博士論文 (要約)

Efficient Constructions of Cryptographic Schemes and Generic Techniques for Security Enhancement (効率的な暗号方式の設計と，安全性を高めるための汎用的技術の研究)

山田翔太

Abstract

Cryptographic primitives enable secure transmission and integrity of data, access control to data, and so on. In order to be used in the real world, a cryptographic scheme should be efficient and secure enough. Many research has been dedicated to provide more efficient and secure schemes. We put forward research in this direction.

First our focus is constructions of cryptographic schemes that can be used in settings where saving transmission costs is a primary issue. In such settings, one would like to use a public key encryption scheme or a digital signature scheme with short ciphertexts or signatures even if they are not efficient enough in other aspects. Some previous works provide public key encryption schemes with very short ciphertexts and digital signature schemes with very short signatures aiming at being used in such settings. While the size of the ciphertexts/signatures are very compact, these schemes often require prohibitively long public keys. Due to this problem, they are not practical. We introduce novel techniques to reduce the public key size of the previous schemes without increasing the size of ciphertexts or signatures. Our proposed schemes drastically reduce the public key size at the cost of higher computational cost.

Second our focus is constructions of cryptographic schemes with high security. Especially, we study constructions of predicate encryption scheme with high security. Predicate encryption is a generalized form of public key encryption and provides fine-grained access control to a ciphertext. Compared to more basic primitives such as public key encryption and identity-based encryption, only few effort has been spent to construct predicate encryption schemes with high security. To remedy this situation, we propose a new generic conversion that converts any predicate encryption scheme with certain property that is secure against chosen plaintext attack into one that is secure aginst chosen ciphertext attack (CCA). By applying this conversion to existing schemes, we obtain new CCA-secure predicate encryption schemes. Moreover, we can use the resulting scheme to construct a new primitive that we call deniable anonymous predicate authentication scheme.

Contents

Chapter 0

Some Remarks

This is a summary of the dissertation. We cannot make all of the contents public because of the copyright policy issues. Full text will be available once permission is obtained from the publisher. The dissertation is organized by the following 6 chapters.

Chapter 1 Introduction
Chapter 2 Preliminaries
Chapter 3 New Schemes in the Bilinear Group Settings
Chapter 4 New Signature Schemes in the RSA Group Settings
Chapter 5 Generic Security Enhancement Technique for Predicate Encryption Schemes
Chapter 6 Concluding Remarks and Open Questions

This summary only contains Chap. 1 and 6. One can find similar contents to that of chapter 2 in [64, 63, 62], that of Chap. 3 in [64, 63], 4 in [63], and 5 in [62].

Chapter 1

Introduction

1.1 Overview and Motivations

Cryptographic primitives ensure secure transmission and integrity of data, access control to data, and so on. There are many cryptographic primitives and each has different functionality. Some of them have been used in practice and they are indispensable to realizing electronic society. At first, we explain several important cryptographic primitives related to this dissertation here.

Digital Signatures. The notion of digital signature was first proposed by Diffie and Hellman [22]. Digital signature schemes are digital analogue of signatures in the sense that it ensure integrity of digital data. That is, a valid signature on a digital text can only be generated by a specific user who has a secret key corresponding to a public key. First concrete construction (with weak security) of digital signature scheme was given by Rivest, Shamir, and Adleman [54] using multiplicative group of integer modulo N where N is product of two large primes (RSA group).

Public Key Encryption. The paper written by Diffie and Hellman [22] was the first to propose the notion of public key encryption. Public key encryption schemes ensure secure transmission of digital data *without sharing secret information between the sender and the reciever*. Anyone can encrypt a message to a user by using a public key of the user. But only the user who has secret key corresponding to the public key can decrypt the ciphertext and retrieve the message. This is very different from secret key encryption schemes that require sharing of secret information (i.e., secret key) between sender and reciever before starting communication. First concrete construction of public key encryption scheme were published by Rivest, Shamir, and Adleman [54] using RSA group. We note that nowadays, it is known that James H. Ellis, Clifford Cocks, and Malcolm Williamson at the Government Communications Headquarters in the UK secretly developed similar notion and construction before the publication of above papers.

