y)}_{[2,1]}$		$*$		$*$	$*$		$*$	$*$	W^2Y^3

我々は，2.3 章での定義に基づいて，できるだけ Helpful な多項式のみを選んで行列を構成することを目標として攻撃を構成する．k, τ を，

$$k = \lfloor 2\delta_1 m \rfloor, \quad \tau = 1 - 2\beta - 2\delta_1 + 2\delta_2 \tag{4.9}$$

となるようにとる．この値 (4.9) は，以下の補題によって定めた．

補題 4.4. 補題 *4.3* の行列 $\boldsymbol{B}$ に対して，多項式 $g^{(y)}_{[u,j]}(x,y)$ は，以下を満たすとき，*Helpful* である．

$$j \leq 2\delta_1 m + (1 - 2\beta - 2\delta_1 + 2\delta_2)u \tag{4.10}$$

補題 4.4 の証明.

補題 4.3 のような三角行列 $\boldsymbol{B}$ が構成できたとする．いま，あるインデックスの組 (u', j') を，$u' = l_{k,\tau}(j')$ となるようにおく．インデックスの定め方 (3.4) より，行列 $\boldsymbol{B}$ のあるひとつの列は，多項式 $g^{(y)}_{[u',j']}(x,y)$ に対応するものである．またこのとき，定義 3.1 より，

$$l^{MSBs}_{k,\tau}(u' + j') = u' \tag{4.11}$$

となる．

このような行列 $\boldsymbol{B}$ に対して，多項式 $g^{(y)}_{[u',j']}(x,y)$ に対応する列を使わないような新たな行列を $\boldsymbol{B}'$ とする．このとき，新たな $\boldsymbol{B}'$ も補題 4.3 を満たしていると仮定する．いま，多項式 $g^{(y)}_{[u',j']}(x,y)$ が，行列 $\boldsymbol{B}, \boldsymbol{B}'$ に対して Helpful であるかどうかを判別する条件を導出する．

$\boldsymbol{B}$ の対角成分のうち，$g^{(y)}_{[u',j']}(x,y)$ に対応するものは，補題 4.3 および式 (4.11) より，

$$W^{u'} Y^{u'+j'} (eM_2)^{m-u'}$$

となる．いま，多項式

$$g^{(y)}_{[u'+1,j'-1]}(x,y), g^{(y)}_{[u'+2,j'-2]}(x,y), \ldots, g^{(y)}_{[u'+j'-1,1]}(x,y),$$

および

$$g^{(x)}_{[u'+j',u'+j']}(x,y), g^{(x)}_{[u'+j'+1,u'+j']}(x,y), \ldots, g^{(x)}_{[m,u'+j']}(x,y)$$

は行列 $\boldsymbol{B}, \boldsymbol{B}'$ に含まれる．$\boldsymbol{B}$ の対角成分のうち，これらの多項式に対応するものはそれぞれ

$$W^{u'} X Y^{u'+j'} (eM_2)^{m-(u'+1)}, W^{u'} X^2 Y^{u'+j'} (eM_2)^{m-(u'+2)}, \ldots,$$
$$W^{u'} X^{j'-1} Y^{u'+j'} (eM_2)^{m-(u'+j'-1)},$$

および

$$W^{u'} X^{j'} Y^{u'+j'} (eM_2)^{m-(u'+j')}, W^{u'} X^{j'+1} Y^{u'+j'} (eM_2)^{m-(u'+j')}, \ldots,$$
$$W^{u'} X^{m-u'} Y^{u'+j'} (eM_2)^{m-(u'+j')}$$

である．また，$\boldsymbol{B}'$ の対角成分のうち，これらに対応するものはそれぞれ

$$W^{u'+1} Y^{u'+j'} (eM_2)^{m-(u'+1)}, W^{u'+1} X Y^{u'+j'} (eM_2)^{m-(u'+2)}, \ldots,$$

$$W^{u'+1}X^{j'-2}Y^{u'+j'}(eM_2)^{m-(u'+j'-1)},$$

および

$$W^{u'+1}X^{j'-1}Y^{u'+j'}(eM_2)^{m-(u'+j')}, W^{u'+1}X^{j'}Y^{u'+j'}(eM_2)^{m-(u'+j')}, \ldots,$$
$$W^{u'+1}X^{m-(u'+1)}Y^{u'+j'}(eM_2)^{m-(u'+j')}$$

