Collaboration Projects

"Secure" Distributed Management Scheme of Confidential Information

There is a scheme called a threshold cryptosystem for "secure" distributed management of confidential information. We are focusing on the construction of the threshold cryptosystem, which allows efficient calculation without compromising security, and the development of a threshold cryptosystem based on RSA to realize that construction. This research was conducted jointly with Associate Professor Junji Shikata, the Graduate School of Environment and Information Sciences, Yokohama National University.

Takeru Ishiara, Hiroshi Aono and Sadayuki Hongo

1. Introduction

Today, mobile terminals are dealing with such important data as electronic money of i-mode FeliCa. Such data are not completely secure merely because it is stored in an IC card; "how to retrieve the data securely" is also important to consider. For example, if the data are retrieved via authentication by a PIN code, its security depends only on the PIN code, not the IC card. The PIN code is convenient but not completely secure; therefore, bank ATMs adopt safer authentication method than PIN codes recently. From the above circumstances, information management schemes that prove their safety are attracting increasing attention.

Among secure information management schemes, one called a secret sharing scheme [1] [2] divides and stores confidential information. For example, under a situation where a parent gives an electronic key to a child, by dividing the electronic key data amongst the child's belongings, the parent can increase the security of the data based on a secret sharing scheme. Existing secret sharing schemes, however, increase the volume of their divided data according to the volume of the original secret information and impose constraints on the simultaneous use of IC cards that are supposed to enhance security. In the case of existing secret sharing schemes, how to deliver their divided data presents another problem. In order to solve these problems, we have conducted a research of threshold cryptosystem [3]-[6] as a type of secret sharing scheme. When using threshold cryptosystems, as long as certain lengths of data called private keys are kept secret, the data themselves are sufficiently secure. Therefore if the private keys are divided separately beforehand amongst the one's belongings, the problems of existing secret sharing schemes can be solved.

The aim of this research is to enhance the efficiency of calculation and transmission without compromising the security of the threshold cryptosystem that is a basic technology of distributed management. This article deals with a threshold cryptosystem using the Rivest-Shamir-Adleman (RSA) [7], which is the main purpose of our research. Although our proposed scheme is based on the hypothesis of the Ref. [8], it is the first threshold cryptosystem in the world that proves its security as an RSA-based scheme.

2. Existing Technology and Its Issues

2.1 Threshold Cryptosystem

Threshold cryptosystems are used, for example, as shown in **Figure 1**. Fig. 1 shows the usage of an electronic key handed to a child from his/her parent. First, the parent encrypts the electronic key and creates a ciphertext. The same ciphertext is sent to both the child's mobile terminal and IC card in his/her bag. The IC card creates a share using secret information in the card called a private key. The child gathers the shares and decrypt the electronic key. Although two is the number of both the private key and the share in Fig. 1, the private key and share numbers needed for decryption can be selected respectively and with flexibility.

Figure 2 shows the operational principle image of a threshold cryptosystem. Users use a public key to encrypt plaintext

