コンピュータセキュリティ　18−41
(2002.　7.　19)

情報量的安全性に基づく暗号化方式に対する安全性の概念および構成法について

四方　順司[†]　花岡悟一郎[††]　鄭　玉良[†††]　今井　秀樹[††]

[†] 横浜国立大学大学院環境情報研究院　〒240–8501 横浜市保土ヶ谷区常盤台 79–7
[††] 東京大学生産技術研究所　〒153–8505 東京都目黒区駒場 4–6–1
[†††] Department of Software and Information Systems, University of North Carolina at Charlotte,
9201, University City Blvd, Charlotte, NC 28223, USA.
E-mail: [†]shikata@mlab.jks.ynu.ac.jp, [††]hanaoka@imailab.iis.u-tokyo.ac.jp, [†††]yzheng@uncc.edu,
[††††]imai@iis.u-tokyo.ac.jp

あらまし　本稿では，情報量的に安全性が保証される暗号化方式に対しての安全性の概念の解析および構成法に関して考察する．安全性の概念に関しては，新しい概念である "almost perfect secrecy" を与えると共に，頑強性（non-malleability）の概念の情報理論的な立場からの定式化を行う．また，安全性の概念の関係についても明らかにする。さらに本稿では，我々の安全性の定義の意味で安全性が証明可能な暗号化方式に対する構成法を提案する．

キーワード　情報量的安全性，暗号化方式，完全秘匿性，頑強性

Security Notions and Construction Methods for Unconditionally Secure Encryption Schemes

Junji SHIKATA[†], Goichiro HANAOKA[††], Yuliang ZHENG[†††], and Hideki IMAI[††]

[†] Graduate School of Environment and Information Sciences, Yokohama National University
Tokiwadai 79–7, Hodogaya-ku, Yokohama, 240–8501 Japan
[††] Institute of Industrial Science, University of Tokyo　Komaba 4–6–1, Meguro-ku, Tokyo, 153–8505 Japan
[†††] Department of Software and Information Systems, University of North Carolina at Charlotte,
9201, University City Blvd, Charlotte, NC 28223, USA.
E-mail: [†]shikata@mlab.jks.ynu.ac.jp, [††]hanaoka@imailab.iis.u-tokyo.ac.jp, [†††]yzheng@uncc.edu,
[††††]imai@iis.u-tokyo.ac.jp

Abstract　This paper focuses on analysis of security notions and construction methods for encryption schemes whose resistance against attacks is not dependent on unproven computational assumptions. In the aspect of analysis of security notions, this paper introduces a new notion of almost perfect secrecy, gives precise formulation of non-malleability in unconditional setting, and reveals relations among security notions. In addition, this paper proposes construction methods which are provably secure in terms of our strong security definition.

Key words　unconditional security, encryption scheme, perfect secrecy, non-malleability

1. Introduction

In this paper we address security notions and construction methods for encryption schemes that do not depend on any computational assumption. This paper is an extended version of [24] and [25].

Since the discovery of public-key cryptography [10], significant advances have been reported on public-key encryption schemes [21] [14]. However, it is known that a number of technical problems arise if encryption schemes are implemented as suggested in [21] and [14] (For example, see [6]). Thus it is important to have a formal notion of what a secure encryption scheme is, and to construct an encryption scheme which can be proven to be secure in the formal notion. The current standard security notion which was regarded as the strongest notion is non-malleability [12] [13] under adaptive chosen-ciphertext attacks [20] (NM-CCA2) or equivalently indistinguishability [16] under adaptive chosen-ciphertext attacks (IND-CCA2) [4]. So far, many provable secure public-key encryption schemes have been proposed by researchers [3] [9] [19] [5] [27].

These schemes and the infrastructure within which they operate have a limitation in that their underlying security relies on the presumed computational difficulty of certain number-theoretic problems such as the integer factoring problem and the (elliptic curve) discrete logarithm problem. Although the hardness of these problems is unquestioned at the moment, it can be dangerous to base the security of the global information economy on a very small number of mathematical problems. More importantly, in the past several years there have been significant progress in quantum computers. It has been known that the quantum computer can solve both factoring and discrete logarithm problems with ease [7] [26] if it can be realized.

On the other hand, researchers have studied unconditionally secure encryption schemes which do not rely on any unproven assumption, such as the hardness of the integer factoring problem, since the famous information-theoretic work on cryptography by Shannon [22]. Let us briefly look existing unconditionally secure schemes. In [22], Shannon introduced a strong security notion, so-called *perfect secrecy*, of information-theoretic or unconditional security where no limits on an adversary's computational power are assumed. The Vernam's one-time pad is the prime example which satisfies perfect secrecy. Also, some researches dealing with unconditionally secure encryption have been reported with the aim of reducing the size of shared secret keys so as to overcome the limitations imposed by Shannon's result [2] [8] [11] [17]. However, in these results, there exist some assumptions such as *memory-bounded adversaries* or *noisy channel*. In this paper, we study unconditionally secure encryption schemes without any assumption.

As mentioned earlier, the focus of this research is to analyze strong security notions for encryption schemes whose security does not depend on any computational assumption. It is discussed by taking into account the security notions for public-key encryption schemes and additional requirements for encryption schemes in the unconditional security setting. The main contribution for analysis of security notions is to introduce a notion of *almost perfect secrecy*, to give precise formulation of *non-malleability* in unconditional setting, and to reveal relations among security notions. In addition, the other contribution of this paper is to propose construction methods for unconditionally secure encryption schemes.