Identity Based Encryption. One of main concern in using public key encryption in the real world is that malicious user would replace a public key of a honest user with a fake public key that is generated by himself. Then, a message for the honest user will be encrypted under the fake public key. The malicious user can decrypt the ciphertext

because the fake public key is generated by himself (possibly along with secret key). The problem is that there is no way to check whether a public key really corresponds to a user whom one intends to send a message or not. To resolve this problem, Shamir proposed the notion of identity based encryption (IBE) [57]. In IBE, a public key of a user corresponds to the unique identity of the user in the system and thus the concern we explained above does not arise. After the proposal of the notion of IBE, concrete construction had been left open for about twenty years. First constructions of IBE were proposed by Sakai, Ohgishi, and Kasahara [56] and Boneh and Franklin [10] independently.

Predicate Encryption. The notion of predicate encryption (PE) is proposed by [55] and it is an extension of identity-based encryption. In PE, a ciphertext/private key is associated with certain attribute X/Y. The decryption is possible if X and Y satisfy certain relation $f(X, Y) = 1$. IBE is captured as a special case of PE in which f is an equality checking function (i.e., $f(X, Y) = 1$ iff $X = Y$). In PE with more expressive relation f, a user can encrypt a message for fine-grained condition. For example, in an attribute-based encryption scheme, which is an instance of PE, one can encrypt a message for a Boolean formula. Large amount of PE schemes have been proposed aiming at realizing more complex access structure (or relation f) [11, 55, 32, 8, 31, 41, 12, 4, 46, 50, 59, 29, 30].

One of important research directions in the area of cryptography is to construct efficient cryptograhpic schemes. Especially, improving the efficiency of basic cryptographic primitives such as public key encryption and digital signature is very important. The reason of this is that basic primitives are used more often than complex primitives in the real world. Another reason is that they are often used as building block to construct more complex primitives such as group signature schemes [6, 7]. Such schemes become more efficient if the efficiency of underlying basic primitives are improved.

Another important research direction is to construct schemes with higher security. Since the techniques to attack systems in the real world are continuously improving, we should prepare for such attacks by constructing schemes with high security. One remarkable example of this is Bleichenbacher's attack [9]. He demonstrated that PKCS ♯1 can be broken by executing chosen ciphertext attack (CCA) [49, 53, 24] by exploiting a certain property of the system. The CCA is an attack in which the adversary can access an oracle that decrypts any ciphertexts other than the one the adversary tries to break. His result was surprising, because CCA was not considered to be a threat to systems in the real world. Since then, CCA-security has been considered to be "golden standard" for secure public key encryption and constructions that satisfy the security notion have been studied extensively [19, 20, 15, 44, 14, 16, 33, 38, 1, 35].

In this dissertation, we focus on the above two topics. Namely, the constructions of efficient cryptographic schemes and schemes with higher security. Especially, we mainly studied signature schemes with short signatures and predicate encryption schemes with higher security. We also obtained some other results related to these topics as explained in the next section.

1.2 Summary of Contributions

Our contributions can be divided into two parts.

- At first, we focus on how to construct efficient cryptogtaphic primitives. Especially, we study construction of digital signature with short signatures and public key encryption with short ciphertexts. Such schemes would be important in the settings where the transmission cost are very restricted. There are some previous works on the topic [18, 37, 36]. They achieve very short signatures/ciphertexts whereas the public key size is very large. Due to the large public key size, they are impractical. Thus, it would be desireble to obtain schemes with the same size of ciphertexts/signatures and short public keys. To achieve this goal, we introduce some new techniques and construct schemes that achieve the same size of ciphertexts/signatures and shorter public keys as we explain below.

