On the Security of Multiple Encryption or CCA-security+CCA-security=CCA-security?

Rui Zhang[1], Goichiro Hanaoka[1⋆], Junji Shikata[2], and Hideki Imai[1]

[1] Institute of Industrial Science, University of Tokyo, Japan
{zhang,hanaoka}@imailab.iis.u-tokyo.ac.jp, imai@iis.u-tokyo.ac.jp
[2] Graduate School of Environment and Information Science,
Yokohama National University, Japan
shikata@ynu.ac.jp

Abstract. In a practical system, a message is often encrypted more than once by different encryptions, here called multiple encryption, to enhance its security. Additionally, new features may be achieved by multiple encrypting a message, such as the key-insulated cryptosystems and anonymous channels. Intuitively, a multiple encryption should remain "secure", whenever there is one component cipher unbreakable in it. In NESSIE's latest Portfolio of recommended cryptographic primitives (Feb. 2003), it is suggested to use multiple encryption with component ciphers based on different assumptions to acquire long term security. However, in this paper we show this needs careful discussion, especially, this may *not* be true according to adaptive chosen ciphertext attack (CCA), even with all component ciphers CCA-secure. We define an extended model of (standard) CCA called *chosen ciphertext attack for multiple encryption* (ME-CCA) emulating partial breaking of assumptions, and give constructions of multiple encryption satisfying ME-CCA-security. We further relax CCA by introducing *weak* ME-CCA (ME-wCCA) and study the relations among these definitions, proving ME-wCCA-security can be acquired by combining IND-CCA-secure component ciphers together. We then apply these results to key-insulated cryptosystem.

1 Introduction

A practical cryptosystem often encrypts a message several times with independent secret keys or even distinct encryption schemes based on different assumptions to enhance the confidentiality of message. We call such cryptosystems multiple encryption, specifically double encryption and triple encryption for two times and three times multiple encryptions respectively. In this paper, we investigate the security notion of multiple encryption against partial breaking of underlying assumptions as well as key exposure.

⋆ The second author is supported by a Research Fellowship from Japan Society for the Promotion of Science (JSPS).

Why Multiple Encryption. It is widely believed that multiple encryption provides better security because even if underlying assumptions of some component ciphers are broken or some of the secret keys are compromised, the confidentiality can still be maintained by the remaining encryptions. Historically, sudden emergence of efficient attacks against the elliptic curve cryptosystem on supersingular curves [?,?] and on prime-field anomalous curves [?,?,?] have already reminded us the necessity to do this. Especially, it is suggested by NESSIE ([?], pp. 5, line 7-11) on asymmetric encryption scheme to "*use double encryption using ACE-KEM and RSA-KEM with different DEMs gives a good range of security, based on various different assumptions*", "*if very long term security is important*". Furthermore, "*Triple encryption that also uses a public-key scheme not based on number-theoretical assumptions might increase the security against future breakthrough*". However, it seems that this needs more careful discussions.

On the other hand, multiple encryption can bring favorable additional new features to a scheme. Combination of ordinary threshold encryptions may yield new threshold encryption with various access structures. Many practical applications achieving sender anonymity via practical open network, like Mix-net [?,?], onion routing [?] and key-insulated cryptosystems [?] are all practical examples of multiple encryption.

Contradiction to the Intuition. In this paper, we show that even if it consists of only *independently* selected semantically secure against adaptive chosen ciphertext attack (IND-CCA) secure components, a multiple encryption is not necessarily secure against chosen ciphertext attack (CCA) with with partial component ciphers broken. This contradicts our intuition at the first sight, but such "natural" constructions of multiple encryption can be shown easily to lose the CCA-security. Meanwhile, this result may imply CCA-security is too strong because practical schemes with "pretty good" security could be considered insecure in the sense. Then we propose a generic construction of multiple encryption scheme achieving CCA-security exactly. On the other hand, we relax security definition based on the "natural" constructions emphasizing practical usability, and investigate the relations among security notions for multiple encryption. Finally as a byproduct, we give the first generic construction of CCA-secure key-insulated cryptosystem.

1.1 Related Work

Multiple Encryption and Related Primitives. Multiple encryption has been used in practical schemes, for instance Triple DES. NESSIE [?] has also lately announced its recommendation to use (public key) multiple encryption with encryptions under diverse assumptions to ensure long term security. Another example is the key-insulated cryptosystem, proposed by Dodis, Katz, Xu and Yung [?], whose generic construction is actually multiple encryption of messages under a number of keys from cover free family [?].

