Methodology for designing cryptographic systems with advanced functionality based on a modular approach

— Towards reducing the barrier to introducing newly-designed cryptographic schemes into real-world systems —

Goichiro HANAOKA[1]*, Satsuya OHATA[1, 2], Takahiro MATSUDA[1], Koji NUIDA[1] and Nuttapong ATTRAPADUNG[1]

[Translation from *Synthesiology*, Vol.7, No.2, p.93-104 (2014)]

In this article, we point out that in general, newly-designed highly functional cryptographic schemes have significantly complicated structures that hinder user understanding. Furthermore, this fact may prevent these new technologies from being introduced into real world systems. We propose a new methodology for overcoming this barrier. We take proxy re-encryption as an example, and discuss how the barrier to user understanding is reduced by our proposed methodology.

Keywords : Public-key cryptosystems, digital signature, proxy re-encryption, provable security, standardization

1 Introduction

1.1 Background and Motivation

Background

With the advancement of the network society, new advanced or highly functional cryptographic schemes are being designed to provide secure information services that are becoming ever complex, as exemplified by cloud storage. One representative example of such highly functional cryptographic schemes is proxy re-encryption.[1]

In proxy re-encryption, the sender designates a receiver and conducts encryption. Then the server called “proxy” can re-designate a different receiver without conducting decryption. By using this technology, data access is allowed to an indefinite number of authorized users, while viewing by any unauthorized user can be prevented. For example, one may wish to encrypt and protect the electronic charts used at hospitals because they contain private information, but the information must be shared when the patient is transferred to another residence or hospital, and proxy re-encryption will be significantly useful in such a situation.

However, although such highly functional cryptographic schemes including proxy re-encryption are expected to provide high security and convenience, it is not easy to intuitively understand the security and functionalities due to their complex construction. For example, four papers on highly functional cryptographic schemes were published at the CRYPTO 2012, which is the most authoritative international conference on cryptology, and the papers were on average 34 pages long of which on average 24 pages were devoted to security definitions and security proofs. The contents are lists of difficult-to-understand mathematical formulas, and it is not easy to understand the correlation between these formulas and actual security. This is thought to be the major barrier in introducing highly functional cryptographic schemes to the real world. Particularly, even specialized researchers find it difficult to be convinced of the security, and a general user cannot be expected to use these schemes with full confidence. In fact, error in proof is often discovered later, even with cryptographic schemes that the designers have claimed that their security has been mathematically proven. Hereinafter, this problem will be called *the security verification problem* in cryptographic schemes.

Motivation

In light of the above situation, this paper addresses the methodology to promote the introduction of a new highly functional cryptographic scheme with complex functions to the real world. Particularly, we propose a design principle to simplify the understanding of the security of the cryptographic schemes where the security verification tends to be complex and difficult for the researchers and engineers who are not specialists of the field. Specifically, we indicate the importance of breaking down the needed functionalities before engaging in design and describing them by the combination of simple functionalities as much as possible, rather than conducting scratch development[Term] for highly functional cryptographic schemes with complex functionalities. In this case, it is desirable to breakdown

1. Research Institute for Secure Systems, AIST Tsukuba Central 2, 1-1-1 Umezono, Tsukuba 305-8568, Japan ＊ E-mail: hanaoka-goichiro@aist.go.jp, 2. Graduate School of Information Science and Technology, The University of Tokyo 7-3-1 Hongo, Bunkyo-ku 113-8656, Japan

Original manuscript received July 31, 2013, Revisions received November 9, 2013, Accepted November 15, 2013

the functionalities into basic cryptographic schemes where the individual functionalities are already widely in use. By achieving the complex functionalities only through the combination of existing schemes without scratch development, the security can be based on the reliability of the existing schemes that comprise the elemental technologies. Moreover, since the existing technologies are already widely used in the real world, their reliability can be considered sufficiently high.

The modularization where the complex problem is reduced to smaller, easier-to-understand elements is a common practice in the field of programming, but it was not commonly done in cryptographic research. One of the reasons is that compared to the usual information technology where "appropriate things are done," the cryptographic schemes differ greatly in characteristic because it is necessary to ensure that "inappropriate things cannot be done." This is a point that necessitates a new set of arguments to justify the modularization method. Since previously, in the field of highly functional cryptographic scheme field, system design for specialists was mainstream, and the work of "making things understandable" like modularization was taken lightly. However, it has come to the point that recent highly functional cryptographic schemes have become increasingly complex, and even the specialists cannot correctly understand the newly proposed schemes. There are cases where errors in security proofs are pointed out in the schemes that were peer-reviewed and accepted by the international conferences that are supposed authorities. Currently, as highly functional cryptographic schemes are put to practical use, it is important to explain the technology to those who are not specialists, and we believe the necessity and importance of incorporating the modularization method into cryptographic research are increasing.

Note that the objective of the proposed methodology is not to strengthen the security of the cryptographic schemes, but the main objective is to achieve equivalent security in a form that is understandable to a third party (potential user). This research is to point out that there is a significant difference between the cryptographic schemes where just the theoretical verification for security has been done (to some degree), and the cryptographic schemes where the security verification result is easy to understand for the user, in terms of ease of introduction to the real world, and this difference is the barrier to the practical use of new highly functional cryptographic schemes. This research attempts to promote the wide use of highly functional cryptographic schemes in the real world by removing such barriers.

In the next section, we discuss the case of proxy re-encryption as a specific case study to observe the barrier due to the security verification problem.

1.2 Outline and current status of the proxy re-encryption

Outline of the proxy re-encryption

Proxy re-encryption is a technology that allows conversion of encrypted data addressed to a different receiver without decrypting the encrypted data that is addressed to a certain receiver (Fig. 1). It was proposed for the first time by Blaze *et al.*[1] in 1998. In a normal situation, the proxy re-encryption works similarly to public key encryption, and the receiver can designate a certain user, other than oneself, to the server called the "proxy," and can deposit a "re-encryption key." The proxy can convert the ciphertext addressed to each user to the ciphertext addressed to a different designated user by activating the re-encryption key. By using this cryptographic scheme, multiple users can be adaptively designated instead of one certain user. We note that some proxy re-encryption schemes allow multiple re-encryptions, but in this paper, proxy re-encryption schemes that allow re-encryption only once will be discussed.

Proxy re-encryption is significantly useful in achieving secure access control in an environment where there is indefinite number of users such as in cloud storage, and R&Ds have been done actively and globally since 2006. While the discussions for security had been insufficient back in 1998, focus was placed on designing a system with powerful, mathematically provable security in a series of research since 2006. Such powerful mathematical proof for security arose not merely from theoretical interest, but due to practical necessity. In the work of standardization, for example, in the selection of CRYPTREC e-Government Recommended Ciphers,[2] which is considered as the standard cryptographic schemes in Japan, the presence of mathematical security proof is an important selection criterion.

Necessity of proxy re-encryption

In the cloud storage such as Dropbox[3] and Google Drive[4] that are widely used, the reading and writing of the files can be done only by multiple users with valid authorization, and such authorization can be set flexibly.