  Two Dimensional Representation of a Cover Free Family. The cover free family [25] is a combinatorial object and often used as a building block to construct a cryptographic primitives [23, 51, 18, 42, 65, 36]. In Chap. 3, we introduce slight twist to the use of cover free family. We call this as "two-dimensional representation of a cover free family". Combining this technique with a power of the bilinear map, we can construct new q-resilient IBE. A q-resilient IBE scheme is IBE scheme that is secure under the situation where the number of malicious users is bounded by q. The scheme has optimal ciphertext overhead, i.e., only consists of one group element, and relatively short public key size. Applying Canetti-Halevi-Katz transform [15, 14] to the scheme, we obtain a new public key encryption scheme that is q-bounded CCA-secure. A q-bounded CCA-security is weaker notion than CCA-security in the sense that the security is only guaranteed when the adversary access the decryption oracle less than q times. The ciphertext overhead of the resulting scheme is optimal and the public key size is much shorter than the scheme in [18] that achieves the same size of ciphretexts and security. On the other hand, we can obtain a new q-time signature with very short signature size by applying the Naor transformation [10, 21] to our q-resilient IBE scheme. A q-time signature scheme is a signature scheme that the security of the scheme is guaranteed only when signer generates signatures less than q times. The public key size of the resulting scheme is shorter than the previous scheme [65] that achieves the same size of signatures and security.

  New Technique to Construct Short Signatures and Its Realization in Bilinear Groups. In Chap. 3, we also introduce another technique. We observe that combination of a q-time signature and a weakly secure signatures would yield a (full-fuledged) short signature scheme. This can be seen as an extension of the previous result [43, 58] that construct a full-fuledged signature from a one-time signature (or chameleon hash that is closely related to one-time signature) and a weakly secure signature. This is only an informal idea and we do not have any

formal framework to explain this, but the idea has some possiblity to construct new and efficient signature schemes. Actually, we construct new signature scheme in the bilinear groups with the shortest signature size in the literature based on the idea. The public key size of the scheme is much shorter (about 1/100 in a typical parameter setting) than the previous scheme in [36] that achieves the same size of signatures as ours. While our scheme provides much better space efficiency than the scheme in [36], the computational cost of our scheme is higher.

Realization in RSA Groups. In the above, we showed that our technique of constructing signature scheme from a weakly secure signature scheme and q-time signature is useful in the settings where groups that are equipped with bilinear maps are available. We further demonstrate that our technique is useful to construct short signature schemes even in other settings. In Chap. 4, we construct various signature schemes from the RSA assumption with short signatures. Conceptually, we construct the schemes in two steps. First, we construct new q-time signatures. Then, we combine these schemes with known weakly secure signature scheme from [40] using algebraic structure. Resulting new schemes are space efficient. For example, one of our schemes achieve the shortest signature size and public key size simultaneously. On the other hand, computational cost of our schemes are rather high.

- Secondly, we focus on constructions of predicate encryption (PE) schemes that achieve CCA-security. As we explained in Sec. 1.1, large amount of studies are devoted to widen the expressibility of access structure in predicate encryption scheme. However, most of previous proposed schemes only achieve chosen plaintext security, which is much weaker security than CCA-security. (There are some exceptions such as [50].)

  Generic Constructions of CCA-Secure PE. To remedy the situation that we explained above, we propose a new generic conversion that converts any chosen plaintext secure PE scheme with certain natural property into CCA-secure one. Since many existing schemes [11, 32, 8, 41, 12, 4, 5, 46, 50] have this property or can be modified to have this property, we can apply this conversion to obtain chosen ciphertext secure version of these PE schemes. There are similar results in the literature [37, 61], but they are only applicable to specific PE such as broadcast encryption scheme and attribute based encryption scheme. Our conversion technique is an extension of their technique and can be applied to wider range of PE schemes.