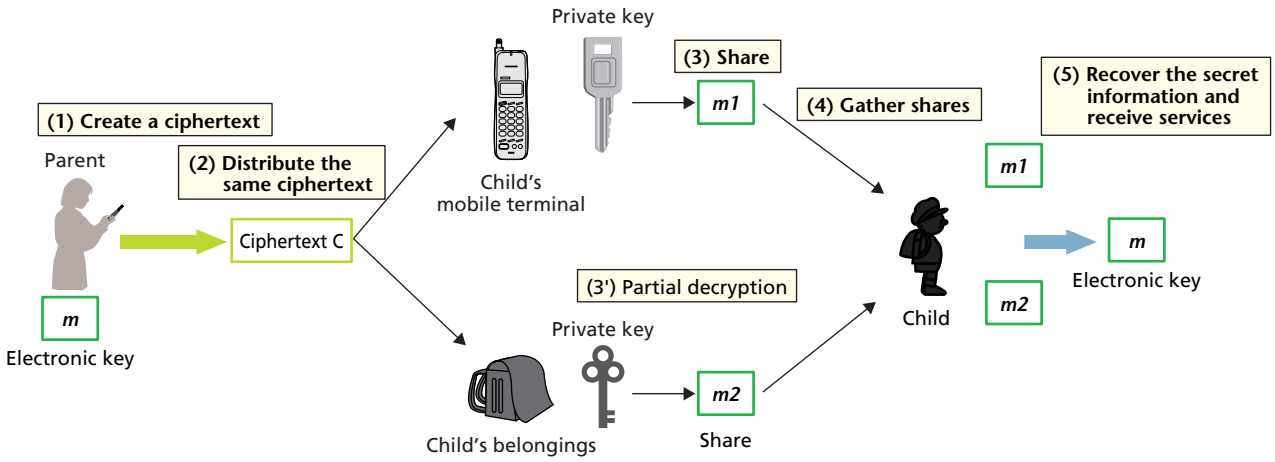


Figure 1 How to use threshold cryptosystem

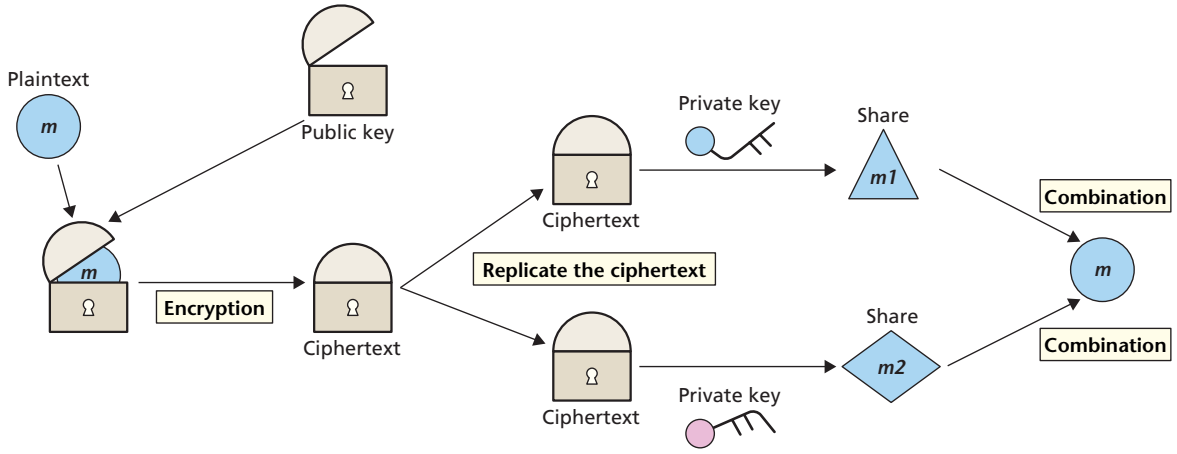


Figure 2 Image of the threshold cryptosystem

(the encryption corresponds to putting the plaintext in the keyed box in Fig. 2, the plaintext to the electronic key in Fig. 1) and calculate a ciphertext. Anybody can perform the encryption with the public key, but decryption requires private keys. In the threshold cryptosystem process, the modified plaintext is output after the ciphertexts have been decoded with private keys. The output data are called shares. The private key is cleverly designed, and information on the plaintext cannot be acquired through a piece of share alone since a share is neatly modified that the original is unable to be recognized. With two pieces of share, however, the plaintext can be decoded. This intelligent design has been realized with the Shamir scheme [2].

2.2 Issues

Our focus is on the security and efficiency of calculation and transmission as an issue of the threshold cryptosystem. Although there are other issues to be examined such as usability and the environment for usage of the threshold cryptosystem (the degree of assumption of secure communication channels and the degree of reliability of third-party organizations), this research specifically deals with the security of the threshold cryptosystem itself and the efficiency of the cryptosystem's calculation and transmission. Regarding the efficiency of calculation in particular, we aim at a scheme that can be fully realized in mobile terminals. Concerning security, we have examined two points like much other research, the validity of hypothesis for representing security, and security when attacks called chosen ciphertext attacks[*1] is performed. When an encryption scheme is used in various kinds of application, it is known that the scheme should be secure against chosen ciphertext attacks. Therefore, we seek a secure scheme that does not leak any information against the chosen ciphertext attack.