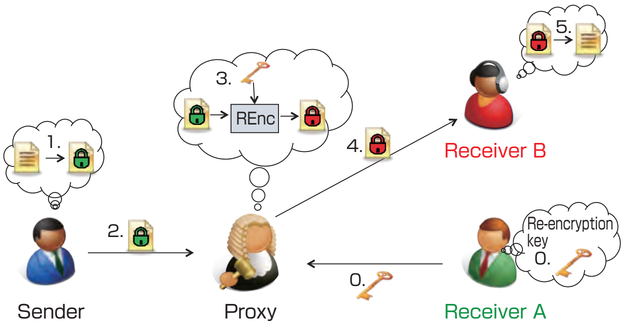


Fig. 1 Overview of proxy re-encryption

However, since the data stored in these storages are assumed to be shared by multiple users, they are either not encrypted or are encrypted in a manner in which the data storage server can decrypt them, and the data can be accessed by the server manager. Therefore, even if the user takes extra caution to manage the data, there is danger of data leakage due to the server manager with malicious intentions or negligence. Recently, the whistleblowing by the employee of the Central Intelligence Agency (CIA) and National Security Agency (NSA) of the United States had international repercussions. There are also reports of possibility that mail addresses and phone numbers of 6 million Facebook users were released due to a fault on the server side. Such events are examples of the limitations of the system design that places unconditional confidence in the server.

One of the methods to prevent spying and leakage of data through the server as mentioned above is to store the data that have been encrypted by the user in the storage. The server that does not have the decryption key cannot read the data, and the plaintext will not leak from the server. However, it should not be assumed that the decryption key needed to access the data is safely distributed only to users with valid authorization. This is because if there is a mechanism where the decryption key can be safely distributed to authorized users only, the data can be distributed only to authorized users using that mechanism.

When proxy re-encryption is used in such a situation, each user can not only store the data in storage in encrypted form, but other authorized users are allowed flexible access control by depositing the re-encryption key to the proxy. The cloud storage using proxy re-encryption is being used commercially.[5] Since the problems that occurred in Facebook and others were due to complex factors, not all problems can be immediately solved by introducing proxy re-encryption. However, it will be significantly effective as it can eliminate the assumption of the existence of a highly reliable server.

Barriers in introducing the proxy re-encryption

As mentioned above, while proxy re-encryption is useful in achieving the cloud storage with flexible access control that is secure against spying and leakage of data through the server, there are still barriers in introducing this technology to the real system. The barrier is not directly related to the functionality of proxy re-encryption, and actually there will be absolutely no problem if the given proxy re-encryption scheme can be confirmed to work as intended. Here, detailed explanation will be given on the barriers to introducing proxy re-encryption.

There are security verification problems as mentioned at the beginning of this section in most of the highly functional cryptographic schemes, and this is particularly significant in proxy re-encryption. The proxy re-encryption scheme proposed at PKC 2009, an international conference that is the authority on public key cryptography, had excellent efficiency,[6] but it was pointed out in PKC 2010 of the following year that the security proof was wrong and it could be attacked.[7] In that paper, a new proxy re-encryption scheme was proposed, but the error in the security proof was pointed out and attacked at the following PKC 2011.[8]

Therefore, there seems to be no method in which the functionality and security are reliable as claimed by the designer for the various proxy re-encryption schemes that had been proposed so far, and this is a major barrier to practical use. For the proxy re-encryption scheme[5] that has been commercialized recently, it should be noted that the service is provided by the company to which the designer belongs, and the practical use has not necessarily been promoted after wide recognition of the technological adequacy.

Other highly functional cryptographic schemes

As mentioned earlier, this paper proposes the guideline for solving the common problems in the practical use of various highly functional cryptographic schemes that have recently been proposed, and proxy re-encryption is just one example. The examples of highly functional cryptographic schemes other than proxy re-encryption include attribute-based encryption, keyword-searchable encryption, homomorphic encryption, group signature, and others. In all these highly functional cryptographic schemes, the structure and security definition become complex as in proxy re-encryption, and this again is a major barrier to their practical use.

2 Functionalities and security definitions of proxy re-encryption

In this chapter, we explain the functionalities and security definitions of proxy re-encryption, and discuss how the construction and its security proofs become complex when a proxy re-encryption scheme that satisfies them is designed by conventional approaches.

2.1 Formal model of proxy re-encryption

First, we explain the algorithms that constitute proxy re-encryption. These are listed as follows:

[Algorithm 1] Key generation for each user
As in an ordinary public key encryption scheme, a proxy re-encryption scheme has the algorithm with which each user generates a pair of a public encryption key and a secret decryption key.

[Algorithm 2] Re-encryption key generation
A proxy re-encryption scheme has the algorithm for

generating a re-encryption key that can be used to transform a ciphertext for User A into a ciphertext for User B. User A generates a re-encryption key by using User A's secret key and User B's public key, and gives it to a proxy.

[Algorithm 3] Encryption
As in an ordinary public key encryption scheme, a proxy re-encryption scheme has the algorithm with which a user can generate a ciphertext that can be decrypted by a legitimate receiver who possesses a secret key. In the encryption algorithm, a ciphertext is generated from a plaintext to be encrypted and the receiver's public key. Moreover, as mentioned above, a ciphertext generated by this algorithm must be transformable to a ciphertext that can be decrypted by a different receiver by using a re-encryption key.

[Algorithm 4] Re-encryption
A proxy re-encryption scheme has the algorithm that enables a proxy who holds a re-encryption key to transform a ciphertext that was originally designated to some receiver into a ciphertext that can be decrypted by another receiver who is different from the original receiver. In this re-encryption algorithm, a re-encrypted ciphertext is generated from a ciphertext (that has not been re-encrypted) and a re-encryption key.

[Algorithm 5] Decryption of ciphertexts that are not re-encrypted
A proxy re-encryption scheme has the algorithm that enables us to decrypt ciphertexts that are generated by the encryption algorithm (Algorithm 3). In this decryption algorithm, a plaintext is recovered from a ciphertext (generated under a legitimate receiver's encryption key) and the receiver's decryption key.

[Algorithm 6] Decryption of re-encrypted ciphertexts.
Similarly to the above, a proxy re-encryption scheme has the algorithm that enables us to decrypt re-encrypted ciphertexts that are generated by the re-encryption algorithm (Algorithm 4). In this decryption algorithm, a plaintext is recovered from a re-encrypted ciphertext and a legitimate receiver's decryption key.

As can be seen from Algorithms 1 to 6, there are six algorithms that constitute a proxy re-encryption scheme, and all of them have complex functionalities. Therefore, even if a designer of a proxy re-encryption scheme claims that the proposed scheme satisfies the functionalities, it is not always easy to verify the correctness.

2.2 Security Definitions of proxy re-encryption

As mentioned in subchapter 2.1, the formal model of proxy re-encryption is already quite complex, and the security definitions are even more complicated and hard-to-understand for non-specialists. In this section, we provide the security requirements of proxy re-encryption. For details, refer to reference [9], for example.