2. Definitions

2.1 Discussion

In this section, we consider how unconditionally secure encryption should be defined. Of course, *unconditionally secure encryption* implies that the underlying security must not depend on any computational assumption, and that the security of the encryption under consideration here should be guaranteed for an adversary who has unlimited computing power. To address the question, there are two issues to be discussed. The first is how to establish a proper model for encryption schemes, and the second is to define, in a formal way, unconditional security notion in that model.

When introducing a model for unconditionally secure encryption schemes, care should be taken so that properties of public-key encryption schemes are captured. In addition, the model should be as simple as possible.

We start with the following typical model for encryption schemes.

[Definition 1] An *encryption scheme* $\Pi = (GEN, ENC, DEC)$ consists of a key generation algorithm, GEN, an encryption algorithm, ENC, and a decryption algorithm, DEC.

(1) **Key Generation:** The *key generation algorithm* GEN outputs an encryption-key e for a sender and a decryption-key d for a receiver, respectively.

(2) **Encryption:** The *encryption algorithm* takes an encryption-key e and a plaintext m to produce a ciphertext $c := ENC(e, m)$.

(3) **Decryption:** The *decryption algorithm* takes a decryption-key d and a ciphertext c to produce either a plaintext m or a special symbol $\perp$ to indicate that the ciphertext was "invalid", where the precise definition that a ciphertext is *invalid* is provided below.

[Definition 2] Let e be an encryption-key of a sender. Then, a ciphertext c is called *valid* if $c = ENC(e, m)$ for some plaintext m. Otherwise, c is called *invalid.*

To simplify our discussions, we consider a model of encryption schemes in which there are a single receiver R and multiple senders $S_1, S_2, \ldots$. We wish an encryption scheme to fulfill the following requirement.

[Requirement 1]

(1) *Encryption and Decryption:* Any sender can non-interactively create a ciphertext with his encryption-key and the encryption algorithm. Also, a receiver can non-interactively check whether a ciphertext received from a sender is valid with his decryption-key and the decryption algorithm, and can non-interactively recover a correct plaintext if the ciphertext is valid. More precisely, for a receiver R with his decryption-key d, if c is valid, $DEC(d, c) \neq \perp$

and $DEC(d, ENC(e, m)) = m$ for any plaintext m and any pair of matching encryption and decryption key (e, d); and if c is invalid, $DEC(d, c) = \perp$.

(2) *Security:* It is difficult for any adversary to succeed in an attack. Here, we assume that not only any outsider in our model is dishonest but also any user in our model, except a legitimate sender who created a target ciphertext and a legitimate receiver who receives the ciphertext, is not always honest. And each of them may become an adversary who tries an attack.

The security which we require in the above will be discussed for more details in Section 2.2 (see the next subsection).

A part of requirements in Requirement 1 can be relaxed admitting an *small error probability* as follows.

[Requirement 2] A part of *Encryption and Decryption* in Requirement 1 is replaced with the following:

(1) *Encryption and Decryption:* For a receiver R with his decryption-key d, if a ciphertext c is valid, the receiver can always recover a plaintext (i.e. $DEC(d, ENC(e, m)) = m$ for any plaintext m and any pair of matching encryption and decryption key (e, d)); and if c is invalid, DEC does not always returns $\perp$, but the probability that DEC does not erroneously returns $\perp$ (i.e. $DEC(d, c) \neq \perp$ for an invalid ciphertext c) is at most ϵ, where ϵ is not always zero but very small probability.

In encryption schemes based on public-key cryptography, an encryption-key is publicly known and commonly used among plural senders. Then, in order for the encryption scheme to have enough security it is necessary that the encryption algorithm ENC in Definition 1 is probabilistic (see [16]). In fact, if ENC is deterministic, the encryption scheme cannot have *indistinguishability.*

In considering a model of unconditionally secure encryption, we assume that ENC is deterministic so that we can argue the model as simple as possible. Of course, if there exists no encryption that enjoys enough security for an adversary with unlimited computing power under the assumption, it seems to be meaningless to consider such a model in which ENC is deterministic. However, it is shown later that under the assumption an encryption scheme which satisfies a *strong security notion* actually exists, where the *strong security notion* will be precisely defined later. Thus, henceforth in this paper we go on discussion under the assumption that ENC is deterministic.

Although we will give precise definition of strong security later, we can obviously say that an encryption scheme against which an adversary can obtain a corresponding plaintext completely from a ciphertext is insecure. In this sense, we can easily show the following: In encryption schemes based on public-key cryptography, an encryption-key is publicly known and commonly used among plural senders. However, the following insists that it is unlikely in an encryption scheme in which an adversary has unlimited computing power.

[Proposition 1] Suppose that there exists an encryption scheme against which even an adversary with unlimited computing power cannot obtain a corresponding plaintext completely from a ciphertext. Then, in the encryption scheme an encryption-key of each sender must be secret for other senders, where the adversary means an outsider or any user except the legitimate sender and receiver.

Therefore, in an encryption scheme where an adversary has unlimited computing power, from Proposition 1 it follows that key generation algorithm must generate encryption-keys whose number is equal to that of senders and they must be secretly distributed to senders, individually. Thus, this fact make us assume that the number of senders is limited.