A threshold cryptosystem is known as a type of public key encryption as well as a type of secret sharing scheme. Although

*1 Chosen ciphertext attacks: Attacks by which an attacker can acquire decryption results of arbitrary ciphertexts other than valid ciphertexts that are meant to be broken.

there are several representative public key encryption schemes, a scheme called RSA is the most frequently used among them. The encryption speed of RSA becomes faster than other schemes depending on how it is implemented. In addition, the key size and transmission quantity of RSA are practical, and mobile terminals can handle RSA. However, a simply designed threshold cryptosystem based on RSA as a public key cryptosystem is not secure at all against a chosen ciphertext attack, and there has not been a secure threshold cryptosystem based on RSA. For this reason, we have studied and focused on developing an RSA-based threshold cryptosystem that can ensure security against a chosen ciphertext attack.

2.3 The Public Key Cryptosystem as the Base of Our Proposed Scheme

The proposed scheme in this article is constructed based on a public key encryption scheme in Ref. [9]. **Figure 3** gives the operational principle image of public key encryption. A user encrypts a plaintext with a public key. The public key here is the same as the public key of a threshold cryptosystem. Decryption is easily processed since there is only one decryption key unlike in the case of the threshold cryptosystem. However, there is a possibility not only that ciphertext cannot be decrypted if the decryption key is stolen but also that a person who illegally owns the decryption key can acquire the decryption results of the ciphertext.

The following explanation roughly depicts a chosen ciphertext attack in public key encryption. In a chosen ciphertext attack, an attacker tries to have data decrypted that resemble a ciphertext (hereinafter referred to as "dummy ciphertext"). It can be assumed that the dummy ciphertext is modified for the attacker's purposes and that the attacker may acquire information on the decryption key after the dummy ciphertext has been decrypted. In order to avoid those circumstances, it is important to decrypt a ciphertext only after confirming that the ciphertext is not a dummy ciphertext. However, it is generally indistinctive whether or not the ciphertext is a valid ciphertext, and it presents the problem that dummy ciphertexts may be decrypted. **Figure 4** shows the device of using a stamp [9] to assure security against chosen ciphertext attack. The Ref. [9] shows a technique by which a stamp will not be affixed to a dummy ciphertext. According to this technique, security is assured as a ciphertext will not be decrypted without a stamp. To affix a stamp on a dummy ciphertext would amount to solving an unsolved complex mathematical problem [10]; therefore, it is assured that a ciphertext with a stamp is not a dummy ciphertext.