The security notion usually required by ordinary public key encryption (without the re-encryption functionality) is called "security against chosen ciphertext attacks." This security notion ensures that no attacker can obtain even one bit of information of the plaintext from a target ciphertext, even if the attacker is allowed to observe decryption results of arbitrary ciphertexts other than the target ciphertext. It is known that this security not only ensures that the information does not leak from the ciphertext, but also ensures security against "active" attacks such as modification of ciphertexts, and is nowadays considered as a desirable security notion for public key encryption used in practice.

Basically, the aforementioned security is also required for proxy re-encryption. However, as already seen in subchapter 2.1, there are two types of ciphertexts in proxy re-encryption, namely "ciphertexts that are not re-encrypted" and "re-encrypted ciphertexts," and an attacker who wishes to obtain the information of a plaintext may attack either type of ciphertexts. Moreover, since proxy re-encryption has the re-encryption functionality as well as the functionality to generate re-encryption keys, the attacker may try to extract useful information for its attack from these functionalities. Therefore, the security definition of proxy re-encryption must take into account such situations. Particularly important is that the security definition must ensure that the information of a plaintext does not leak from a ciphertext to a proxy that performs re-encryption. Moreover, considering the real use situation, the information of communications to a legitimate user must be protected even when multiple users and proxies collude. Based on the above explanation, the security requirements of proxy re-encryption are organized as follows. (Below, for notational convenience, the user who is under attack will be called A.)

[Security of ciphertexts that are not re-encrypted]
This security notion requires that even if there is any kind of collusion among users and proxies except the "collusion for which attack cannot be prevented in principle," even one bit of plaintext information will not be leaked from a ciphertext (that is not re-encrypted) designated to A. This security notion also requires that a ciphertext cannot be converted to a different, meaningful ciphertext other than a "re-encrypted ciphertext designated to another user." Note that due to the definition of the functionalities of proxy re-encryption, when "User B" and the "proxy that can re-encrypt a ciphertext designated to A to a ciphertext designated to B" form a collusion, all ciphertexts (that have not been re-encrypted) designated to A can be decrypted. Thus, this security notion takes care of all attack situations except the collusion that cannot be prevented in principle.

[Security of re-encrypted ciphertexts]

This security notion requires that in the situation where a ciphertext that has not been re-encrypted is designated to a user different from A (we call the user B), even if all users including B and proxies collude, even one bit of plaintext information will not be leaked from a re-encrypted ciphertext designated to A. This security notion also requires that a re-encrypted ciphertext cannot be transformed to any different, meaningful ciphertext.

The above are the security notions required of proxy re-encryption, and it would be easily seen that there arises the security verification problem in which understanding and verifying the security definitions and security proofs are difficult.

2.3 Example of an existing proxy re-encryption scheme

Figure 2 shows part of the construction of the proxy re-encryption scheme proposed by Libert and Vergnaud.[10] This scheme was designed and implemented from scratch, using a cyclic group with a special kind of mapping (function e in the figure) that has bilinearity. (This mapping is called "pairing" in cryptography.) By assuming the hardness of solving some mathematical problem on the cyclic group, the authors of this paper provided the security proofs which show that this proxy re-encryption scheme satisfies the security notions explained in subchapter 2.2. This proxy re-encryption scheme is known as one of the representative schemes that achieve both security and practical efficiency.

However, as can be seen from the figure, the description of the scheme is quite complex. The components of a ciphertext and various keys cannot be clearly parsed into the component that plays the role of hiding the information, a plaintext, the component that enables re-encryption, or the component that contributes to security, and the components are complexly intertwined. The structure of the parameters and the order of calculations are combined in a "craftsman-like" manner, and it is even difficult for us, the researchers in cryptography, to clearly explain the individual roles. For example, as shown in Fig. 2, the components C_2', C_2'', C_2''' in a re-encrypted ciphertext are not independent, but are correlated via the common internal randomness t. Also, although not explicitly described in the figure, the components C_2''', C_3, C_4 in a re-encrypted are also correlated via the common internal randomness r, and the component σ is generated depending on C_1, C_3, C_4. Thus, it can be seen that all the components in the ciphertext are mutually correlated, and therefore are involved in the various functionalities of proxy re-encryption in one way or the other. Furthermore, the cyclic group with "pairing" described above must use a special cryptographic software library that is difficult to be appropriately used by anyone other than engineers with a certain level of knowledge of cryptography using elliptic curves, and it is also poor in modularity and transplantability.

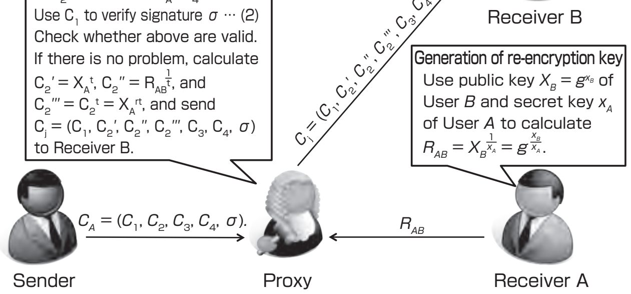

Re-encryption
$e(C_2, u^{C_1} \cdot v) = e(X_A, C_4)$ ··· (1)
Use C_1 to verify signature σ ··· (2)
Check whether above are valid.
If there is no problem, calculate
$C_2' = X_A^t$, $C_2'' = R_{AB}^{\frac{1}{t}}$, and
$C_2''' = C_2^t = X_A^{rt}$, and send
$C_j = (C_1, C_2', C_2'', C_2''', C_3, C_4, \sigma)$
to Receiver B.
$C_j = (C_1, C_2', C_2'', C_2''', C_3, C_4, \sigma)$
Receiver B
Generation of re-encryption key
Use public key $X_B = g^{x_B}$ of
User B and secret key x_A
of User A to calculate
$R_{AB} = X_B^{\frac{1}{x_A}} = g^{\frac{x_B}{x_A}}$.
$C_A = (C_1, C_2, C_3, C_4, \sigma)$.
R_{AB}
Sender
Proxy
Receiver A

Fig. 2 Re-encryption functionality in an existing scheme[10]

3 Proposed method: Methodology and example of application to proxy re-encryption

In order to resolve the security verification problem, in this section we discuss our methodology to make highly functional cryptographic schemes (including proxy re-encryption) that have complex algorithm and security definitions easily understandable by a third party who may be a potential user, and to smoothly introduce them to the real world. Also, we describe the proxy re-encryption scheme that was actually designed based on our methodology, and explain the design philosophy behind the construction.

3.1 Overview of the proposed methodology

So far, highly functional cryptographic schemes with complex functionality requirements have very often been designed from scratch to satisfy their functionalities and security definitions. Since a system designed from scratch tries to achieve required functionalities and security simultaneously in an inseparable manner by voluminous and complex mathematical equations, it is extremely difficult for a third party to verify the correctness of them.