である．他の対角成分は同じなので，

$$\left|\frac{\det \boldsymbol{B}}{\det \boldsymbol{B'}}\right| = W^{u'}Y^{u'+j'}(eM_2)^{m-u'}\left(\frac{X}{W}\right)^{m-u'}$$

となる．この値が $(eM_2)^m$ より小さいことの必要十分条件は，

$$W^{u'}Y^{u'+j'}(eM_2)^{m-u'}\left(\frac{X}{W}\right)^{m-u'} \leq (eM_2)^m$$
$$\Leftrightarrow \quad X^{m-u'}Y^{u'+j'}W^{-m+2u'} \leq (eM_2)^{u'}$$

である．よって，$X = N^{\beta-\delta_1}, Y = N^{1/2}, W = N^{\beta}, e \approx N, M_2 = 2^{\delta_2 \log N}$ を代入すると，条件

$$(\beta-\delta_1)(m-u') + \frac{1}{2}(u'+j') + \beta(-m+2u') \leq (1+\delta_2)u'$$

を得る．これを整理すると，

$$j' \leq 2\delta_1 m + (1-2\beta-2\delta_1+2\delta_2)u'$$

となる．

したがって，u', j' が式 (4.10) を満たすとき，多項式 $g^{(y)}_{[u',j']}(x,y)$ は Helpful である．　□

式 (4.9) で決められた k, τ の値によって構成される行列 $\boldsymbol{B}_2$ の次元 r は，

$$r = \sum_{(u,i)\in\mathcal{I}_{x1}} 1 + \sum_{(u,j)\in\mathcal{I}_{y1}} 1 = (1-\beta+\delta_1+\delta_2)\,m^2 + o(m^2)$$

となる．$\det \boldsymbol{B}_2 = W^{s_W}X^{s_X}Y^{s_Y}(eM_2)^{s_{eM_2}}$ と表すと，これらはそれぞれ，

$$s_W = \sum_{(u,i)\in\mathcal{I}_{x1}} (l_{k,\tau}(i)) + \sum_{(u,j)\in\mathcal{I}_{y1}} l_{k,\tau}(u+j) = \frac{1}{3}(1-\beta-\delta_1+\delta_2)\,m^3 + o(m^3),$$
$$s_X = \sum_{(u,i)\in\mathcal{I}_{x1}} (u - l_{k,\tau}(i)) + \sum_{(u,j)\in\mathcal{I}_{y1}} (u - l_{k,\tau}(u+j)) = \frac{1}{3}(1-\beta+2\delta_1+\delta_2)\,m^3 + o(m^3),$$
$$s_Y = \sum_{(u,i)\in\mathcal{I}_{x1}} i + \sum_{(u,j)\in\mathcal{I}_{y1}} (u+j) = \frac{2}{3}\big((1-\beta+\delta_2)^2 + \delta_1(1-\beta+\delta_2) + \delta_1^2\big)m^3 + o(m^3),$$
$$s_{eM_2} = \sum_{(u,i)\in\mathcal{I}_{x1}} (m-u) + \sum_{(u,j)\in\mathcal{I}_{y1}} (m-u) = \frac{1}{6}(3-2\beta+4\delta_1+2\delta_2)\,m^3 + o(m^3)$$

となる．このとき，条件 $|\det \boldsymbol{B}_2|^{1/r} < (eM_2)^m$ を満たせば攻撃が成功する．条件を整理すると，

$$2\delta_1^2 + 2(1-\beta+\delta_2)\delta_1 + 2(1-\beta+\delta_2)^2 - (1+\delta_2) > 0$$

となる．この不等式を解くことによって，

$$\delta_1 > \frac{1}{2}\left(-1+\beta-\delta_2+\sqrt{-3(1-\beta+\delta_2)^2+2(1+\delta_2)}\right)$$