In this paper, for simplifying a model we prepare a trusted authority, denoted by TA, whose roles are: to generate encryption-keys and a decryption-key by using a key generation algorithm; and to distribute the decryption-key to the receiver and each encryption-key to each corresponding sender, respectively, in a secure way.

2.2 Security

We now address the security notions in our encryption model: $\mathcal{U} := \{S_1, S_2, \ldots, S_n, R\}$ is a set of users, where S_i $(1 \leqq i \leqq n)$ are all senders and R is a receiver.

In discussing security notions of encryption schemes in public-key cryptography, it is a current standard approach to consider separately the various possible *goals* and various possible *attack models*, and then to obtain each security definition as a pairing of a particular goal and a particular attack model (see [4]). Thus, throughout this paper we also take this idea in discussing security notions of encryption schemes in unconditional security setting.

2.2.1 Goals

In encryption schemes in public-key cryptography, three different goals are mainly considered: *Non-malleability* [12] [13]; *Semantic security* [16]; and *Indistinguishability of encryptions* [16]. First, non-malleability means that given a challenge ciphertext c, it is infeasible for an adversary to create a different ciphertext c', where $c' \neq c$, such that the plaintexts m and m' of these ciphertexts c and c', respectively, are meaningfully related (for example, $m' = m + 1$). Secondly, semantic security is a computational analogue of Shannon's definition of *perfect secrecy* [22], and hence means that given a challenge ciphertext c, it is infeasible for an adversary to derive any partial information on the plaintext m underlying the ciphertext c. Finally, indistinguishability of encryptions means that it is infeasible for an adversary to distinguish encryptions of any known pair of plaintexts. This definition is technical in nature, and is known to be equivalent to semantic security [16].

As a strong security definition, perfect secrecy due to Shannon [22] is widely recognized. And of course we should take into account this notion in considering security notions of encryption in unconditional security setting. In this paper, we also consider *almost perfect secrecy* which is a relaxed notion of perfect secrecy: *Almost Perfect Secrecy* means that given a challenge ciphertext c, the partial information on the plaintext from the ciphertext which an adversary can derive might exist, but it is very small.

In addition, taking into account security definitions of encryption schemes in public-key cryptography, it is reasonable to consider an information-theoretic analogue of the non-malleability. Thus, in this paper we consider the following security definitions in unconditionally secure encryption schemes:

[Definition 3] (Security Notions: Goals)

(1) Perfect Secrecy (PS): It is difficult for an adversary to derive any partial information on the plaintext from a target ciphertext.

(2) Almost Perfect Secrecy (APS): The partial information on the plaintext from a target ciphertext which an adversary can derive might exist, but it is very small.

(3) Non-Malleability (NM): Given a challenge ciphertext c, it is difficult for an adversary to create a different ciphertext c', where $c' \neq c$, such that the plaintexts m and m' of these ciphertexts c and c', respectively, are meaningfully related.

2.2.2 Attacking models

In this section we consider attacking models for encryptions in unconditional security setting. We address two points: one is on the secrecy of a receiver's decryption-key; and another is on that of each sender's encryption-key.

On the secrecy of a receiver's decryption-key, the following security notions can be considered as well as that of encryption schemes in public-key cryptography [18] [20].

[Definition 4] (Attacking Models against a Receiver): In the following, an *adversary* means a dishonest sender or an outsider in our model.

(1) *Cihertext-Only Attacks (COA)*: If a dishonest sender is adversary, the information which the adversary can use is that of his encryption-key for attacking the challenge ciphertext. If an outsider is an adversary, information avaiable to him is only publicly known information for attacking the challenge ciphertext.

(2) *(Generalized) Non-adaptive Chosen-Ciphertext Attacks ((g)CCA or (g)CCA1)* [18] [1]: An adversary gets access to an oracle for the decryption function. In CCA (or CCA1), the adversary may use this decryption function only for the period of time preceding his being given the challenge ciphertext. We also generalize the above CCA (CCA1) to gCCA (gCCA1) with respect to some relation $\Im(\cdot,\cdot)$ on the ciphertexts which is recognizable to everyone. If two ciphertexts c_1 and c_2 ($c_1 \neq c_2$) satisfy $\Im(c_1, c_2) = 1$, $DEC(d, c_1) = DEC(d, c_2)$ for any decryption-key d. In gCCA, the adversary cannot ask not only the challenge ciphertext c but also any c' equivalent to c with respect to $\Im(\cdot,\cdot)$, that is, any c' with $\Im(c, c') = 1$.

(3) *(Generalized) Adaptive Chosen-Ciphertext Attacks ((g)ACCA or (g)CCA2)* [20] [1]: An adversary gets access to an oracle for the decryption function. In ACCA (or CCA2), the adversary may use this decryption function not only for the period of time preceding his being given the challenge ciphertext, but also after obtaining the challenge ciphertext. The only restriction is that the adversary may not ask for the decryption of the challenge ciphertext itself. We can also generalize the above ACCA (CCA2) to gACCA (gCCA2) as in the case of gCCA.

We next consider attacking models on the secrecy of a sender's encryption-key, as well. We introduce attacking models against a sender S based on the idea of Definition 4.

[Definition 5] (Attacking Models against a Sender): Let S be a sender. In the following, an *adversary* means a dishonest sender or an outsider in our model.

(1) *Cihertext-Only Attacks (COA)*: If a dishonest sender is adversary, the information which the adversary can use is that of his encryption-key for attacking the challenge ciphertext. If an outsider is an adversary, information avaiable to him is only publicly known information for attacking the challenge ciphertext.