Here, we consider such a conventional approach of designing from scratch to be the major inhibiting factor in introducing highly functional cryptographic schemes to the real world. As the methodology for solving the problem, we propose to "insert the steps of modularizing the required functionalities and security as much as possible before the phase of starting the actual design" and emphasize its importance (See Fig. 3). In particular, considering the security verification problem, we pursue "modularization" as much as possible so that the modularized functionalities and security notions can be achieved by directly using existing basic cryptographic schemes that have already been well-known and well-studied. While expertise in existing basic cryptographic schemes is still required, these basic primitives have already been sufficiently studied and analyzed, and there are many more researchers and engineers who are capable of verifying and understanding them, compared to highly functional cryptographic schemes such as proxy re-encryption.

By designing a highly functional cryptographic scheme after the step of modularizing the requirements of functionalities and security, it becomes possible to facilitate a third party to understand the functionalities and security provided by a designed system. More specifically, the following positive effects can be expected.

- It becomes easier to understand what roles individual modularized functionalities and security play in the designed system.
- Since the functionalities and security of the basic cryptographic schemes used as building blocks have already been well-understood, it becomes easier to understand and to verify the correctness of functionalities and security of the designed system.
- For each modularized functionality and security, it becomes possible to select a suitable building block that works in the most effective way, depending on applications. Furthermore, once any problems are found in the building blocks, we can easily and quickly replace them with some other building blocks.

Due to these positive effects, the barriers in introducing a newly designed highly functional cryptographic scheme into a real world system will be significantly reduced.

In the next section, we will explain a concrete proxy re-encryption scheme that was designed based on our proposed methodology. Before doing so, in order to confirm that the above positive effects are indeed achieved by the proposed methodology, we exemplify a simpler case of public key encryption that allows variable length of plaintexts.

Generic construction of public key encryption that allows plaintexts with variable length

In most of the existing public key encryption schemes, for example, references [11] and [12], the size of plaintexts that can be encrypted is strictly limited due to the algebraic structure on which the schemes are based. In practice, however, it is often the case that we need to be able to encrypt data of various sizes. On the other hand, in the research on symmetric key encryption, it is usual to design schemes that can encrypt messages of variable length by default. In the beginning of the 2000s, the methodologies for constructing a public key encryption scheme that allows plaintexts of variable length were systematized, and the following generic construction was proposed: (1) First, a session-key K with a fixed length is selected, and a plaintext is encrypted by a symmetric key encryption scheme using the session-key K. (2) Next, the session-key K is encrypted using a public key encryption scheme (that allows only fixed length plaintexts). Finally, the set of two ciphertexts obtained in the above steps (1) and (2) are used as a ciphertext of this construction.

This construction can be seen as a specific example of the design methodology of highly functional cryptographic schemes proposed in this paper. Specifically, the basic functionality of public key encryption and the functionality to encrypt variable length plaintexts are separated into an (ordinary) public key encryption scheme and a symmetric key encryption scheme , respectively. This construction has been further refined and sophisticated, and currently, the above functionalities (1) and (2) are standardized individually in the standardization activities, such as ISO[13], of public key cryptographic schemes. From this simple example, the effectiveness of the design methodology proposed in this paper can be appreciated.

3.2 Application to proxy re-encryption

Here, we introduce the proxy re-encryption scheme that was designed by Hanaoka et al.[9] based on the methodology proposed in the previous section. This scheme is constructed by combining a public key encryption scheme,[11][12] a digital signature scheme,[11][14] and a threshold public key encryption scheme[15] as building blocks, and it is easy to understand the correspondence of how and by which building blocks the required individual functionalities and security are achieved.

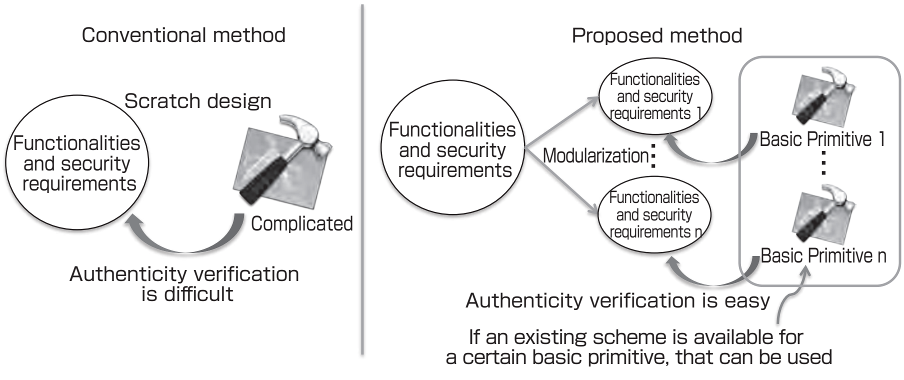

Conventional method
Scratch design
Functionalities and security requirements
Complicated
Authenticity verification is difficult
Proposed method
Functionalities and security requirements
Modularization
Functionalities and security requirements 1
Functionalities and security requirements n
Basic Primitive 1
Basic Primitive n
Authenticity verification is easy
If an existing scheme is available for a certain basic primitive, that can be used

Fig. 3 Difference between the conventional and proposed methodologies

Building blocks

In the following, we will first briefly explain public key encryption, digital signature, and threshold public key encryption. We will explain how to construct a proxy re-encryption scheme from these building blocks in subchapter 3.2. We note that each of the building blocks has multiple functionalities (algorithms), and the six algorithms of proxy re-encryption can be achieved by combining them appropriately.

· Public key encryption
A pair of secret and public keys are generated by a receiver of a message, and the public key is publicized. A sender of a message uses the receiver's public key to encrypt the message and sends the ciphertext to the receiver. The receiver can decrypt the ciphertext using the secret key. By using public key encryption, we can communicate privately with others without sharing any information in advance , and this is one of the most basic cryptographic primitives used widely, such as in SSL and TLS.Note)

· Digital signature
A signer of a message generates a signing key and a verification key, and publicizes the verification key. The signer signs on a message using the signing key. A verifier who obtains the pair of the message and the generated signature can verify them by using the verification key. Digital signature is an analogue of a seal in the real world, and is the most important cryptographic primitive that supports authentication infrastructures in the network society. It is already widely used in PKI and in many other applications.