を得る．式 (4.9) で定めた k,τ が

$$-k/m \le \tau \le 0$$

を満たすとき，この攻撃は EJMW 攻撃の改良攻撃となっている．k,τ についてこの制約を整理すると，

$$\frac{1}{2} - \delta_1 + \delta_2 \le \beta \le \frac{1}{2} + \delta_2$$

となる． □

4.2.3 RSA に対する攻撃 3

RSA に対する攻撃 2 は $-1 \le \tau \le 0$ のとき成立するが，τ が

$$-1 \le \tau < -k/m$$

の範囲にあるときは，より良い条件のもとで成功する攻撃を構成することができる．RSA に対する攻撃 3 は，前章の式 (4.9) で定めた k,τ の値が $-1 \le \tau < -k/m$ を満たしているときにのみ成立する．

RSA に対する攻撃 2 と同様に，Coppersmith の手法を用いて，法付き方程式 $f_{eM_2}(x,y) = 0 \pmod{eM_2}$ の解 $(\tilde{x},\tilde{y}) = (\ell-\ell_0, -p-q+1)$ を求める．式 (4.1) で定めたものと同じ多項式 $g^{(x)}_{[u,i]}(x,y), g^{(y)}_{[u,j]}(x,y)$ を使って攻撃を構成するが，RSA に対する攻撃 2 とは別のインデックスを使う．k,s を $k<s$ なる正整数，τ を $-1 \le \tau \le -k/m$ なる実数とする．インデックスの集合 $\mathcal{I}_{x2}, \mathcal{I}_{y2}$ には，(3.4) と同じものを使う．$(u,i) \in \mathcal{I}_{x2}$ を満たす多項式 $g^{(x)}_{[u,i]}(x,y)$ と，$(u,j) \in \mathcal{I}_{y2}$ を満たす多項式 $g^{(y)}_{[u,j]}(x,y)$ を使う．

このような多項式と，変数 $w := \ell_0 + x$ を用いて行列 $\boldsymbol{B}_3$ を構成する．このとき行列 $\boldsymbol{B}_3$ は，補題 4.3 で示したものと同じ対角成分をもつ三角行列をなす．また，正整数 k，実数 τ を式 (4.9) と同様に

$$k = 2\delta_1 m, \quad \tau = 1 - 2\beta - 2\delta_1 + 2\delta_2$$

と定める．これは，補題 4.4 が，行列 $\boldsymbol{B}_3$ に対しても成り立つためである．

$\sigma := s/m$ とする．上で決められた k,τ の値によって構成される行列 $\boldsymbol{B}_3$ の次元 r は，

$$r = \sum_{(u,i)\in\mathcal{I}_{x2}} 1 + \sum_{(u,j)\in\mathcal{I}_{y2}} 1 = \left(\sigma - \frac{(\sigma-2\delta_1)^2}{2(2-2\beta-2\delta_1+2\delta_2)}\right) m^2 + o(m^2)$$

となる．$\det \boldsymbol{B}_3 = W^{s_W} X^{s_X} Y^{s_Y} (eM_2)^{s_{eM_2}}$ と表すと，これらはそれぞれ，