  Anonymous Deniable Predicate Authentication. We also demonstrate that CCA-secure PE schemes obtained by the above conversion can be used to construct new cryptographic primitive that we call anonymous deniable predicate authentication (ADPA). ADPA is an extension of authentication scheme. In ADPA, a user is associated with an attribute X and he can convince verifier that he has an attribute X' such that $f(X', Y) = 1$ for any Y that satisfies $f(X, Y) = 1$ without revealing the actual value of X. Furthermore, he can deny the fact that he has interacted

with the verifier. This property would be useful in the settings where one would like to leak an information about some company or organization without revealing much information about him, but at the same time he wants to convince someone that the information is reliable.

Chapter 6

Concluding Remarks and Open Questions

In the first half of this dissertation, we introduce some new techniques and construct new public key encryption schemes and signature schemes. Especially, we show that combination of q-time signature schemes and weakly secure signature schemes yield short signature schemes. There are some interesting open questions regarding efficient construction of public key encryption schemes and signatures.

- First question is that whether it is possible to construct a CCA-secure (not bounded CCA secure) public key encryption scheme with shorter ciphertext than [14] using only mild assumption. Regarding this question, there are some possibility and impossibility results. The result in [34] says that it is impossible to construct such a scheme within certain class. Other recent results [27, 39] indicate that one can construct $(\mathsf{poly}, 1)$-programmable hash function (or full domain hash). Using their results, we can immediately obtain a CCA-secure public key encryption scheme whose ciphertext overhead consists of only one group element. However, their construction of $(\mathsf{poly}, 1)$-programmable hash function needs multi linear map [28, 17]. Since current constructions of multi linear map are not efficient and need seemingly very strong number theoretic assumption, this is not a satisfactory answer to the question.
- Second question is whether it is possible to construct a signature scheme with even shorter signature size in the standard model. In the random oracle model, it is possible to construct a signature scheme with signatures that is even shorter than the length of the RSA composite number under the factoring assumption [52, 48]. It would be interesting to try to relaize similar scheme in the standard model.

In the second half of this dissertation, we show that it is possible to enhance the security of several CPA-secure PE schemes to CCA one. Furthermore, we also show that it is possible to transform the resulting scheme to a new cryptographic primitive that we call anonymous deniable predicate authentication scheme. There are some open questions related to our result.

- The first question is whether there is more generic conversion from CPA-secure PE schemes to CCA one. Even if our conversion can be applied to wide range of existing schemes, it does not seem to be applicable to PE schemes based on lattices [3, 2, 13, 60, 30]. It would be an interesting open problem to generalize our result so that it can be applied to such schemes.
- The second question is whether it is possible to construct a PE scheme with even higher security such as security against chosen ciphertext selective opening attack [26] and leakage resilient security. Regarding this question, there are some important progress [47, 45].

Acknowledgement

Firstly I would like to thank my supervisor, Associate Professor Noboru Kunihiro, and Professor Hirosuke Yamamoto for their creative comments on the research and encouragement during my studies. Noboru Kunihiro also gave me a chance to join the summer intern at NTT.

I would like to thank previous and current member of Yamamoto-Kunihiro laboratory, Junya Honda, Tomoki Kubo, Yohei Taniguchi, Yuito Kikuchi, Takeaki Harima, Kunihiko Harada, Yu Nureki, Shunji Kinoshita, Yasuki Fukahori, Keishi Okudera, Shogo Takahashi, Elliot Taniguchi, Kenji Hamano, Shuhei Kotani, Yui Taniguchi, Haoji Chen, Yasuaki Miyazaki, Akari Sato, Kota Katagiri, Keita Tomokuni, Stefan Skudlarek, Yuta Ohashi, Motoki Nagata, Yuji Ono, Kaori Tosu, Yutaka Kawai, Jun Kogure, Takuya Matsumoto, Sigeru Maya, Yoshitaka Murai, Kosuke Yato, Gyoho Ei, Takayuki Kawai, Takahisa Suzuki, Yuto Sogo, Yuji Nagashima, Masayuki Yoshino, Toru Akishita, Masashi Ueda, Atsushi Takayasu, Kosei Endo, Takashi Yamakawa, Takuma Koyama, Tomohiro Nakata, Yuka Kuwaori, Ko Sugimoto, Yuki Takahashi, Yuho Matsunaga, Yoshinao Uchide, Vannet Thomas Francis, and Weilun liu for discussion on study and enjoyable talk. I also would like to thank previous and current secretary of the laboratory, Takako Ohashi and Chihiro Sakakibara for their help.