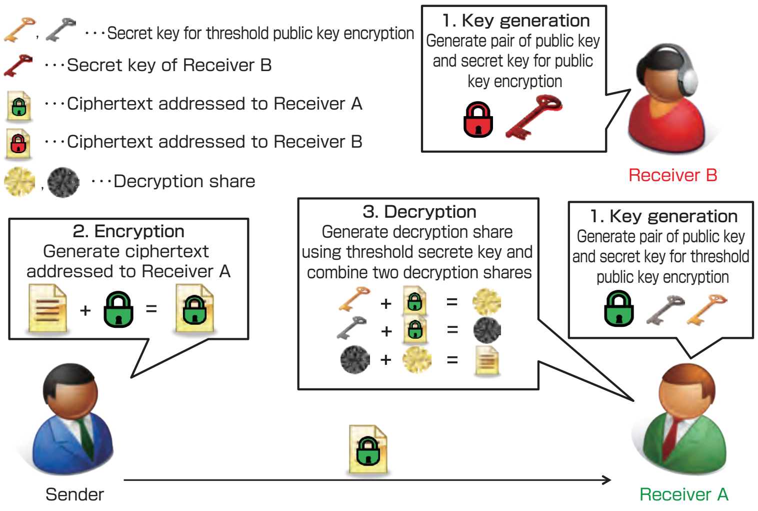
· Threshold public key encryption
This is an extension of public key encryption, in which a secret key, which is normally a single element, is divided into multiple "partial secret keys." In threshold public key encryption, a plaintext is encrypted by a (single) public key as in ordinary pubic key encryption, and using one of the partial secret keys, the ciphertext can be "decrypted" into a partial decryption result called a "decryption share". One can recover the original plaintext hidden in the ciphertext by collecting more decryption shares than the "threshold." In the proxy re-encryption scheme described in this section, we use a threshold public key encryption scheme in which a secret key is divided into two partial secret keys and a ciphertext can be decrypted by collecting the two decryption shares of the ciphertext.

Threshold public key encryption is an important cryptographic scheme in the construction of electronic voting (e-voting) systems, and research on it has been active since the 1990s. It has already been introduced to some practical systems, and its functionalities and security have been well-studied and deeply understood.

The proposed construction of proxy re-encryption

In the construction of proxy re-encryption explained here, the threshold public key encryption scheme plays a central role. As shown in Fig. 4, in this construction, a sender encrypts a message using the Receiver A's public key of the threshold public key encryption scheme, and sends the ciphertext. This ciphertext can be decrypted by Receiver A who possesses the secret key of the threshold public key encryption scheme. This functionality corresponds to that of ordinary public key encryption.

As shown in Fig. 5, when generating a re-encryption key, User A encrypts one of the two partial secret keys using User B's public key, where User B is the designated receiver of re-encrypted ciphertexts, and gives this to the proxy. Here,



, ···Secret key for threshold public key encryption
···Secret key of Receiver B
···Ciphertext addressed to Receiver A
···Ciphertext addressed to Receiver B
, ···Decryption share
1. Key generation
Generate pair of public key and secret key for public key encryption
Receiver B
2. Encryption
Generate ciphertext addressed to Receiver A
+ =
3. Decryption
Generate decryption share using threshold secrete key and combine two decrption shares
+ =
+ =
+ =
1. Key generation
Generate pair of public key and secret key for threshold public key encryption
Sender
Receiver A

Fig. 4 Construction by the proposed method (key generation, encryption, decryption by Receiver A)

the authenticity of the re-encryption key is ensured by using the digital signature scheme. When re-encrypting, the proxy partially decrypts the ciphertext using the partial secret key that is not encrypted, calculates the decryption share, and sends this to User B along with the encrypted partial secret key.

As shown in Fig. 6, User B who receives the re-encrypted ciphertext decrypts the encrypted partial secret key, and then recovers the original plaintext by obtaining the other decryption share using the partial secret key, and combining both of the decryption shares.

4 Evaluation of the proposed method

To gain confidence in the security of highly functional cryptographic schemes, as mentioned above, it is important to break things down into basic elemental schemes that are already widely used. Here, using the example of the proxy re-encryption scheme described in the previous section, we explain in detail into which basic scheme it was broken down, and why the breakdown into those basic schemes were done.

Specifically, the proxy re-encryption scheme of the previous section is broken down into basic schemes such as public key encryption, digital signature, and threshold public key encryption, and these are not only basic compared to proxy re-encryption scheme, but are also already used widely. The breakdown was not accidental, but was intentional since highly secure and reliable implementations have been done for these schemes. For public key encryption, the RSA-OAEP method is widely used, as well as the RSASSA-PKCS1-v1_5 method for the digital signature in SSL/TLS. In fact, although there are over 800 thousand SSL server certificates issued and installed by the Symantec Corporation of the USA,[16] there have been no security problems despite such wide use (however, not all implementation of the RSASSA-PKCS1-v1_5 method is secure, and it is necessary to carefully select the implementation with highly reliable performance). Threshold public key encryption is not widely used compared to the above two schemes, but it is used in e-voting, and can be considered sufficiently reliable. From the above, one can understand what policy is employed in the functionality breakdown in the proxy re-encryption scheme as presented in the previous section.

There are the following five advantages when the functionalities are broken down as above.

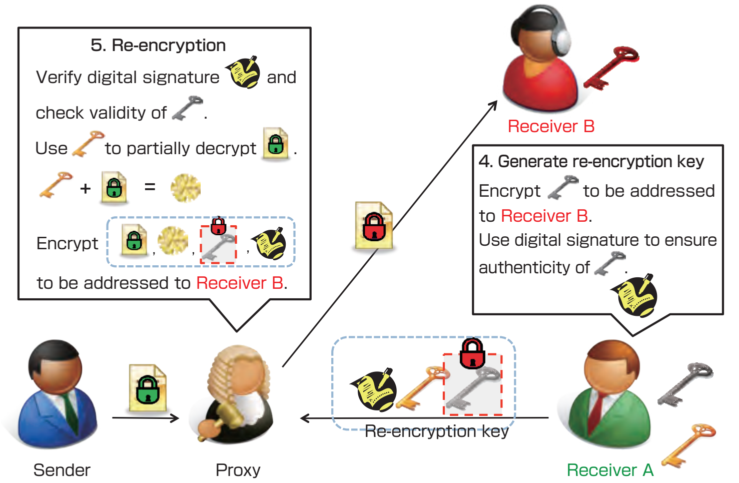

5. Re-encryption
Verify digital signature and check validity of .
Use to partially decrypt .
+ =
Encrypt , , ,
to be addressed to Receiver B.
Receiver B
4. Generate re-encryption key
Encrypt to be addressed to Receiver B.
Use digital signature to ensure authenticity of .
Re-encryption key
Sender
Proxy
Receiver A

Fig. 5 Construction by the proposed method (generation of re-encryption key, re-encryption)

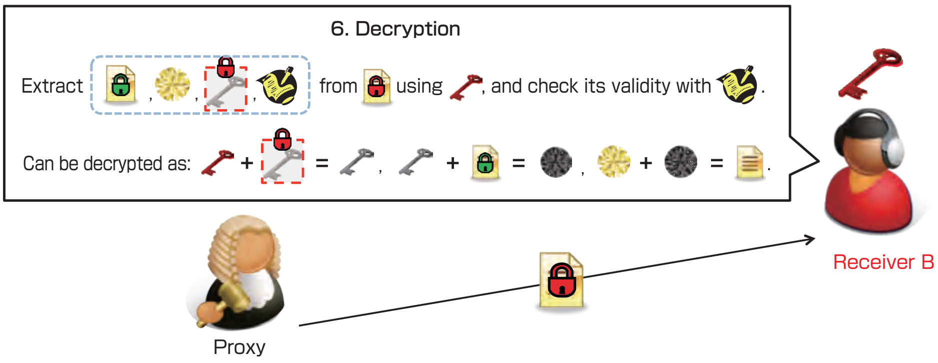

6. Decryption
Extract , , , from using , and check its validity with .
Can be decrypted as: + = , + = , + = .
Receiver B
Proxy

Fig. 6 Construction by the proposed method (decryption by Receiver B)

[Advantage 1] Compared to scratch construction, it can be readily understood that a highly functional scheme called proxy re-encryption has been achieved. Considering how the functionalities described in subchapter 2.1 are achieved, the following points can be intuitively understood without following the difficult mathematical equations.