Another important category of applications using multiple encryption are those practical implementations of anonymous channel in open network, such as, the Mix-net [?] and onion routing [?]. In these settings, several agents are appointed to transmit data from the sender to the receiver without revealing identity of the sender. Typical design of such protocols is to encrypt data under multiple public keys of these agents, which decrypt the data one layer after another until eventually reach the destination. It is essential to perform these decryption correctly, e.g., [?] has shown some practical attacks against some carelessly designed Mix-net protocols [?,?], which if translated in our language, are insecure multiple encryption.

A related notion to multiple encryption is the threshold cryptosystem [?,?], which maintains secrecy of decryption key even if part of the secret key servers storing key shares are compromised. However, all known constructions are based on particular number theoretic assumption and can be employed to only a restrictive range of applications.

Security Notions. Standard definitions of public key encryption scheme are founded gradually in literature, e.g. [?,?,?,?,?]. *Semantic security*, first defined by Goldwasser and Micali [?], later refined by Goldreich [?,?] and Watanabe, Shikata and Imai [?], captures the computational approximation of Shannon's information-theoretic security [?], regulating that it should be infeasible for any PPT (Probabilistic Polynomial Time) adversary to obtain any partial information about the plaintext of a given ciphertext. Another rather technical definition, *indistinguishability*, defines that given a ciphertext an adversary cannot distinguish which plaintext is encrypted from two plaintexts. Indistinguishability is proven to be equivalent to semantic security in several attack models, namely chosen plaintext attack (CPA), (non-adaptive) chosen-ciphertext attack (CCA1) and adaptive chosen-ciphertext attack (CCA2) [?,?,?,?]. Another intricate notion, *non-malleability*, defined by Dolev, Dwork and Naor [?,?] formulates that the adversary should not be able to create a ciphertext of a different message that is meaningfully related to the original ciphertext and non-malleability implies indistinguishability in all above three attack models. Independently in [?] and [?], indistinguishability and non-malleability are proven to be equivalent under (adaptive) chosen-ciphertext attack (herefter CCA).

CCA-security is crucial in analyzing security of protocols. Mainly it allows the adversary can make arbitrary decryption queries on any ciphertext other than the target message. However, Shoup first argues CCA-security is too stringent for practical schemes and suggests "benign malleability" in the proposal for ISO public key encryption standard [?], as a relaxation for CCA model. An, Dodis and Rabin [?] give similar discussion under the name "generalized-CCA" (gCCA). In these two relaxed definitions, a relation function checks and rejects "obvious" decryption queries decrypted to the target message. Canetti, Krawczyk and Nielsen recently propose another relaxation, RCCA (Replayable CCA), which is strictly weaker than gCCA in most of cases [?].

Previous Work on Multiple Encryptions and Relations. Multiple encryption was addressed by Shannon as early as [?] under the name "product cipher", and in [?,?,?] in context of symmetric key cryptosystems. Massay and Maurer [?] have also studied the problem under the name "cascade cipher". However, all above work lacks considerations for CCA-security and is not adequate, for applying their underlying notions to public key setting straightforwardly, even only to the sequential case.

In ongoing work of [?], Dodis and Katz, independently of our work, propose another generic construction of CCA-secure multiple encryption. The security of their scheme can be proven in the standard model and can be generated to threshold settings. The difference lies in that first their scheme needs CCA-secure components while we only require component ciphers to be CPA secure. Besides, threshold setting seems not fit for our main goal "to enhance security of single component cipher". So far, they have presented their work in Rump Session in Crypto'03, Aug. 2003, while an earlier version [?] of our work was publicly announced in SCIS'03, Jan. 2003.

1.2 Our Contributions

Our contributions lie in following aspects:

Model and Security Definition of Multiple Encryption. We give the first formal model regarding public key multiple encryption. To the best of our knowledge, no previous work has strict formalization including CCA-security on this respect, and actually our model can be extended to both public key and symmetric key based cryptosystems. Our model consorts the modular design: combining "secure" component ciphers to have a "secure" multiple encryption. As a theoretical extension of traditional security definitions, we give the corresponding security definitions on multiple encryption based on indistinguishability and non-malleability against different attacks, especially chosen ciphertext attack (ME-CCA). Without loss of generality, breaking underlying assumptions of component ciphers can be esuriently modelled as the secret key is leaked to the adversary. Also some analyses here can be applied to symmetric key schemes.

Vulnerability of Natural Multiple Encryption. We demonstrate generic attacks against some "natural" constructions of multiple encryption schemes with each component IND-CCA-secure, by an adversary that breaks the indistinguishability of the scheme with only accesses to the Decryption Oracle and the Key Exposure Oracle. In fact, such adversary even breaks the onewayness. This suggests the necessity that multiple encryption should be treated as a separate primitive from single encryption.

Secure Construction of Multiple Encryption. We build multiple encryption schemes satisfying "strong" security, e.g. CCA from those satisfying only "weak" security, e.g., CPA. Though this task can be achieved using general zero-knowledge proof or one-time signature, considering efficiency of practical schemes, we design a scheme that is provably secure in the random oracle model.