I would like to thank all researchers with whom I worked with: Goichiro Hanaoka, Koji Nuida, Nuttapong Attrapadung, Takahiro Matsuda, Bagus Santoso, Jacob Schuld, Hajime Watanabe, (They are/were from AIST or its predecessor RCIS), Keita Emura (from NICT), Go Ohtake, Yuki Hironaka, Kenjiro Kai, Yosuke Endo (from NHK science and technology research laboratory), Kohei Kasamatsu, Professor Hideki Imai (from the Chuo University). Interaction with them were exciting and productive. I also thank the members of Shin-Akarui-Angou-Benkyou-Kai for interesting discussions.

I would like to thank members of NTT secure Platform Laboratories for accepting me as an internship student. Especially, I thank to Keita Xagawa, the mentor, for helpful discussion and encouragement in the summer intern.

All results presented in this dissertation is supported by Research Fellowships of Japan Society for the Promotion of Science for Young Scientists. Finally, I would like to thank my parents and our cat for their understanding and encouragement.

Bibliography

[1] Masayuki Abe, Yang Cui, Hideki Imai, and Eike Kiltz. Efficient hybrid encryption from id-based encryption. *Des. Codes Cryptography*, Vol. 54, No. 3, pp. 205–240, 2010.

[2] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck Wee. Functional encryption for threshold functions (or fuzzy ibe) from lattices. In *Public Key Cryptography*, pp. 280–297, 2012.

[3] Shweta Agrawal, David Mandell Freeman, and Vinod Vaikuntanathan. Functional encryption for inner product predicates from learning with errors. In *ASIACRYPT*, pp. 21–40, 2011.

[4] Nuttapong Attrapadung and Benoît Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In *Public Key Cryptography*, pp. 384–402, 2010.

[5] Nuttapong Attrapadung, Benoît Libert, and Elie de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *Public Key Cryptography*, pp. 90–108, 2011.

[6] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT*, pp. 614–629, 2003.

[7] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA*, pp. 136–153, 2005.

[8] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[9] Daniel Bleichenbacher. Chosen ciphertext attacks against protocols based on the rsa encryption standard pkcs #1. In *CRYPTO*, pp. 1–12, 1998.

[10] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO*, pp. 213–229, 2001.

[11] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO*, pp. 258–275, 2005.

[12] Dan Boneh and Michael Hamburg. Generalized identity based and broadcast encryption schemes. In *ASIACRYPT*, pp. 455–470, 2008.

[13] Xavier Boyen. Attribute-based functional encryption on lattices. In *TCC*, pp. 122–142, 2013.

[14] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identity-based techniques. In *ACM Conference on Computer and Communications*

Security, pp. 320–329, 2005.

[15] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. In *EUROCRYPT*, pp. 207–222, 2004.

[16] David Cash, Eike Kiltz, and Victor Shoup. The twin diffie-hellman problem and applications. In *EUROCRYPT*, pp. 127–145, 2008.

[17] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In *CRYPTO (1)*, pp. 476–493, 2013.

[18] Ronald Cramer, Goichiro Hanaoka, Dennis Hofheinz, Hideki Imai, Eike Kiltz, Rafael Pass, Abhi Shelat, and Vinod Vaikuntanathan. Bounded cca2-secure encryption. In *ASIACRYPT*, pp. 502–518, 2007.

[19] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO*, pp. 13–25, 1998.

[20] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT*, pp. 45–64, 2002.