- The key generation of Algorithm 1 is achieved as Receiver A generates a pair of threshold public and secret keys, and Receiver B generates a pair of the usual public and secret keys (Fig. 4).
- The re-encryption key generation of Algorithm 2 is achieved as one of the two threshold secret keys is encrypted by Receiver B's (usual) public key, and then combined with the remaining threshold secret key, is used as the re-encryption key (Fig. 5).
- The encryption and decryption of Algorithms 3 and 5 are achieved by the encryption and the decryption of the threshold public key encryption scheme (Fig. 4).
- The re-encryption of Algorithm 4 is achieved as the proxy partially decrypts the ciphertext using the obtained threshold secret key, and then encrypts and sends the bundle of obtained decryption share, ciphertext addressed to A, and encrypted threshold secret key to Receiver B (Fig. 5).
- In the decryption of the re-encrypted ciphertext of Algorithm 6, Receiver B decrypts the sent ciphertext using its own secret key, and then decrypts the encrypted threshold secret key in the sent material. The obtained threshold secret key is used to partially decrypt the ciphertext addressed to A, whereby the second decryption share is obtained and the message can be decrypted, and Algorithm 6 is achieved (Fig. 6).

[Advantage 2] In relation to Advantage 1, the understanding of the achieved security as a whole is facilitated, by clarifying the role division of the component for each functionality of proxy re-encryption. Also, if error is found in the security proof, the proof can be corrected readily since it is clear which part of the error corresponds to which component scheme.

[Advantage 3] Even when replacing a component cryptographic scheme of the above proxy re-encryption scheme with another scheme with equivalent functionalities, the performance and customization of the resulting proxy re-encryption scheme can be done readily. In the case of scratch construction, the burden is great because one must check whether the change does not interfere with the functionalities or security by returning to the whole construction each time a part is changed, for example, for increasing the execution speed. On the other hand, with this methodology, the local characteristics need only to be checked to see whether the function of a component is maintained when the construction of a component is changed, and the work is facilitated.

[Advantage 4] In relation to Advantage 3, even when the update of the encryption method will be needed due to increased cryptographic attacks in the future, using this methodology, only the component scheme whose security is compromised can be replaced, and the operation cost necessary for updating can be reduced. Similarly, in case one wishes to construct a proxy re-encryption scheme that cannot be cracked with a quantum computer (i.e. quantum resistant) that is expected to be available in the future, the above mentioned three components can each be made quantum resistant. This is much easier compared to developing a quantum-resistant proxy re-encryption scheme from scratch.

[Advantage 5] In relation to Advantage 4, in the case of this methodology, for example, by developing a superior scheme compared to the conventional digital signature schemes, the digital signature scheme itself and the proxy re-encryption scheme that uses digital signature schemes as its components can be simultaneously improved. Such a characteristic of this methodology will contribute to increased efficiency of the research resource allotment for the R&Ds of the entire field of cryptography.

5 Application to other highly functional cryptographic scheme

In this chapter, we discuss the applicability of the design policy of highly functional cryptographic schemes proposed in this paper to other cryptographic schemes other than proxy re-encryption, particularly to group signature. The interference of the components that may occur when the proposed method is used and the ways to avoid such interference will also be discussed.

5.1 On application to group signatures

A group signature scheme is a digital signature scheme in which the privacy of the signer is ensured. Since its concept was first proposed by Chaum *et al.*[17] in 1991, several specific constructions have been proposed. Other than the functionalities of the conventional digital signatures, the group signature has the confidentiality for identity of the signature issuer. It is a digital signature with enhanced privacy protection functionality that is significantly effective for electronic bulletin boards, electronic auction sites, and others.

However, since the functionalities are significantly complex compared to the conventional digital signatures, a concrete construction with sufficiently high level of security was hardly in existence. In response, in 2003, Bellare *et al.*[18] indicated that the group signature could be achieved by combining the functionalities of digital signature, public key encryption, and zero-knowledge proof. Since this accomplishment, there was a paradigm shift where the designers of group signatures started to consider the appropriate selection of a digital signature scheme, public key encryption scheme, and zero-knowledge proof system, in the mode of the breakdown of functionalities as mentioned above. As a result, compared to the conventional schemes by scratch design, the functionalities and security of the newly proposed scheme can be thoroughly understood by a third party, and this is affecting the progress of commercialization and standardization.[19]

There are already widely used, highly reliable schemes of digital signature and public key encryption as mentioned above. Zero-knowledge proofs are widely used in user authentication schemes, and are sufficiently reliable scheme.

The importance of functionality breakdown in designing the highly functional cryptographic scheme as proposed in this paper has been implied by Bellare *et al.* in some sense, and the main result of this paper is to explicitly discuss this point and indicate that it is a universal design concept not just for group signatures. For group signatures where the proposed method was implicitly used in this paper, the effectiveness of the proposed method can be understood since the standardization of this scheme has progressed.

5.2 On the interference of the components to security

This paper claims the effectiveness of achieving the functionalities of a highly functional cryptographic scheme to be designed through the combination of basic cryptographic schemes. However, there are cases where the basic cryptographic schemes used interfere with each other, and the total security cannot be ensured even if the security is ensured for individual schemes. Here, we discuss the method for investigating whether such a problem is occurring in the designed system.

In a case where the targeted highly functional cryptographic scheme can be generically constructed using only the basic component schemes in a strict sense, the security proof of the individual scheme that is a special case will not be necessary, if the security proof of this generic construction has been done. That is, if the underlying basic schemes fulfill certain conditions required for this generic construction, the security of the total scheme that is constructed using the above basic schemes is automatically ensured regardless of which basic component schemes are used. The construction of the proxy re-encryption scheme discussed in this paper is generic in this strict sense.

There is a concept called universal composability that is the concept of security that ensures that the elemental schemes do not interfere with each other. The interference among the elemental schemes can be prevented by using the component schemes that fulfill this security concept.