$$\begin{aligned}
s_W &= \sum_{(u,i)\in\mathcal{I}_{x2}} l_{k,\tau}(i) + \sum_{(u,j)\in\mathcal{I}_{y2}} l_{k,\tau}(u+j) \\
&= \left(\frac{(\sigma-2\delta_1)^2}{2(2-2\beta-2\delta_1+2\delta_2)} + \frac{(\sigma-2\delta_1)^3}{3(2-2\beta-2\delta_1+2\delta_2)^2} \right) m^3 + o(m^3), \\
s_X &= \sum_{(u,i)\in\mathcal{I}_{x2}} (u - l_{k,\tau}(i)) + \sum_{(u,j)\in\mathcal{I}_{y2}} (u - l_{k,\tau}(u+j)) \\
&= \left(\frac{\sigma}{2} - \frac{(\sigma-2\delta_1)^3}{6(2-2\beta-2\delta_1+2\delta_2)^2} \right) m^3 - s_W + o(m^3), \\
s_Y &= \sum_{(u,i)\in\mathcal{I}_{x2}} i + \sum_{(u,j)\in\mathcal{I}_{y2}} (u+j) \\
&= \left(\frac{\sigma^3 - 8\delta_1^3}{6(2-2\beta-2\delta_1+2\delta_2)} + \frac{\sigma^2}{2} \left(1 - \frac{\sigma-2\delta_1}{2-2\beta-2\delta_1+2\delta_2} \right) \right) m^3 + o(m^3), \\
s_{eM_2} &= \sum_{(u,i)\in\mathcal{I}_{x2}} (m-u) + \sum_{(u,j)\in\mathcal{I}_{y2}} (m-u) \\
&= \left(\sigma - \frac{\sigma^2}{2} + \frac{\sigma^3}{6} - \frac{(\sigma-2\delta_1)^2}{2(2-2\beta-2\delta_1+2\delta_2)} + \frac{(\sigma-2\delta_1)^3}{6(2-2\beta-2\delta_1+2\delta_2)^2} \right) m^3 + o(m^3)
\end{aligned}$$

となる．このとき，条件 $|\det \boldsymbol{B}_3|^{1/r} < (eM_2)^m$ を満たせば攻撃が成功する．条件を整理すると，

$$6(\beta-\delta_1)\sigma - 3(1+2\delta_2)\sigma^2 + 2(1+\delta_2)\sigma^3 < \frac{(\sigma-2\delta_1)^3}{2-2\beta-2\delta_1+2\delta_2}$$

を得る．この不等式の右辺を最大化するような σ は，

$$\sigma = 1 - \frac{2\beta - 2\delta_2 - 1}{1 - 2\sqrt{(1+\delta_2)(1-\beta-\delta_1+\delta_2)}}$$

となる．k, s, τ が

$$-1 \le \tau \le -k/m \quad \text{かつ} \quad k < s$$

を満たすとき，この攻撃は EJMW 攻撃の改良攻撃となり，かつ，RSA に対する攻撃 2 より良い攻撃となっている．k, τ についてこの制約を整理すると，

$$\frac{1}{2} + \delta_2 \le \beta \le \delta_1(4(1+\delta_2)(1-\delta_1) - 1)$$

となる．□

4.3　数値実験

本節では，既存攻撃と提案攻撃に対する数値実験の結果を述べる．この実験は，8GB のメモリを持つ 2.70GHz の Intel Core m5 を用いて行われた．また，各攻撃の実装には，NTL ライブラリのバージョン 11.3.2 を用い，C++ で実装した．

本実験では，秘密鍵の大きさが指定ビットサイズとなるように鍵生成をした，2048 ビットの合成数をもつ RSA 暗号を攻撃対象とする．このような RSA 暗号のサンプルを 50 組ずつ生成し，それぞれに $m = 2$ としたときの既存攻撃および提案攻撃を適用した．既存攻撃としては EJMW 攻撃と Sarkar の攻撃の自明な拡張を，提案攻撃としては RSA 暗号に対する攻撃 1 と 2 を実装した．各攻撃によってノルムの小さい多項式を生成できた場合を成功とし，50 組のサンプルのうち，それぞれの攻撃が成功したサンプルの数を数え，比較をした．

以下，実験結果を述べる．

表 4.6. $\beta = 0.3125$ のときの EJMW 攻撃の成功率

		$\delta_1 \log N$（ビット）					
		125	126	127	128	129	130
$\delta_2 \log N$（ビット）	125	0.00	0.00	0.02	0.10	0.22	0.36
	126	0.00	0.02	0.06	0.14	0.36	0.46
	127	0.04	0.08	0.14	0.32	0.50	0.80
	128	0.10	0.20	0.30	0.52	0.86	1.00
	129	0.24	0.32	0.46	0.86	1.00	1.00
	130	0.32	0.40	0.82	1.00	1.00	1.00