Re-defining Security of Multiple Encryption. IND-CCA-security has been treated as standard definition for single encryption, which is shown modular design can be achieved for cryptographical protocols in the UC framework [?]. However, our analysis shows CCA-security may be too stringent since even IND-CCA-secure components would result in a CCA insecure multiple encryption for most of "natural" constructions. We argue the CCA-security definition is too strong for defining the multiple encryptions. As a reasonable relaxation, we give a new security definition named *weak chosen ciphertext attack for multiple encryption* (ME-wCCA) that is sufficient in most of interesting cases.

Security Notions of Multiple Encryption. We study the relations among different security definitions for multiple encryption. We believe a good analysis of these relations will help protocol designer more than simply give a specific construction based on concrete mathematical assumptions. Security definitions, namely indistinguishability and non-malleability, are formulated under different attack models. We show indistinguishability and non-malleability are still equivalent under ME-CCA, which corresponds to previous results: A multiple encryption degenerates to an ordinary public key cryptosystem, if there is only one component cipher in it. Similar relation holds for the relaxed definitions.

Application to Key Insulated Encryption. We reconsider the chosen ciphertext security of key-insulated encryption. It is only previously known in [?] that a generic construction exists provably secure against CPA attack. In this paper, we show that their scheme is in fact provably secure in the relaxed wCCA model, which reasonably supports the correctness and practical usability of their scheme. We further give a generic construction meeting exact CCA-security (in the random oracle model). We point out this is the first generic construction of CCA-secure key-insulated cryptosystem ever reported.

2 Multiple Encryption

Informally a multiple encryption is to encrypt a message by multiple cryptosystems. A multiple encryption scheme $\mathcal{ME}$ is generated by component ciphers.

Specification Multiple encryption is a cryptosystem composed by separate component ciphers, each of which may be independent. Suppose $\{\mathcal{E}_i\}_{1\leq i\leq n}$ is a set of *compatible* component ciphers, where for $\mathcal{E}_i$,

- $\mathsf{Enc\text{-}Gen}_i$ a probabilistic key-generation algorithm, with the input (1^k) and the internal coin flipping produces a public-secret key pair (pk_i, sk_i);
- Enc_i an encryption algorithm, with an input message $m_i \in \mathcal{M}_i$ and the public key pk_i, with the internal coin flipping, outputs a ciphertext $c_i \in \mathcal{C}_i$;
- Dec_i a decryption algorithm, which is a deterministic algorithm, with the input ciphertext c_i and the secret key sk_i, outputs a message m_i or "$\perp$".

A multiple encryption is a 3-tuple algorithm (MEnc-Gen,MEnc,MDec), where each algorithm may be combined from a number of public key cryptosystems with a unifilar connecting order. MEnc-Gen invokes every $\mathsf{Enc\text{-}Gen}_i$, and writes their outputs to a key list with public keys $PK = (pk_1, ..., pk_n)$ and secret keys $SK = (sk_1, ..., sk_n)$. MEnc with an input message M from message space $\mathcal{M}$ and PK, performs encryption MEnc on M by invoking a list of component encryption algorithms, eventually outputs a ciphertext $C \in \mathcal{C}$. The decryption algorithm MDec takes (C, SK) as input and outputs M, or "$\perp$" if C is invalid. We also denote in brief the encryption algorithm as $\mathsf{MEnc}(M; \mathtt{COIN})$ (or $\mathsf{MEnc}(M)$), and the decryption algorithm as $\mathsf{MDec}(C)$ in clear context, where COIN stands for the randomness used the multiple encryption. Essentially, we have two typical constructions: *parallel construction*, e.g., the generic construction given in [?], which the message is first split into shares by secret sharing then encrypted separately; *sequential construction*, e.g., the cascade cipher studied in [**?**], the message is encrypted by one component cipher then encrypted by another, and eventually forms the ciphertext. By combining these two constructions, we get a hybrid construction, which we refer to hereafter as "natural" construction.

3 Chosen Ciphertext Security for Multiple Encryption

Partially breaking of underlying assumptions (key exposure) is usually not considered in the security of a normal public key encryption scheme, such as IND-CCA, whereas a multiple encryption should remain secure even when most of the underlying assumptions are broken. Since this gap cannot merge sometimes, modifications should be performed to the (standard) CCA-security definition in order to catch this act. We here introduce an additional oracle into standard CCA game to emulate this scenario: a Key Exposure Oracle that upon the adaptive request of the adversary, reveals secret keys of the component ciphers to the adversary. Note that more has been considered in our model than mere key exposure and the situations are more complicated.