5.3 Basic schemes to which the breakdown is done

In breaking down the functionalities of highly functional cryptographic schemes, it is necessary to keep in mind that the basic scheme to which the breakdown is done shall be the ones for which security is considered highly reliable. In that case, as the criteria for determining whether it is evaluated highly for its security, it should have usage performance in a wide range and that there has been no essential problem in security over a long-term. From such perspectives, there is no doubt that public key encryption, digital signature, symmetric key encryption, and message authentication code are reliable schemes. For public key encryption and digital signature, as mentioned earlier, implementations with high use performance are known. There are also schemes that are already widely diffused with no security problem found as in the AES (95.4 % deployment in commercial products) for symmetric key encryption, and the HMAC (82.1 % deployment in commercial products) for message authentication code.[20] Other than the aforementioned threshold public key encryption and zero-knowledge proof, broadcast encryption is widely used in the protection of copyrights for Blue Ray discs, and it can be considered a sufficiently reliable scheme.

6 Summary

While highly functional cryptographic schemes are useful in recent highly sophisticated networks, the introduction into society is not progressing well. In this paper, we indicated that to promote the use of highly functional cryptographic schemes, not only do the functionality and security have to be advanced, but also they must be readily understandable. Then, we proposed the design concept to achieve such understandability.

In response to the expected advancement of the network technology in the future, highly functional cryptographic schemes with even more advanced functions and security will be required. Considering practical use, they must not just satisfy the required functionality and security but also must be readily understandable to the third party, and we think it is possible to promote the practical use by using the method proposed in this paper. Since the proposed method is to improve the “ease of understanding,” the establishment of the quantitative evaluation method for “ease of understanding” is necessary to widely communicate the effectiveness of this method to society. As one method, it may be possible to evaluate it by estimating the input size for the automatic security verification tool. This shall be a future research topic.

Notes

Note) SSL and TLS are communication protocols that require security, and provide the functionalities of authentication, encryption, and forgery detection. We can choose some algorithms for these protocols, and selection are made among the algorithms which allowed by both parties as the start of communication.

Terminologies

Term. Scratch development: Development where the (cryptographic) system is constructed from zero (or scratch) without utilizing the already existing technologies.

References

[1] M. Blaze, G. Bleumer and M. Strauss: Divertible protocols and atomic proxy cryptography, *EUROCRYPT '98*, 1403, 127-144 (1998).

[2] CRYPTREC Ciphers List, http://www.cryptrec.go.jp/english/list.html

[3] Dropbox https://www.dropbox.com/

[4] Google Drive https://drive.google.com/

[5] Digital Kashi Kinko (Digital Rental Safe) http://tosafebox.com/

[6] J. Shao and Z. Cao: CCA-secure proxy re-encryption without pairings, *PKC 2009*, 5443, 357-376 (2009).

[7] T. Matsuda, R. Nishimaki and K. Tanaka: CCA proxy re-encryption without bilinear maps in the standard model, *PKC 2010*, 6056, 261-278 (2010).

[8] J. Weng, Y. Zhao and G. Hanaoka: On the security of a bidirectional proxy re-encryption scheme from PKC 2010, *PKC 2011*, 6571, 284-295 (2011).

[9] G. Hanaoka, Y. Kawai, N. Kunihiro, T. Matsuda, J. Weng, R. Zhang and Y. Zhao: Generic construction of chosen ciphertext secure proxy re-encryption, *CT-RSA*, 7178, 349-364 (2012).

[10] B. Libert and D. Vergnaud: Unidirectional chosen-ciphertext secure proxy re-encryption, *PKC 2008*, 4939, 360-379 (2008).

[11] R. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 21 (2), 120-126 (1978).

[12] R. Cramer and V. Shoup: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, *CRYPTO '98*, 1462, 13-25 (1998).

[13] V. Shoup: A proposal for an ISO standard for public key encryption (version 2.1), http://www.shoup.net/papers/iso-2_1.pdf (2001).

[14] Digital Signature Standard, http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

[15] Y. Desmedt and Y. Frankel: Threshold cryptosystems, *CRYPTO '89*, 435, 307-315 (1989).

[16] VeriSign, Inc.: (Press Release) Symantec achieves highest number of SSL certificates issued globally, https://www.verisign.co.jp/press/2012/pr_20120427.html (2012).

[17] D. Chaum and E. Heyst: Group signatures, *EUROCRYPT '91*, 547, 257-265 (1991).

[18] M. Bellare, D. Micciancio and B. Warinschi: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions, *EUROCRYPT 2003*, 2656, 614-629 (2003).

[19] NEC Corporation: (Press Release) NEC develops technology for anonymous authentication to achieve both security and privacy in a cloud environment, http://www.nec.co.jp/press/ja/1106/0703.html (2011).

[20] CRYPTREC Report 2012, http://www.cryptrec.go.jp/report/c12_opr_web.pdf (2013).

Authors

Goichiro HANAOKA

Graduated from the School of Engineering, The University of Tokyo in 1997. Completed the doctorate course at the Department of Electrical Engineering and Information Systems, Graduate School of Engineering, The University of Tokyo in 2002 (Doctor, Engineering). Postdoctoral Fellow, Japan Society for the Promotion of Science. Joined AIST in 2005. Currently, Leader, Research Group for Innovative Cryptography, Research Institute for Secure Systems, AIST. Engages in the R&Ds for encryption and information security technologies including the efficient design and security verification of public key cryptosystem. Received the Wilkes Award (2007), British Computer Society; Best Paper Award (2008), The Institute of Electronics, Information and Communication Engineers; Innovative Paper Award (2012), Symposium on Cryptography and Information Security (SCIS); Award of Telecommunication Advancement Foundation (2005); 20th Anniversary Award (2005), SCIS; Best Paper Award (2006), SCIS; Encouragement Award (2000), International Symposium on Information Theory and its Applications (SITA); and others. For this paper, was in charge of coordinating the write-up.

Satsuya OHATA

Graduated from the Department of Informatics and Image Science, Faculty of Engineering, Chiba University in March 2011. Completed the master's course at the Graduate School of Information Science and Technology, The University of Tokyo in March 2013 (Master, Information Science and Technology). Currently, enrolled in the doctorate program at the Graduate School of Information Science and Technology, The University of Tokyo. Technical Staff, Innovative Security Research Group, Research Institute for Secure Systems, AIST from May 2012. Engages mainly in the research of public key cryptosystem, provable security, and its application. In this paper, was in charge of the survey and systematization of the technological research trend of the proxy re-encryption, as well as creating the figures.

Takahiro MATSUDA

Graduated from the Department of Electrical Engineering and Information Systems, Faculty of Engineering, The University of Tokyo in March 2006. Completed the doctoral program at the Department of Information and Communication Engineering, Graduate School of Information Science and Technology, The University of Tokyo in March 2011 (Ph.D., Information Science and Technology). JSPS Postdoctoral Fellow, at the Research Center for Information Security (Research Institute for Secure Systems from April 2012), AIST for two years from April 2011. Researcher, Innovative Security Research Group, Research Institute for Secure

Systems, AIST from April 2013. Engages mainly in the research of design and security evaluation of cryptosystems, and theoretical aspects of cryptography. In this paper, was in charge of organizing the functionality requirements and security definitions of the proxy re-encryption and other cryptographic primitives.