(2) *Non-adaptive Chosen-Plaintext Attacks for S (CPA or CPA1)*: An adversary gets access to an oracle for the encryption function of S. The adversary may use this encryption function only for the period of time preceding his being given the challenge ciphertext.

(3) *Adaptive Chosen-Plaintext Attacks for S (ACPA or CPA2)*: An adversary gets access to an oracle for the encryption function of S. The adversary may use this encryption function not only for the period of time preceding his being given the challenge ciphertext, but also after obtaining the challenge ciphertext.

Therefore, a strong notion of attacking models is *ACPA and (g)ACCA*: An adversary gets to an oracle for the encryption function of any sender. The adversary may use this encryption function not only for the period of time preceding his being given the challenge ciphertext, but also after obtaining the challenge ciphertext. In addition, the adversary gets access to an oracle for the decryption function. The adversary may use this decryption function not only for the period of time preceding his being given the challenge ciphertext, but also after obtaining the challenge ciphertext. The only restriction is that the adversary may not ask for the decryption of the challenge ciphertext itself (and equivalent ciphertexts).

2.2.3 Strong security notions

In this section, we summarize a strong security notion based on the argument in Sections 2.2.1 and 2.2.2. From Definitions 3, 4 and 5, we can conclude:

[Definition 6] (Strong Security Notion) Let Π be an encryption scheme. Then, Π is called *secure* if Π satisfies both (A)PS-ACPA&(g)ACCA and NM-ACPA&A(g)CCA, where ACPA&(g)ACCA means ACPA and (g)ACCA.

2.3 Some Remarks on Security Notions

2.3.1 The security parameter

In defining a precise model of unconditionally secure encryption schemes, we introduce the notions of *security parameter* which is usually introduced in encryption schemes with computational security in public-key cryptography. As well as a security parameter in public-key encryption schemes, a security parameter in the context of unconditionally secure encryption is introduced as follows:

[Definition 7] A *security parameter* k is a parameter which determines: (1) overall security; (2) the key-length of encryption-keys and that of decryption-keys; (3) the length of plaintexts and that of ciphertexts; (4) the running time of encrypting and decrypting algorithms.

2.3.2 The number of colluders

It is resonable to assume that some dishonest users might collude to succeed an attack. Thus, we adopt the idea of threshold scheme. Namely, we assume that there exists at most ω colluders among the users $\mathcal{U} = \{S_1, S_2, \ldots, S_n, R\}$.

2.3.3 The numbers of encrypting and decrypting operations

In order to strictly give security notions, we should introduce the number up to which an adversary can have access to an encryption oracle, and the number up to which the adversary can have access to a decryption oracle. In this paper, we introduce the number up to which each sender is allowed to encrypt plaintexts, denoted by ψ, and the number up to which the receiver is allowed to decrypt ciphertexts, denoted by ψ'. This implies that in order to decrypt a target ciphertext an adversary can obtain at most $\psi - 1$ pairs of some plaintexts and corresponding ciphertexts from the target sender by using him as an encryption oracle, and that the adversary can obtain at most ψ' pairs of some ciphertexts and corresponding plaintexts from the receiver by using him as a decryption oracle.

3. Security notions and their relations

3.1 The model

As mentioned in the previous section, we consider the following model of encryption schemes.

[Definition 8] An *encryption scheme* Π consists of ($\mathcal{U}$, TA, $\mathcal{M}$, $\mathcal{C}$, $\mathcal{E}$, $\mathcal{D}$, GEN, ENC, DEC):

1. **Notation:**

- $\mathcal{U} := \{S_1, S_2, \ldots, S_n, R\}$ is a finite set of users, where R is a receiver and others $S_i (1 \leqq i \leqq n)$ are senders,
- TA is a trusted authority,
- $\mathcal{M} = \{\mathcal{M}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible plaintexts. Here, k is a security parameter and $\mathcal{M}_k \subset \{0,1\}^{l_M(k)}$, where $l_M(k)$ is a polynomial of k,
- $\mathcal{C} = \{\mathcal{C}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible ciphertexts. Here, k is a security parameter and $\mathcal{C}_k \subset \{0,1\}^{l_C(k)}$, where $l_C(k)$ is a polynomial of k,
- $\mathcal{E} = \{\mathcal{E}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible encryption-keys. Here, k is a security parameter and $\mathcal{E}_k \subset \{0,1\}^{l_E(k)}$, where $l_E(k)$ is a polynomial of k,
- $\mathcal{D} = \{\mathcal{D}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible decryption-keys. Here, k is a security parameter and $\mathcal{D}_k \subset \{0,1\}^{l_D(k)}$, where $l_D(k)$ is a polynomial of k,
- GEN is a key generation algorithm which outputs encryption-keys and a decryption-key,
- $ENC : \mathcal{E} \times \mathcal{M} \longrightarrow \mathcal{C}$ is an encryption algorithm,
- $DEC : \mathcal{D} \times \mathcal{C} \longrightarrow \mathcal{M} \bigcup \{\perp\}$ is a decryption algorithm.