[21] Yang Cui, Eiichiro Fujisaki, Goichiro Hanaoka, Hideki Imai, and Rui Zhang 0002. Formal security treatments for ibe-to-signature transformation: Relations among security notions. *IEICE Transactions*, Vol. 92-A, No. 1, pp. 53–66, 2009.

[22] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644–654, 1976.

[23] Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung. Key-insulated public key cryptosystems. In *EUROCRYPT*, pp. 65–82, 2002.

[24] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *STOC*, pp. 542–552, 1991.

[25] Péter L. Erdös, Peter Frankl, and Zoltán Füredi. Families of finite sets in which no set is covered by the union of two others. *J. Comb. Theory, Ser. A*, Vol. 33, No. 2, pp. 158–166, 1982.

[26] Serge Fehr, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Encryption schemes secure against chosen-ciphertext selective opening attacks. In *EUROCRYPT*, pp. 381–402, 2010.

[27] Eduarda S. V. Freire, Dennis Hofheinz, Kenneth G. Paterson, and Christoph Striecks. Programmable hash functions in the multilinear setting. In *CRYPTO (1)*, pp. 513–530, 2013.

[28] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In *EUROCRYPT*, pp. 1–17, 2013.

[29] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In *CRYPTO (2)*, pp. 479–499, 2013.

[30] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In *STOC*, pp. 545–554, 2013.

[31] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. Bounded ciphertext policy attribute based encryption. In *ICALP (2)*, pp. 579–591, 2008.

[32] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based en-

cryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[33] Goichiro Hanaoka and Kaoru Kurosawa. Efficient chosen ciphertext secure public key encryption under the computational diffie-hellman assumption. In *ASIACRYPT*, pp. 308–325, 2008.

[34] Goichiro Hanaoka, Takahiro Matsuda, and Jacob C. N. Schuldt. On the impossibility of constructing efficient key encapsulation and programmable hash functions in prime order groups. In *CRYPTO*, pp. 812–831, 2012.

[35] Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, and Victor Shoup. Simple and efficient public-key encryption from computational diffie-hellman in the standard model. In *Public Key Cryptography*, pp. 1–18, 2010.

[36] Dennis Hofheinz, Tibor Jager, and Eike Kiltz. Short signatures from weaker assumptions. In *ASIACRYPT*, pp. 647–666, 2011.

[37] Dennis Hofheinz and Eike Kiltz. Programmable hash functions and their applications. In *CRYPTO*, pp. 21–38, 2008.

[38] Dennis Hofheinz and Eike Kiltz. Practical chosen ciphertext secure encryption from factoring. In *EUROCRYPT*, pp. 313–332, 2009.

[39] Susan Hohenberger, Amit Sahai, and Brent Waters. Replacing a random oracle: Full domain hash from indistinguishability obfuscation. *IACR Cryptology ePrint Archive*, Vol. 2013, p. 509, 2013.

[40] Susan Hohenberger and Brent Waters. Short and stateless signatures from the rsa assumption. In *CRYPTO*, pp. 654–670, 2009.

[41] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pp. 146–162, 2008.

[42] Jonathan Katz and Vinod Vaikuntanathan. Signature schemes with bounded leakage resilience. In *ASIACRYPT*, pp. 703–720, 2009.

[43] Hugo Krawczyk and Tal Rabin. Chameleon signatures. In *NDSS*, 2000.

[44] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In *CRYPTO*, pp. 426–442, 2004.

[45] Kaoru Kurosawa and Le Trieu Phong. Leakage resilient ibe and ipe under the dlin assumption. In *ACNS*, pp. 487–501, 2013.

[46] 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 *EUROCRYPT*, pp. 62–91, 2010.

[47] Allison B. Lewko, Yannis Rouselakis, and Brent Waters. Achieving leakage resilience through dual system encryption. In *TCC*, pp. 70–88, 2011.

[48] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *ASIACRYPT*, pp. 598–616, 2009.

[49] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *STOC*, pp. 427–437, 1990.