Koji NUIDA

Graduated from the Department of Mathematics, School of Science, the University of Tokyo in March 2001. Completed the doctoral course at the Graduate School of Mathematical Sciences, The University of Tokyo in March 2006 (Ph.D., Mathematical Sciences). Postdoctoral Researcher, Research Center for Information Security, AIST from April 2006. Worked as Researcher, Research Team for Physical Analysis; Researcher, Innovative Security Research Group, Research Institute for Secure Systems; and currently Senior Researcher. Engages mainly in the research for construction and security evaluation of the cryptosystems using advanced mathematics, as well as theoretical foundations of cryptology. In this paper, was in charge of the investigation for the comparing the proposed and previous methods.

Nuttapong ATTRAPADUNG

Graduated from the Faculty of Engineering, Chulalongkorn University, Thailand in 2001. Completed the doctoral course at the Department of Information and Communication Engineering, Graduate School of Information Science and Technology, The University of Tokyo in March 2007 (Ph.D., Information Science and Technology). Postdoctoral Fellow for Foreign Researchers, Japan Society for the Promotion of Science at the Research Center for Information Security, AIST from April 2007; and then Researcher, Security Fundamental Research Team. Researcher, Innovative Security Research Group, Research Institute for Secure Systems; and currently Senior Researcher. Engages mainly in the research of design and security evaluation for the cryptographic systems. Received the Ericsson Young Scientist Award in 2010. In this paper, was in charge of the survey of research trend for overall highly functional cryptosystems as well as creating figures.

Discussions with Reviewers

1 Definition of the problem in question

Question and comment (Toshihiro Matsui, Research Institute for Secure Systems, AIST)

You state repeatedly that the verification and proof of security for the highly functional cryptosystem is difficult. Since the main subject of this paper is how to overcome this difficulty, we recommend giving an appropriate name to this matter, so you can refer to the problem by name.

Though you express the difficulty using the phrase “craftsman-like,” it should be discussed in a more scientific manner, since it relates to the definition of the problem. If you understand the content of the difficulty, you can derive a solution. Difficulty overlaps with complexity. Complexity is dissolved to the types of elements, the types of links (relationships), and the numbers of these elements and links. Clues to the solution might be found in a task to unravel the complexity.

Answer (Goichiro Hanaoka)

I shall name the difficulty in having a third party understand the security of highly functional cryptographic scheme, the “security verification problem.” To see the difficulty of the security verification problem, we exemplified the papers on highly functional cryptographic schemes from the major international conferences in the area of cryptography, and pointed out that the security definition, description of the systems, and security proofs dominate a large portion of the papers. We can consider the usage of formal method to solve the security verification problem, and it may possible to evaluate the complexity of problem based on the input data size for verification tools. However, as of now, the application of formal method to the security proof in highly functional cryptographic schemes as addressed in this paper is still very difficult, and we shall leave this as a future research topic.

2 Solution by modularization

Question and comment (Toshihiro Matsui)

In this paper, the solution of the problem is sought through the modularization by breaking down the problem into elements. Since reductionism is an orthodox approach in science, this paper might be regarded as another example of general reductionism. Can you compare your modularization with other contrasting problem-solving methods? Or, giving a more precise modularization guideline, particularly for functional cryptosystems among other modularization principles is useful.

Question and comment (Hideyuki Nakashima, Future University Hakodate)

Since this is a difficult problem (or unfamiliar to the general public), I think you need some more explanations in various places. Particularly, the description of the intention of “why I did it this way” is important for *Synthesiology*, not just “how I did it.”

Answer (Goichiro Hanaoka)

Since the above two comments that I received from the two reviewers are closely related to each other, I would like to answer them both in a single reply.

As you indicated, the proposed method can be seen as following the orthodox approach that should be considered. However, the modular approach was not taken in the research for cryptosystems up to now. There are probably two reasons. First reason is that in cryptosystems, one must prove not only the “correctness” where the functionality one wishes to achieve is completed, but also the “security” where nothing other than the functionality to be achieved can be carried out. Therefore, the modularization of security technology is much more complex than other technologies. Second reason is that the cryptography researchers did not have sufficient motivation to engage in such complex modularization. In the previous technology, the user side could somehow understand the technology, and I don’t think the cryptography researchers ever thought of spending so much effort in modularization. In contrast, the series of highly functional cryptosystems that are being proposed recently seem to exceed the range. In such a situation, I think it is extremely useful for our related field to explicitly indicate the importance of the orthodox general theory called decomposition.

As the policy for modularization, from the perspective of pursuing highly reliable security, we shall adopt modularized individual primitives which have already been widely used in practice.

Including the above, I added the descriptions throughout the paper to clarify the intent of the authors.

3 Problem of module interference

Question and comment (Toshihiro Matsui)

The interference between the components you mention in subchapter 5.2 is the wall to complete reductionism. The optimization of the entire system cannot be achieved by a simple sum of the elemental technologies. For the proxy re-encryption, can you add the findings to see whether such interferences are happening or not, how such interferences can be avoided if any are present, and how this experience can be generalized (in what case do you regard the interferences to be minor)?

Answer (Goichiro Hanaoka)

The removal of interferences among the building blocks is, as you indicate, the part that requires careful consideration in our proposed method. As measures, rather than intuitive and rough decomposition, we must conduct generic construction in the strict sense including the mathematical security proof. The proxy re-encryption scheme addressed in this paper is such a generic construction, and as long as the individual building blocks are secure, the security of the whole system is automatically ensured. As a more general discussion, universal composability is known as the concept for security to ensure that mutual interferences do not occur when the building blocks for cryptosystems are combined. This is also briefly addressed in this paper.

4 Effect of modularization

Question and comment (Toshihiro Matsui)

I think the argument will become more convincing if there is a comparison of the proposed method with the total optimization that is a contrasting approach to this problem. For example, an energy-saving system is not only about increasing efficiency of the component machines such as the boiler, generator, or condenser, but the energy-saving becomes more effective by increasing the linkage of the elements, such as warming the bath using the excess heat from the boiler or returning the heat from the condenser to the boiler. Although decomposition is powerful approach, when ultimate efficiency is pursued, the option of attempting total optimization or building from scratch is attractive. Compared to such total optimization, I think one way is to discuss why modularization is so important in the cryptosystems development.

Answer (Goichiro Hanaoka)

As you indicate, it is better to aim for total optimization by building from scratch from the perspective of good efficiency (length of the ciphertext, computational cost, etc.). On the other hand, the maintenance of sufficient security is of top priority in cryptosystems, and I think the advantage is on the modularization side, considering the security verification problem. Whether the security is formally proved or not is very important from the perspective of standardization, and I think this way of thinking should be prioritized in diffusing highly functional cryptographic schemes in the future. Furthermore, it is also the attractiveness of modularization that, after conducting construction and security proof by modularization, we can construct various instantiations by choosing different underlying primitives. Particularly, it is expected that efficiency can be improved by changing the individual primitives to more efficient ones, and actual researches on this have been done in the past.