2. **Key Generation and Distribution by TA:** The TA generates an *encryption-key* $e_i \in \mathcal{E}$ for each sender S_i, and a *decryption-key* $d \in \mathcal{D}$ for a receiver R using GEN. Here GEN is a probabilistic algorithm which produce, on input 1^k, where k is a security parameter, keys $(e_1, e_2, \ldots, e_n, d)$ of matching encryption and decryption keys, where $e_i \in \mathcal{E}_k$ for $1 \leqq i \leqq n$ and $d \in \mathcal{D}_k$. Then, TA transmits the encryption-key e_i to the sender S_i and the decryption-key d to the receiver R via a secure channel. After delivering these keys, the TA may erase the keys $(e_1, e_2, \ldots, e_n, d)$ from his memory. Each sender keeps secret his encryption-key, and the receiver keeps secret his decryption-key.

3. **Encryption:** For a plaintext $m \in \mathcal{M}_k$, the sender S_i generates a ciphertext $c = ENC(e_i, m) \in \mathcal{C}_k$ by using his encryption-key e_i in conjunction with ENC. Here, we assume that ENC is deterministic, but in general it might be a randomized algorithm. If it is deterministic, for a plaintext m and an encryption-key e_i, the ciphertext $c := ENC(e_i, m)$ is uniquely determined, while in the case of a randomized algorithm many different ciphertexts can be produced for the same plaintext.

4. **Decryption:** On receiving a ciphertext c from a

sender S_i, the receiver R recovers a plaintext using his decryption-key d and DEC. More precisely, if $DEC(d,c) = \perp$, R regards the received ciphertext c as invalid. Otherwise, R recovers the plaintext $m = DEC(d,c)$ as valid ciphertext. Here, we assume that DEC is deterministic.

Let ψ and ψ' be the number up to which each sender is allowed to encrypt plaintexts and the number up to which the receiver is allowed to decrypt ciphertexts, respectively, and let ω be the number of possible colluders among users. Let $\mathcal{W} := \{W \subset \mathcal{U} | \, |W| \leqq \omega\}$. Each element of $\mathcal{W}$ represents a group of possibly collusive users. For a set $\mathcal{T}$ and a non-negative integer t, let $\wp_t^{\mathcal{T}} := \{T \subset \mathcal{T} \mid |T| \leqq t\}$ be the family of all subsets of $\mathcal{T}$ whose cardinality are less than or equal to t. Of course, the empty set $\emptyset$ is always contained in $\wp_t^{\mathcal{T}}$.

With notations above, we will discuss the security notions in unconditionally secure encryption schemes in the sequel.

3.2 Security notions

In this subsection, we formally define security notions based on the argument in Section 2. First of all, we define an *exponentially negligible function* as follows.

[Definition 9] (Exponentially Negligible Function) Let $\epsilon(k)$ be a function defined over the positive integers $k \in \boldsymbol{N}$ that takes non-negative real numbers. Then, $\epsilon(k)$ is called *exponentially negligible* if there exists an integer k_0 and some constant a $(1 < a)$ such that $\epsilon(k) \leqq \frac{1}{a^k}$ for all $k \geqq k_0$.

Using the notations introduced in this section, we now formulate the strong security notions in Definition 6, that is, (A)PS-ACPA&(g)ACCA and NM-ACPA&(g)ACCA along with our encryption model. First, we give PS-ACPA&(g)ACCA as follows.

[Definition 10] (Perfect Secrecy under ACPA&gACCA) (cf: [22]) Let k be a security parameter. Let $\Pr(m)$ be probability distribution on M. For $W \in \mathcal{W}$ such that $S_j, R \notin W$, we define

$$\begin{aligned} P^{PS}(S_j, W) := & \max_{e_W} \max_{M_{S_j}=\{m_{S_j}, c_{S_j}\}} \\ & \max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_n}(l \neq j)} \max_{C_R} \max_{c} \\ & |\Pr(m \mid c, e_W, M_{S_1}, \ldots, M_{S_n}, C_R) - \Pr(m)|, \end{aligned}$$

where e_W is taken over all possible combination of encryption-keys of W; $M_{S_j} = \{m_{S_j}, c_{S_j}\}$ is taken over $\wp_{\psi-1}^{\mathcal{M}_k \times \mathcal{C}_k}$ such that any element (m_{S_j}, c_{S_j}) of M_{S_j} is a pair of a plaintext m_{S_j} and a corresponding ciphertext c_{S_j} encrypted by S_j; $M_{S_l}(l \neq j)$ is taken over $\wp_{\psi}^{\mathcal{M}_k \times \mathcal{C}_k}$ such that any element (m_{S_l}, c_{S_l}) of M_{S_l} is a pair of a plaintext m_{S_l} and a corresponding ciphertext c_{S_l} encrypted by S_l; C_R is taken over $\wp_{\psi'}^{\mathcal{C}_k \times (\mathcal{M}_k \bigcup \{\perp\})}$ such that any element of C_R is a pair of a ciphertext c_R and a decryption result of c_R by R; and c is taken over valid ciphertexts which is not equivalent to any $c_R \in C_R$ with respect to any recognizable relation $\Im(\cdot,\cdot)$. Furthermore, we define $P^{PS} := \max_{S_j, W} P_1^{PS}(S_j, W)$. Then, we require $P^{PS} = 0$.

Next, we define *almost perfect secrecy* which means that the information on the plaintext obtained from the target ciphertext is exponentially negligible, which is new and a relaxed notion of perfect secrecy.

[Definition 11] (Almost Perfect Secrecy under ACPA&gACCA) Let k be a security parameter and $\epsilon(k)$ an exponentially negligible function. For simplicity, we denote the exponentially negligible function $\epsilon(k)$ by ϵ. We define P^{PS} as in Definition 10. Then, we require $P^{PS} \leqq \epsilon$.