表 4.7. $\beta = 0.3125$ のときの提案攻撃（RSA 暗号に対する攻撃 1）の成功率

		$\delta_1 \log N$（ビット）					
		125	126	127	128	129	130
$\delta_2 \log N$（ビット）	125	0.00	0.0	0.02	0.12	0.22	0.38
	126	0.02	0.04	0.10	0.14	0.38	0.62
	127	0.04	0.10	0.16	0.32	0.60	0.88
	128	0.10	0.24	0.38	0.62	0.86	1.00
	129	0.18	0.28	0.50	0.88	1.00	1.00
	130	0.28	0.50	0.86	1.00	1.00	1.00

表 4.6，4.7 は，それぞれ EJMW 攻撃と，RSA 暗号に対する攻撃 1 の成功率を示したものである．これらは，640 ビット ($\beta = 0.3125$) の秘密鍵のうち，125〜130 ビットの上位ビットおよび下位ビット ($\delta_1, \delta_2 \approx 0.125$) の部分情報が得られた状況を攻撃対象とした．

また表 4.8，4.9 は，それぞれ Sarkar らの攻撃の自明な拡張と，RSA 暗号に対する攻撃 2 の成功率を示したものである．これらは，1152 ビット ($\beta = 0.5625$) の秘密鍵のうち，852〜857 ビットの上位ビットおよび 253〜258 ビットの下位ビット ($\delta_1 \approx 0.4, \delta_2 \approx 0.125$) の部分情報

表 4.8. $\beta = 0.5625$ のときの Sarkar らの攻撃の成功率

		$\delta_1 \log N$（ビット）					
		852	853	854	855	856	857
$\delta_2 \log N$（ビット）	253	0.00	0.00	0.04	0.08	0.28	0.86
	254	0.02	0.02	0.06	0.22	0.62	1.00
	255	0.02	0.06	0.16	0.38	0.92	1.00
	256	0.02	0.04	0.28	0.82	1.00	1.00
	257	0.04	0.26	0.66	1.00	1.00	1.00
	258	0.10	0.50	0.92	1.00	1.00	1.00

表 4.9. $\beta = 0.5625$ のときの提案攻撃（RSA 暗号に対する攻撃 2）の成功率

		$\delta_1 \log N$（ビット）					
		852	853	854	855	856	857
$\delta_2 \log N$（ビット）	253	0.00	0.00	0.04	0.08	0.60	1.00
	254	0.02	0.08	0.12	0.42	0.92	1.00
	255	0.04	0.08	0.36	0.70	1.00	1.00
	256	0.04	0.18	0.52	1.00	1.00	1.00
	257	0.08	0.26	0.92	1.00	1.00	1.00
	258	0.34	0.72	1.00	1.00	1.00	1.00

が得られた状況を攻撃対象とした．

これらの表から，得られた上位ビット，下位ビットが増えるごとに攻撃の成功率が上がっていくことが分かる．また，提案攻撃は既存攻撃よりも少ない部分情報で，多項式の生成に成功することが分かる．

第 5 章

一般化 RSA 暗号に対する部分鍵導出攻撃の改良

本章では，3.2 章で述べた一般化 RSA 暗号に対する既存の部分鍵導出攻撃の，改良攻撃を提案する．

5.1 改良攻撃

この章では，3 章および 4 章で述べた RSA 暗号に対する攻撃を，一般化 RSA 暗号に適用する．

$\delta_1 < 1$ のとき，以下の定理が成立する．

定理 5.1. (N, e) を公開鍵，d を秘密鍵とする *EQ-RSA* を考える．$e \approx N^2, d \approx N^\beta, \beta \leq 2$ とする．秘密鍵 d のうち，上位 $\delta_1 n$ ビットの値 $d_1 \approx N^{\delta_1}$ および下位 $\delta_2 n$ ビットの値 $d_2 \approx N^{\delta_2}$ が与えられたとする．$\delta_1 < 1$ とする．このとき，以下を満たすならば，N の入力長の多項式時間で N を素因数分解するアルゴリズムが存在する．