[50] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with

general relations from the decisional linear assumption. In *CRYPTO*, pp. 191–208, 2010.

[51] Josef Pieprzyk, Huaxiong Wang, and Chaoping Xing. Multiple-time signature schemes against adaptive chosen message attacks. In *Selected Areas in Cryptography*, pp. 88–100, 2003.

[52] David Pointcheval. The composite discrete logarithm and secure authentication. In *Public Key Cryptography*, pp. 113–128, 2000.

[53] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *CRYPTO*, pp. 433–444, 1991.

[54] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, Vol. 21, No. 2, pp. 120–126, 1978.

[55] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *EUROCRYPT*, pp. 457–473, 2005.

[56] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing over elliptic curve. In *The 2001 Symposium on Cryptography and Information Security*, 2001. (in Japanese).

[57] Adi Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pp. 47–53, 1984.

[58] Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In *CRYPTO*, pp. 355–367, 2001.

[59] Brent Waters. Functional encryption for regular languages. In *CRYPTO*, pp. 218–235, 2012.

[60] Keita Xagawa. Improved (hierarchical) inner-product encryption from lattices. In *Public Key Cryptography*, pp. 235–252, 2013.

[61] Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro. Generic constructions for chosen-ciphertext secure attribute based encryption. In *Public Key Cryptography*, pp. 71–89, 2011.

[62] Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Jacob C. N. Schuldt, Goichiro Hanaoka, and Noboru Kunihiro. Verifiable predicate encryption and applications to cca security and anonymous predicate authentication. In *Public Key Cryptography*, pp. 243–261, 2012.

[63] Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Space efficient signature schemes from the rsa assumption. In *PKC*, 2012.

[64] Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Two-dimensional representation of cover free families and its applications: Short signatures and more. In *CT-RSA*, pp. 260–277, 2012.

[65] G.M. Zaverucha and D.R. Stinson. Short one-time signatures. Cryptology ePrint Archive, Report 2010/446, 2010. `http://eprint.iacr.org/`.

List of Publications Related to the Dissertation

Refereed Conference Papers (with Formal Proceedings)

1. Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Space efficient signature schemes from the rsa assumption. In *Public Key Cryptography*, pp. 102–119, 2012.
2. Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Jacob C. N. Schuldt, Goichiro Hanaoka, and Noboru Kunihiro. Verifiable predicate encryption and applications to cca security and anonymous predicate authentication. In *Public Key Cryptography*, pp. 243–261, 2012.
3. Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Two-dimensional representation of cover free families and its applications: Short signatures and more. In *CT-RSA*, pp. 260–277, 2012.

List of All Publications

Journal Papers

1. Shota Yamada, Yutaka Kawai, Goichiro Hanaoka, and Noboru Kunihiro. Public key encryption schemes from the (b)cdh assumption with better efficiency. *IEICE Transactions*, 93-A(11):1984–1993, 2010.

Refereed Conference Papers (with Formal Proceedings)

1. Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, Noboru Kunihiro. A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption. In *Public Key Cryptography*, pp. ???-???, 2014. (To Appear)
2. Go Ohtake, Yuki Hironaka, Kenjiro Kai, Yosuke Endo, Goichiro Hanaoka, Hajime Watanabe, Shota Yamada, Kohei Kasamatsu, Takashi Yamakawa, and Hideki Imai. Partially wildcarded attribute-based encryption and its efficient construction. In *SECRYPT*, pp. 339–346, 2013. (Short Paper)
3. Keita Emura, Goichiro Hanaoka, Go Ohtake, Takahiro Matsuda, and Shota Yamada. Chosen ciphertext secure keyed-homomorphic public-key encryption. In *Public Key Cryptography*, pp. 32–50, 2013.
4. Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Space efficient signature schemes from the rsa assumption. In *Public Key Cryptography*, pp. 102–119, 2012. (辻井重男セキュリティ学生論文賞受賞)
5. Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Jacob C. N. Schuldt, Goichiro Hanaoka, and Noboru Kunihiro. Verifiable predicate encryption and applications to cca security and anonymous predicate authentication. In *Public Key Cryptography*, pp. 243–261, 2012.
6. Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Two-dimensional representation of cover free families and its applications: Short signatures and more. In *CT-RSA*, pp. 260–277, 2012.
7. Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro. Generic constructions for chosen-ciphertext secure attribute based encryption. In *Public Key Cryptography*, pp. 71–89, 2011.
8. Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. Toward an easy-to-understand structure for achieving chosen ciphertext security from the decisional diffie-hellman assumption. In *ProvSec*, pp. 229–243, 2010.