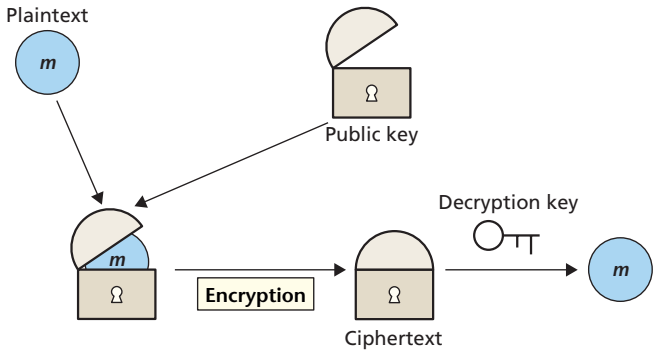


Figure 3 Image of public key encryption

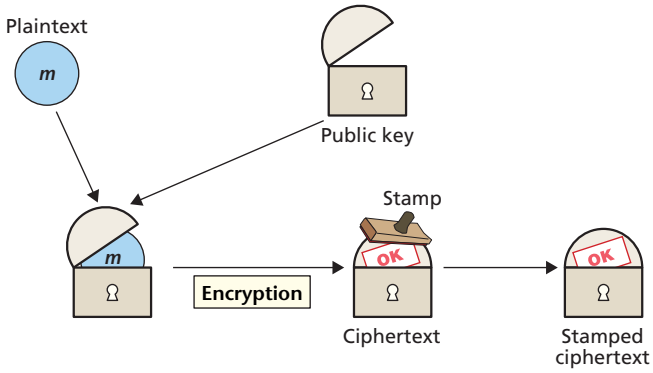


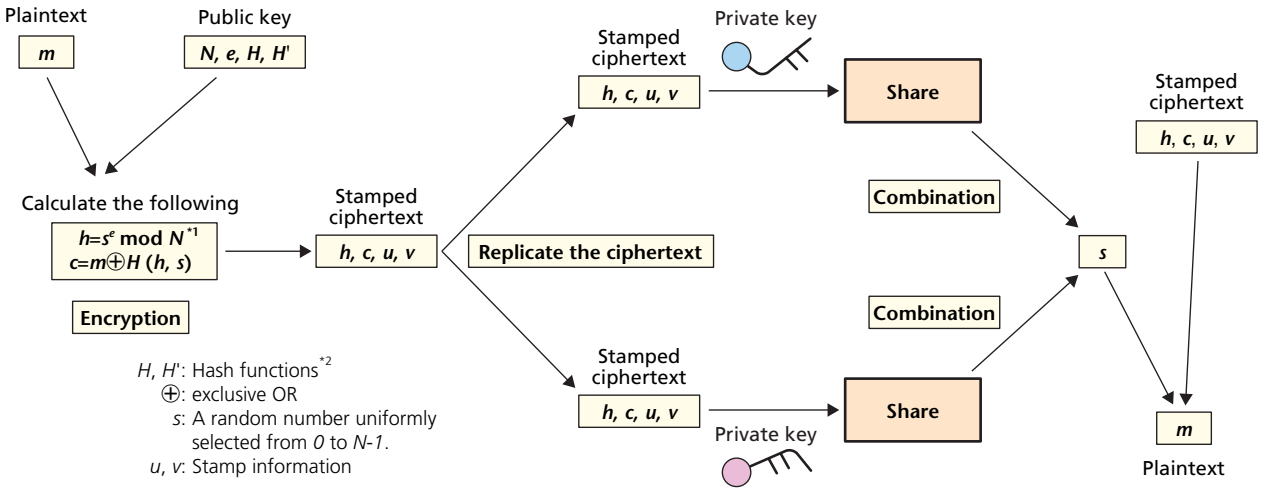
Figure 4 Devices for assuring security

3. The Proposed Scheme

Our research proposes a new scheme which applies the aforementioned stamping scheme to a threshold cryptosystem. It is severer than the normal public key cryptosystem to determine whether a ciphertext is a dummy ciphertext or not. The reason to set a severer condition is that the types of dummy ciphertexts which are suitable for an attacker's purpose are known to be increasing as it is possible to retrieve a share containing modified contents of a plaintext in a threshold cryptosystem as in [11]. In creating a threshold cryptosystem with RSA, the point is to prevent a stamp from being affixed to any ciphertext that is suitable for an attacker's purposes. It is equal to solving an unsolved difficult mathematical problem and proved to be impossible to affix a stamp ignoring the above condition [10].

Figure 5 shows the data flow of our proposed scheme. In order to generate keys, safe primes[*2], p and q, are selected, $N=pq$ is calculated, and a prime number, e, is selected. In the encryp-

*2 Safe prime: When a prime p is a safe prime, p' that fulfills the condition $p=2p'+1$ is also a prime.



*1 *x* mod *N*: The remainder of *N* into *x*.
*2 Hash function: A one-way function that outputs a certain length of data from inputs. SHA-1 is a famous hash function.

Figure 5 Flow of the proposed scheme

tion process, the calculations of h and c correspond to the encryption, and the calculations of u and v correspond to affixing a stamp (The way to create u and v is almost the same as in Ref. [10]). The decryption process of a ciphertext is divided into three parts, "verification," "partial decryption" and "combination." First, it is verified whether a ciphertext to be decrypted has a stamp affixed to it, and the ciphertext is determined to be valid if it has the stamp. The ciphertext, then, is partially decrypted only after verification of its validity. Lastly, shares are combined and the original plaintext is recovered. Because the processes of partial decryption and combination are almost as same as in Ref. [5], their details are not repeated here.