1. $\beta \leq \dfrac{9 - \sqrt{21}}{6}$ のとき，

$$\delta_1 + \delta_2 > \frac{1}{2}\left(-2 + \beta + \sqrt{-3(2-\beta)^2 + 8}\right)$$

2. $1 - \delta_1 + \delta_2 \leq \beta \leq 1 + \delta_2$ のとき，

$$\delta_1 > \frac{1}{2}\left(-2 + \beta - \delta_2 + \sqrt{-3(2 - \beta + \delta_2)^2 + 4(2 + \delta_2)}\right)$$

3. $1 + \delta_2 \leq \beta \leq 2 - \delta_1 + \delta_2 - (1 - \delta_1)^2(2 + \delta_2)$ のとき，

$$3(\beta - \delta_1)\sigma - 3(1 + \delta_2)\sigma^2 + (2 + \delta_2)\sigma^3 < \frac{(\sigma - \delta_1)^3}{2 - \beta - \delta_1 + \delta_2},$$

$$\sigma = 1 - \frac{\beta - \delta_2 - 1}{1 - \sqrt{(2 + \delta_2)(2 - \beta - \delta_1 + \delta_2)}}$$

4. $2-\delta_1+\delta_2-(1-\delta_1)^2(2+\delta_2) \le \beta \le \dfrac{11+16\delta_2+12\delta_2^2}{8+4\delta_2}$ のとき，

$$\delta_1 > \beta - \frac{3(1+\delta_2)^2}{4(2+\delta_2)}$$

5. $1 \le \delta_1$ のとき，

$$\delta_1+\delta_2 > \frac{2}{3}\left(\beta - 1 + \sqrt{\beta^2+\beta-2}\right)$$

$\dfrac{9-\sqrt{21}}{6} \le \beta \le 1-\delta_1+\delta_2$ のときは，3.2.2 節で紹介した条件 (3.7) が最も少ない部分情報で秘密鍵を復元できる攻撃となる．また，$\dfrac{11+16\delta_2+12\delta_2^2}{8+4\delta_2} < \beta$ かつ $\delta_1 < 1$ のときは，攻撃は成立しない．

定理 5.1 の条件 1 のときの攻撃を一般化 RSA に対する攻撃 1，条件 2 のときを一般化 RSA に対する攻撃 2，条件 3 のときの攻撃を一般化 RSA に対する攻撃 3，条件 4 のときの攻撃を一般化 RSA に対する攻撃 4，条件 5 のときの攻撃を一般化 RSA に対する攻撃 5 とする．

一般化 RSA に対する攻撃 1–4 の各攻撃構成は，4 章の各攻撃構成と同じである．また，一般化 RSA に対する攻撃 5 の攻撃構成は，[7] の 4.2 章および Appendix C で Ernst らが示した攻撃構成と同じである．

5.1.1　一般化 RSA に対する攻撃 1

多項式 $f_{eM_2}(x,y), f_e(x,y)$ をそれぞれ，3.2.1 節の式 (3.6) および (3.5) で定めたものとし，法付き方程式 $f_{eM_2}(x,y) = 0 \pmod{eM_2}$ および $f_e(x,y) = 0 \pmod{e}$ の解 $(\tilde{x},\tilde{y}) = (\ell-\ell_0, -p^2-q^2+1)$ を探す．

これ以降の攻撃構成は，4.2.1 節で述べた RSA に対する攻撃 1 の構成と同じである．

攻撃の成功条件は，

$$(\delta_1+\delta_2)^2 + (2-\beta)(\delta_1+\delta_2) + (2-\beta)^2 - 2 > 0$$

となる．この不等式を解くことによって，

$$\delta_1+\delta_2 > \frac{1}{2}\left(-2+\beta+\sqrt{-3(2-\beta)^2+8}\right)$$

を得る．この攻撃を成功させるための制約を整理すると，

$$\beta \le \frac{9-\sqrt{21}}{6}$$

となる．

5.1.2　一般化 RSA に対する攻撃 2

一般化 RSA に対する攻撃 2 の構成は，4.2.2 節で述べた RSA に対する攻撃 2 の構成と同じである．

攻撃の成功条件は，

$$\delta_1^2 + (2 - \beta + \delta_2)\delta_1 + (2 - \beta + \delta_2)^2 - (2 + \delta_2) > 0$$