Finally, we define an information-theoretic analogue of the non-malleability as follows. To the authors' current knowledge, this is the first time when the formulation is precisely presented.

[Definition 12] (Non-Malleability under ACPA&gACCA) Let k be a security parameter and $\epsilon(k)$ an exponentially negligible function. For simplicity, we denote the exponentially negligible function $\epsilon(k)$ by ϵ. For a relation $\Re$ on $\mathcal{M}_k$, we write $\Re(x_1, x_2) = 1$ if the relation $\Re$ holds for $x_1, x_2 \in \mathcal{M}_k$, and we write $\Re(x_1, x_2) = 0$ otherwise. For any relation $\Re$ on $\mathcal{M}_k$, we extend $\Re$ to the relation $\hat{\Re}$ on $\mathcal{M}_k \bigcup \{\perp\}$ as follows:

$$\hat{\Re}(x_1, x_2) := \begin{cases} \Re(x_1, x_2) & \text{if } x_1, x_2 \in \mathcal{M}_k \\ 0 & \text{if } x_1 = \perp \text{ or } x_2 = \perp \end{cases}$$

For $W \in \mathcal{W}$ such that $S_j, R \notin W$ and a relation $\Re$ on $\mathcal{M}_k$, we define

$$\begin{aligned} P^{NM}(\Re; S_j, W) := & \max_{e_W} \max_{M_{S_j}=\{m_{S_j}, c_{S_j}\}} \\ & \max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_n}(l \neq j)} \max_{C_R} \max_{c} \max_{c'} \\ & |\Pr_d(\hat{\Re}(DEC(d,c), DEC(d,c')) = 1 | c, c', e_W, \\ & M_{S_1}, \ldots, M_{S_n}, C_R) - \Pr_{d,m}(\hat{\Re}(m, DEC(d,c')) = 1)|, \end{aligned}$$

where e_W is taken over all possible combination of encryption-keys of W; $M_{S_j} = \{m_{S_j}, c_{S_j}\}$ is taken over $\wp_{\psi}^{\mathcal{M}_k \times \mathcal{C}_k}$ such that any element (m_{S_j}, c_{S_j}) of M_{S_j} is a pair of a plaintext m_{S_j} and a corresponding ciphertext c_{S_j} encrypted by S_j; $M_{S_l}(l \neq j)$ is taken over $\wp_{\psi}^{\mathcal{M}_k \times \mathcal{C}_k}$ such that any element (m_{S_l}, c_{S_l}) of M_{S_l} is a pair of a plaintext m_{S_l} and a corresponding ciphertext c_{S_l} encrypted by S_l; C_R is taken over $\wp_{\psi'-1}^{\mathcal{C}_k \times (\mathcal{M}_k \bigcup \{\perp\})}$ such that any element of C_R is a pair of a ciphertext c_R and a decryption result of c_R by R; c is taken over valid ciphertexts generated by S_j; and c' is taken over ciphertexts such that $c' \neq c$. Here c is not equivalent to c' with respect to any recognizable relation $\Im(\cdot,\cdot)$, and both c and c' are also not equivalent to any ciphertext in C_R with respect to $\Im(\cdot,\cdot)$. Furthermore, we define

$$P^{NM}(\Re) := \max_{S_j, W} P^{NM}(\Re; S_j, W).$$

Then, we require that for any relation $\Re$, $P^{NM}(\Re) \leq \epsilon$.

3.3 Relations among security notions

In this subsection, we reveal relations among security notions. Among security notions, we consider the following notions: three goals, that is, *Perfect Secrecy (PS)*, *Almost Perfect Secrecy (APS)* and *Non-Malleability (NM)*; and two attacking models, that is, *Ciphertext-Only Attacks (COA)* which is the most powerless attacking model, and *Adaptive Chosen-Plaintext Attacks and generalized Adaptive Chosen-Ciphertext Attacks (ACPA&gACCA)* which is the most powerful attacking model.

[Theorem 1] The following relations among security notions hold:

$$\begin{tikzcd}
\text{NM-ACPA\&gACCA} \arrow[r, "/" marking] \arrow[d, shift right] \arrow[rr, bend left, "/" marking] & \text{PS-ACPA\&gACCA} \arrow[r, shift left] \arrow[d, shift right] & \text{APS-ACPA\&gACCA} \arrow[l, shift left, "/" marking] \arrow[d, shift right] \\
\text{NM-COA} \arrow[u, shift right, "/" marking] \arrow[r, shift left, "/" marking] \arrow[rr, bend right, shift left, "/" marking] & \text{PS-COA} \arrow[u, shift right, "/" marking] \arrow[l, shift left, "/" marking] \arrow[r, shift left] & \text{APS-COA} \arrow[u, shift right, "/" marking] \arrow[l, shift left, "/" marking] \arrow[ll, bend left, shift left, "/" marking]
\end{tikzcd}$$

where "X $\longrightarrow$ Y" means that X always implies Y, while "X $\not\longrightarrow$ Y" means that there exists an encryption scheme which is X but not Y.

4. Construction

In this section we propose construction methods for encryption schemes which is secure in our strong security notion (See Definition 6). We present two kinds of construction methods: One is a generic construction method for strong encryption schemes by the use of weak encryption schemes and signature schemes; and another is a concrete construction method for strong encryption schemes by the use of polynomials over finite fields.