Non-Refereed Papers

1. アッタラパドゥン・ナッタポン，花岡悟一郎, 小川一人，大竹剛，渡辺創，山田翔太，“暗号文区間属性ベース暗号”2014 年暗号と情報セキュリティシンポジウム (SCIS2014), 2E4-1, 鹿児島, 2014 年 1 月.
2. アッタラパドゥン・ナッタポン，花岡悟一郎, 小川一人，大竹剛，渡辺創，山田翔太，“区間属性ベース暗号の一般的構成”2014 年暗号と情報セキュリティシンポジウム (SCIS2014), 2E4-2, 鹿児島, 2014 年 1 月.
3. 山川高志, 山田翔太, 花岡悟一郎, 國廣昇, “セミスムース数を用いた損失落とし戸関数の構成” 2014 年暗号と情報セキュリティシンポジウム (SCIS2014), 3E2-1, 鹿児島, 2014 年 1 月.
4. 山田翔太, 花岡悟一郎, 國廣昇, “損失的代数フィルターのより効率的な構成,” 2013 年暗号と情報セキュリティシンポジウム (SCIS2013), 2A3-3, 京都, 2013 年 1 月.
5. 山川高志, 山田翔太, 花岡悟一郎, 國廣昇, “素因数分解問題に基づく Semi-smooth 部分群上の CCA 安全な公開鍵暗号の安全性証明について,” 2013 年暗号と情報セキュリティシンポジウム (SCIS2013), 4B1-1, 京都, 2013 年 1 月.
6. 大竹剛, 広中悠樹, 加井謙二郎, 遠藤洋介, 花岡悟一郎, 渡辺創, 山田翔太, 笠松宏平, 山川高志, 今井秀樹, “Wildcard を部分的に許す効率的な属性ベース暗号の構成に関する検討,” 2013 年暗号と情報セキュリティシンポジウム (SCIS2013), 3F4-3, 京都, 2013 年 1 月.
7. 江村恵太, 花岡悟一郎, 松田隆宏, 大竹剛, 山田翔太, “選択暗号文攻撃者に対し安全な準同型暗号,” 2012 年暗号と情報セキュリティシンポジウム (SCIS2012), 2A1-6, 金沢, 2012 年 1 月.（口頭発表, 査読なし）(イノベーション論文賞受賞)
8. 山田翔太, 花岡悟一郎, 國廣昇, “カバーフリーファミリーの二次元的表現法に基づく公開鍵が短い署方式のよりタイトな帰着,” 2012 年暗号と情報セキュリティシンポジウム (SCIS2012), 4A2-3, 金沢, 2012 年 1 月.
9. 山田翔太, ナッタポン・アッタラパドゥン, 花岡悟一郎, 國廣昇, “CCA 安全な属性ベース暗号の一般的構成,” 2011 年暗号と情報セキュリティシンポジウム (SCIS2011), 2A4-4, 小倉, 2011 年 1 月.
10. 山田翔太, 川合豊, 花岡悟一郎, 國廣昇, “鍵サイズの小さい (B)CDH 仮定に基づく暗号方式の提案,” 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 1A1-5, 高松, 2010 年 1 月. (SCIS 論文賞受賞)

Posters

1. Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro. New Security Proof for a Variant of the BGW Broadcast Encryption Scheme. In *IWSEC*, 2013. (Best Poster Award)