となる．この不等式を解くことによって，

$$\delta_1 > \frac{1}{2}\left(-2 + \beta - \delta_2 + \sqrt{-3(2 - \beta + \delta_2)^2 + 4(2 + \delta_2)}\right)$$

を得る．この攻撃を成功させるための制約を整理すると，

$$1 - \delta_1 + \delta_2 \leq \beta \leq 1 + \delta_2$$

となる．

5.1.3 一般化 RSA に対する攻撃 3

一般化 RSA に対する攻撃 3 の構成は，4.2.3 節で述べた RSA に対する攻撃 3 の構成と同じである．

攻撃の成功条件は，実数 σ を用いて，

$$3(\beta - \delta_1)\sigma - 3(1 + \delta_2)\sigma^2 + (2 + \delta_2)\sigma^3 < \frac{(\sigma - \delta_1)^3}{2 - \beta - \delta_1 + \delta_2}$$

と表せる．この不等式の右辺を最大化するような σ は，

$$\sigma = 1 - \frac{\beta - \delta_2 - 1}{1 - \sqrt{(2 + \delta_2)(2 - \beta - \delta_1 + \delta_2)}}$$

となる．攻撃が成功するための制約を整理すると，

$$1 + \delta_2 \leq \beta \leq 2 - \delta_1 + \delta_2 - (1 - \delta_1)^2(2 + \delta_2)$$

となる．

5.1.4 一般化 RSA に対する攻撃 4

一般化 RSA に対する攻撃 4 の構成は，4.1 節で述べた RSA 暗号に対する Sarkar らの攻撃の自明な拡張の構成と同じである．

攻撃の成功条件は，

$$\delta_1 > \beta - \frac{3(1 + \delta_2)^2}{4(2 + \delta_2)}$$

となる．$\delta_1 \leq 1$ より，β の範囲は

$$\beta < \delta_1 + \frac{3(1 + \delta_2)^2}{4(2 + \delta_2)} \leq \frac{11 + 16\delta_2 + 12\delta_2^2}{8 + 4\delta_2}$$

となる．

5.1.5　一般化 RSA に対する攻撃 5

一般化 RSA に対する攻撃 5 の構成は，[7] の 4.2 章および Appendix C で Ernst らが示した攻撃構成と同じである．

攻撃の成功条件は，

$$\delta_1 + \delta_2 > \frac{2}{3}\left(\beta - 1 + \sqrt{\beta^2 + \beta - 2}\right)$$

となる．この攻撃は，

$$\delta_1 \geq 1$$

のとき成功する．

第 6 章

結論

本研究では，RSA 暗号について，秘密鍵 d の上位ビットと下位ビット両方から復元する手法を提案することによる，安全性解析を行った．本稿で攻撃対象としたのは，RSA 暗号および一般化 RSA 暗号である．

本論文では，RSA 暗号に対する安全性解析として，上位ビットと下位ビット両方が得られた状況における攻撃を提案した．さらに，数値実験によって，既存攻撃と提案攻撃は既存攻撃と比較して，より少ない部分情報で秘密鍵を復元できるを示した．提案攻撃は，同じ攻撃設定における先行研究である EJMW 攻撃と比較して，$N^{(7-2\sqrt{7})/6} < d < N$ の範囲でより良い攻撃となる．

また本論文では，一般化 RSA 暗号に対しても，同様の状況における攻撃を提案した．提案攻撃は，ZKH 攻撃と比較して，$N^{(7-2\sqrt{7})/3} < d < N^2$ の範囲で，より少ない部分情報で秘密鍵を復元することができる．