4.1 A Generic Composition Method

We present a generic construction method for encryption schemes which is secure in our strong security notion. Loosely speaking, the construction for strong encryption schemes can be obtained by combining weak encryption schemes and signature schemes. More precisely, we can show the following.

[Theorem 2] If there exist an encryption scheme which is APS-COA and a signature scheme which is EAUF-ACMA&ACSA, we can construct an encryption scheme which is APS-ACPA&gACCA and NM-ACPA&gACCA, where "EAUF-ACMA&ACSA" means *Existentially Acceptance UnForgeability under Adaptive Chosen-Message Attacks and Adaptive Chosen-Signature Attacks* which is a strong security notion for unconditionally secure signature schemes proposed in [23].

[Remark 1] From Theorem 2 we can actually construct an encryption scheme which satisfies APS-ACPA&gACCA and NM-ACPA&gACCA. In fact, we can take one-time pad as an encryption satisfying APS-COA and can consider a similar construction of a signature scheme which is EAUF-ACMA&ACSA as in [23].

4.2 An Efficient Construction Method

In this subsection, we propose a concrete construction method for strong encryption schemes by the use of polynomials over finite fields. Essentially, the underlying idea of the construction presented in this subsection is based on Remark 1. However, the construction is better than the construction obtained by directly applying the idea in Remark 1, since the required memory size of the keys in the former construction is less than that of the keys in the latter.

In the following, we propose a construction of key generation algorithm, *GEN*, encryption algorithm, *ENC*, and decryption algorithm, *DEC* along with our model. In the sequel, we use the notations introduced in the previous sections.

- **GEN:** The key generation algorithm, *GEN*, which, on input 1^k, picks a k-bit prime power q, constructs a finite field $\boldsymbol{F}_q$ with q elements. We assume that the identity of each sender S_i is also denoted by S_i and that $S_i \in \boldsymbol{F}_q$. It also picks uniformly at random a polynomial over $\boldsymbol{F}_q$ with two variables $f(X, Y)$ and two polynomials over $\boldsymbol{F}_{q^3}$ with $(\psi + \omega + 2)$ variables $g_s(X, Y_1, Y_2, \ldots, Y_{\psi+\omega}, Z) (s = 1, 2)$ as follows:

$$f(X, Y) = \sum_{i=0}^{\omega} \sum_{j=0}^{\psi} a_{ij} X^i Y^j$$

$$g_s(X, Y_1, Y_2, \ldots, Y_{\psi+\omega}, Z) = \sum_{i=0}^{n-1} \sum_{j=1}^{\psi+\omega} \sum_{k=0}^{\psi} b_{ijk}^{(s)} X^i Y_j Z^k$$

$$+ \sum_{i=0}^{n-1} \sum_{k=0}^{\psi} b_{i0k}^{(s)} X^i Z^k \quad (s = 1, 2) \ (a_{ij} \in \boldsymbol{F}_q, b_{ijk}^{(s)} \in \boldsymbol{F}_{q^3}).$$

where the coefficients a_{ij} are chosen uniformly at random from $\boldsymbol{F}_q$ and the coefficients $b_{ijk}^{(s)}$ are chosen uniformly at random from $\boldsymbol{F}_{q^3}$.

Moreover, it uniformly at random picks two elements $v^{(1)}, v^{(2)}$ $(\in (\boldsymbol{F}_{q^3})^{\psi+\omega})$. Then, an encryption-key e_i of a sender S_i is

$$e_i = (f(S_i, Y), g_1(S_i, Y_1, \ldots, Y_{\psi+\omega}, Z), g_2(S_i, Y_1, \ldots, Y_{\psi+\omega}, Z))$$

and a decryption-key d of the receiver R is

$$d = (f(X, Y), v^{(1)}, v^{(2)}, g_1(X, v^{(1)}, Z), g_2(X, v^{(2)}, Z)).$$

The algorithm *GEN* returns $(\boldsymbol{F}_q, \boldsymbol{F}_{q^3}, \Phi, \Psi)$ and $(e_1, e_2, \ldots, e_n, d)$, where $\Phi : {\boldsymbol{F}_q}^3 \longrightarrow \boldsymbol{F}_{q^3}$ is an isomorphism of vector spaces over $\boldsymbol{F}_q$, and $\Psi : \{1, 2, \ldots, \psi\} \longrightarrow \boldsymbol{F}_q$ is an injective map.

For simplicity, we assume that $(\boldsymbol{F}_q, \boldsymbol{F}_{q^3}, \Phi, \Psi)$ is publicly known information and that $\mathcal{M}_k \subset \boldsymbol{F}_q$ in the sequel.

- **ENC:** When a sender S_i encrypts a plaintext $m \in \boldsymbol{F}_q$, ENC computes :

$$\begin{aligned}
&f(S_i, \Psi(l)) = f(S_i, Y)|_{Y=\Psi(l)} \\
&c' := m + f(S_i, \Psi(l)) \\
&a_1 := g_1(S_i, Y_1, \ldots, Y_{\psi+\omega}, Z)|_{Z=\Phi(S_i,\Psi(l),c')} \\
&a_2 := g_2(S_i, Y_1, \ldots, Y_{\psi+\omega}, Z)|_{Z=\Phi(S_i,\Psi(l),c')}
\end{aligned}$$

where $l(l = 1, 2, \ldots, \psi)$ is a counter and it means that this generation of a ciphertext is exactly the l-th generation. Note that the number up to which each sender is allowed to generate ciphertexts is ψ. Then, the ciphertext of the plaintext m is $c := (S_i, l, c', a_1, a_2)$.