Here we briefly explain the main differences between the proposed scheme and Ref. [9]. If $u=u'$ is true in a dummy ciphertext (h', c', u', v'), decryption results are given to an attacker because of the characteristics of the chosen ciphertext attack. The proposed scheme increases the input of H' more than in Ref. [9] and makes the condition of $u=u'$ more difficult to be true, which means that the proposed scheme admits for a stamp to be affixed only under a severer condition than in the scheme of Ref. [9].

Proposed scheme has advantages as follows. Regarding security, the proposed scheme is as much safe as other existing threshold cryptosystems since it does not leak any information to chosen ciphertext attacks. As to the hypothesis which is the base of security, it is known that the more valid the hypothesis is, the more security is enhanced. Our collaborative research, then, examines a scheme which has a more valid hypothesis called the difficulty of computational problem[*3] with grounds for safety than any other hypothesis used by many threshold cryptosystems. The proof of security is introduced in Ref. [11], and the details of the proof are beyond the scope of this article. The merits regarding efficiency are as follows. The proposed scheme is based on RSA, and therefore the scheme's quantity of calculation for encryption is smaller than other threshold cryptosystems. The proposed scheme has almost the same transmission quantity, ciphertext size, and private key size contained in each mobile terminal as the most efficient existing schemes. Furthermore, the proposed scheme is highly compatible with existing technologies.

In addition, the proposed scheme has a greater calculation quantity than the most efficient scheme described in Ref. [6] regarding partial decryption. However, when the number of private keys is small, the difference between the proposed scheme and the most efficient scheme is also small. In ordinal usage, the difference is not considered to be a considerable issue.

4. Conclusion

In this research, we developed a threshold cryptosystem based on RSA which is proven secure. With this new threshold cryptosystem, secure distributed information management becomes available on mobile terminals. In the future, we will seek a scheme that proves its safety without the hypothesis of Ref. [8].

*3 Computational problem: A problem that requests an answerer to answer descriptively. A computational problem is, generally speaking, more difficult than a decisional problem which requests an answerer to select true or false answers from decision branches.

References

[1] G. Blakely: "Safeguarding cryptographic keys," Afips 1979 Nat. Computer Conf., Vol. 48, Afips Press, pp. 313–317, 1979.

[2] A. Shamir: "How to Share a Secret," Commun. ACM, Vol. 22, No. 11, pp. 612–613, 1979.

[3] Y. Desmedt: "Society and Group Oriented Cryptography: A New Concept," In Crypto87, LNCS 293, Springer-Verlag, pp. 120–127, 1987.

[4] P. A. Fouque and D. Pointcheval: "Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks," ASIACRYPT2001, LNCS 2248, Springer-Verlag, pp. 351–368, 2001.

[5] V. Shoup: "Practical Threshold Signatures," EUROCRYPT 2000, LNCS 1807, Springer-Verlag, pp. 207–220, 2000.

[6] V. Shoup and R. Gennaro: "Securing Threshold Cryptosystems against Chosen Ciphertext Attack," Journal of Cryptology, Vol. 15, No. 2, pp. 75–96, 2002.

[7] R. L. Rivest, A. Shamir and L. M. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun. ACM , Vol. 21, No. 2, 1978.

[8] Y. Tsiounis and M. Yung: "On the Security of ElGamal Based Encryption," PKC1998, LNCS 1431, Springer-Verlag, pp. 117–134, 1998.

[9] M. Abe: "Securing 'Encryption+Proof of Knowledge' in the Random Oracle Model," CT-RSA (The Cryptographer's Track at the RSA Conference) 2002, LNCS 2271, Springer-Verlag, pp. 277–289, 2002.

[10] L. C. Guillou and J.-J. Quisquater: "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Trasmission and Memory," EUROCRYPT 1988, LNCS 330, Springer-Verlag, pp. 123–128, 1988.

[11] T. Ishihara, H. Aono, S. Hongo and J. Shikata: "Construction methods of provably secure threshold cryptosystems in public key setting," The Technical Report of the Institute of Electronics Information and Communication Engineers of Japan, Vol. 105, No. 51, ISEC2005-1 (2005-5), pp. 1–8, 2005 (in Japanese).

Abbreviations

RSA: Rivest-Shamir-Adleman