謝辞

本研究は，指導教員である國廣昇准教授と，東京大学大学院情報理工学系研究科の高安敦助教との共同研究となりました．國廣先生には，論文の書き方から研究方法に至るまで，さまざまなことをご指導していただきました．心より感謝いたします．また高安先生には，論文を書く上での改善点など，多くの有益な助言をいただきました．特に，自分の研究進捗のために，研究の打ち合わせという形でたくさんのお時間をいただきましたことを，本当に感謝しています．

また，研究室の方々には，自分のゼミ発表で，研究発表の際に注意すべき点などについてのコメントを多数いただき，発表に対する意識が変わりました．深く感謝いたします．

参考文献

[1] Aono Y. “A new lattice construction for partial key exposure attack for RSA.” Public Key Cryptography 2009. LNCS, vol. 5443, pp. 34–53. (2009)

[2] Blömer J., May A. “New partial key exposure attacks on RSA.” CRYPTO 2003. LNCS, vol. 2729, pp. 27–43. (2003)

[3] Boneh D., Durfee G. “Cryptanalysis of RSA with private key d less than $N^{0.292}$.” IEEE Trans. Information Theory 46(4), pp. 1339–1349. (2000)

[4] Coppersmith D. “Finding a small root of a univariate modular equation.” EUROCRYPT 1996. LNCS, vol. 1070, pp. 155–165 (1996)

[5] Coppersmith D. “Finding a small root of a bivariate integer equation; factoring with high bits known.” EUROCRYPT 1996. LNCS, vol. 1070, pp. 178–189 (1996)

[6] Elkamchouchi, H., Elshenawy, K., Shaban, H.: Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: ICCS 2002, vol. 1, pp. 9195. IEEE (2002)

[7] Ernst M., Jochemsz E., May A., de Weger B. “Partial key exposure attacks on RSA up to full size exponents.” EUROCRYPT 2005. LNCS, vol. 3494, pp. 371–386. (2005)

[8] Herrmann M., May A. “Attacking power generators using unravelled linearization: When do we output too much?” ASIACRYPT 2009. LNCS, vol. 5912, pp. 487–504. (2009)

[9] Herrmann M., May A. “Maximizing small root bounds by linearization and applications to small secret exponent RSA.” PKC 2010. LNCS, vol. 6056, pp. 53–69. (2010)

[10] Howgrave-Graham N. “Finding small roots of univariate modular equations revisited.” Cryptography and Coding 1997. LNCS, vol. 1355, pp. 131–142. (1997)

[11] Kuwakado, H., Koyama, K., Tsuruoka, Y.: New RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E78A(1), 2733. (1995)

[12] Lenstra A. K., Lenstra H. W. Jr., Lovász L. “Factoring polynomials with rational coefficients.” Mathematische Annalen. 261, pp. 515–534. (1982)

[13] May A. “New RSA vulnerabilities using lattice reduction methods.” University of Paderborn 2003. pp. 1–159 (2003)

[14] May A. “Using LLL-reduction for solving RSA and factorization problems.” The LLL Algorithm - Survey and Applications, Information Security and Cryptography, pp. 315–348 (2010)

[15] Rivest R., Shamir A., Adleman L. M. “A method for obtaining digital signatures and public-key cryptosystems.” Communications of the ACM, vol. 21(2), pp. 120–126. (1978)

[16] Sarkar S., Sen Gupta S., Maitra S. “Partial key exposure attack on RSA - Improvements for limited lattice dimensions.” INDOCRYPT 2010. LNCS, vol. 6498, pp. 2–16. (2010)

[17] Takayasu A., Kunihiro N. “Better lattice constructions for solving multivariate linear equations modulo unknown divisors.” IEICE Transactions, 97-A(6), pp. 1259–1272. (2014)

[18] Takayasu A., Kunihiro N. “Partial key exposure attacks on RSA: Achieving the Boneh-Durfee bound.” Selected Areas in Cryptogaphy 2014. LNCS, vol. 8781, pp. 345–362. (2014)

[19] Zheng M., Kunihiro N., Hu H. “Cryptanalysis of RSA Variants with Modified Euler Quotient.” AFRICACRYPT 2018. LNCS, vol 10831, pp. 266–281. (2018)