- **DEC:** On inputting a ciphertext $c = (S_i, l, c', a_1, a_2)$, DEC computes:

$$\begin{aligned}
r_s &:= a_s|_{(Y_1,\ldots,Y_{\psi+\omega})=v^{(s)}} \qquad (s = 1, 2) \\
r'_s &:= g_s(X, v^{(s)}, Z)|_{X=S_i, Z=\Phi(S_i,\Psi(l),c')} \qquad (s = 1, 2).
\end{aligned}$$

Then, if $r_1 = r'_1$ and $r_2 = r'_2$, the plaintext is recovered by computing $m = c' - f(X, Y)|_{X=S_i, Y=\Psi(l)}$. Otherwise, DEC regards the ciphertext c as invalid, and outputs $\perp$.

Then, we can show the following result.

[Theorem 3] The above construction results in an encryption scheme which satisfies APS-ACPA&gACCA and NM-ACPA&gACCA under the following conditions: there exist at most ω colluders; the maximum number up to which each sender is allowed to encrypt plaintexts is at most ψ; and the maximum number up to which the receiver is allowed to decrypt ciphertexts is at most ψ.

5. Conclusion

This paper presented the analysis of security notions and construction methods for unconditionally secure encryption schemes. This paper introduced a new notion of almost perfect secrecy, gave precise formulation of non-malleability in unconditional setting, and revealed relations among security notions. In addition, this paper proposed construction methods which are provably secure in terms of our strong security definition.

文　献

[1] J. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption", Proc. of Eurocrypt 2002, Springer-Verlag, 2002.

[2] Y. Aumann and M. O. Rabin, "Information theoretically secure communication in the limited storage space model", Proc. of Crypto 99, Springer-Verlag, 1999.

[3] M. Bellare and P. Rogaway, "Optimal asymmetric encryption", Proc. of Eurocrypt 94, Springer-Verlag, 1994.

[4] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, "Relations among notions of security for public-key encryption schemes", Proc. of Crypto 98, Springer-Verlag, 1998.

[5] D. Boneh, "Simplified OAEP for the RSA and Rabin functions", Proc. of Crypto 2001, LNCS 2139, 275-291, Springer-Verlag, 2001.

[6] D. Boneh, A. Joux, and P. Q. Nguyen, "Why textbook ElGamal and RSA encryption are insecure", Proc. of Asiacrypt 2000, LNCS 1976, 30-43, Springer-Verlag, 2000.

[7] D. Boneh and R. J. Lipton, "Quantum cryptanalysis of hidden linear functions", Proc. of Crypto '95, LNCS 963, Springer-Verlag, 424-437, 1995.

[8] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries", Proc. of Crypto 97, Springer-Verlag, 1997.

[9] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", Proc. of Crypto 98, Springer-Verlag, 1998.

[10] W. Diffie and H. Hellman, "New directions in cryptography", IEEE Trans. on IT 22, 6, 644-654, 1976.

[11] Y. Z. Ding and M. O. Rabin, "Provably secure and non-malleable encryption", preprint, 2001.

[12] D. Dolev, D. Dwork and M. Naor, "Non-malleable cryptography", In 23rd Annual ACM Symposium on Theory of Computing, 542-552, 1991.

[13] D. Dolev, D. Dwork and M. Naor, "Non-malleable cryptography", SIAM J. Comput., 30 (2), 391-437, 2000.

[14] T. ElGamal, "A public-key cryptosystem and a signature scheme based on the discrete logarithm", IEEE Trans. on IT 31 (4), 469-472, 1985.

[15] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, "RSA-OAEP is secure under the RSA assumption", Proc. of Crypto 2001, LNCS 2139, Springer-Verlag, 260-274, 2001.

[16] S. Goldwasser and S. Micali, "Probabilistic encryption", Journal of Computer and System Science 28, 270-299, 1984.

[17] U. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher", Journal of Cryptography 5, 53-66, 1992.

[18] M. Naor and M. Young, "Public-key cryptosystems provably secure against chosen ciphertext attacks", In 22nd Annual ACM Symposium on Theory of Computing, 427-437, 1990.

[19] T. Okamoto, E. Fujisaki, S. Uchiyama and H. Morita, "Public-key encryption schemes: EPOC and PSEC", IEICE Technical Report, ISEC 2000-9, May 2000.

[20] C. Rackoff and D. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack", Proc. of Crypto '91, Springer-Verlag, 433-444, 1991.

[21] R. L. Rivest, A. Shamir and L. M. Adleman, "A method of obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21 (2), 120-126, 1978.

[22] C. E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, vol. 28, pp.656-715, 1949.

[23] J. Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Security notions for unconditionally secure signature schemes", Proc. of Eurocrypt 2002, Springer-Verlag, 2002.

[24] J. Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Unconditionally secure encryption schemes" (in Japanese), Proc. of SITA 2001, 2001.

[25] J. Shikata, G. Hanaoka, Y. Zheng and H. Imai, "Unconditionally secure encryption: a model, security notions and construction methods"(in Japanese), Proc. of SCIS 2002, 2002.

[26] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comp., 26, no.5, 1484-1509, 1997.

[27] V. Shoup, "OAEP Reconsidered", Proc. of Crypto 2001, LNCS 2139, 239-259, Springer-Verlag, 2001.