Oracle Access Rules. There are three oracles in our model: An Encryption Oracle $\mathcal{EO}$, which upon calling with input (M_0, M_1), returns C_b, the encryption of M_b, where $b \in \{0,1\}$ decided by internal coin flipping. A Decryption Oracle $\mathcal{DE}$, upon decryption query C, outputs $M = \mathsf{MDec}(C)$, if $C \neq C_b$; otherwise, "$\perp$". A Key Exposure Oracle, upon calling with i as one index of entire n component ciphers, $1 \leq i \leq n$, returns the corresponding secret key sk_i. The adversary can access three oracles in any order at any time of its choice, but it can only query $\mathcal{EO}$ once and $\mathcal{KE}$ at most $n-1$ times.

Definition 1 (IND-ME-CCA). *Assume any PPT adversary play the following game with a multiple encryption $\mathcal{ME}$. First key generation algorithm* MEnc-Gen *is run. The public key $PK = \{pk_i \,|\, i = 1, \ldots, n\}$ is then given to an Encryption Oracle $\mathcal{EO}$ and the adversary. The secret key $SK = \{sk_i | i = 1, \ldots, n\}$ is given to a Decryption Oracle $\mathcal{DO}$ and a Key Exposure Oracle $\mathcal{KE}$. The adversary chooses to access the three oracles in any order and at any time. According to the timing of access to $\mathcal{EO}$, the adversary's strategy is divided into two algorithms $(\mathcal{A}_{\mathsf{find}}, \mathcal{A}_{\mathsf{guess}})$, where $\mathcal{A}_{\mathsf{find}}$ tries to find (M_0, M_1) to submit to $\mathcal{EO}$ which returns C_b, and $\mathcal{A}_{\mathsf{guess}}$ tries to output a guess on b. If the difference of the success probability of the adversary $\mathcal{A}$ compared to random guess in the* IND-ME-CCA *game is negligible:*

$$\Pr\left[b = \tilde{b} \left| \begin{array}{c} (PK, SK) \leftarrow \mathsf{MEnc\text{-}Gen}(1^k), (M_0, M_1, \alpha) \leftarrow \mathcal{A}_{\mathsf{find}}^{\mathcal{KE},\mathcal{DO}}(PK), \\ b \stackrel{R}{\leftarrow} \{0,1\}, C_b \leftarrow \mathsf{MEnc}(M_b), \tilde{b} \leftarrow \mathcal{A}_{\mathsf{guess}}^{\mathcal{KE},\mathcal{DO}}(C_b, \alpha) \end{array} \right. \right] \leq \frac{1}{2} + \mathsf{neg}(k)$$

then we call this $\mathcal{ME}$ IND-ME-CCA*-secure.*

Non-malleability of multiple encryption against CCA (NM-ME-CCA) is similar to IND-ME-CCA except that the adversary succeeds by outputting a new ciphertext with is "meaningfully" related to the challenge ciphertext. That is, suppose R is a prescribed relation, then the adversary wins, if the adversary could output a different ciphertext C' from the challenge ciphertext C_b, with two plaintexts decrypted from C' and C_b satisfying R (R outputs TRUE).

Definition 2 ($\mathsf{NM\text{-}ME\text{-}CCA}$). *Denote $\mathbb{M}, \mathbb{C}$ as sets of plaintexts and ciphertexts being empty initially, respectively. According to the above access rules for the three oracles, if any PPT adversary in the following game has success probability negligibly close to 1/2, we call the multiple encryption scheme* $\mathsf{NM\text{-}ME\text{-}CCA}$*-secure.*

$$\Pr\left[b=1 \middle| \begin{array}{c}(PK,SK) \leftarrow \mathsf{MEnc\text{-}Gen}(1^k), (M_0, M_1, \alpha) \leftarrow \mathcal{A}_1^{\mathcal{KE},\mathcal{DO}}(PK), \\ C_b \leftarrow \mathsf{MEnc}(M_1), (R, \mathbb{C}) \leftarrow \mathcal{A}_2^{\mathcal{KE},\mathcal{DO}}(C_b, \alpha), \\ \mathbb{M} \leftarrow \mathsf{MDec}(\mathbb{C}), (C_b \notin \mathbb{C}) \wedge (\perp \notin \mathbb{M}) \wedge R(M_b, \mathbb{M})\end{array}\right] \leq \frac{1}{2} + \mathsf{neg}(k)$$

These definitions are also applicable to chosen plaintext attack CPA by letting $\mathcal{DO}$ always output an empty string on any decryption query, which results in the definition of *chosen plaintext attack for multiple encryption* $\mathsf{ME\text{-}CPA}$. Analogously, we can define $\mathsf{IND\text{-}ME\text{-}CPA}$, $\mathsf{NM\text{-}ME\text{-}CPA}$. By fixing the number of component ciphers $n = 1$ in the dedition of $\mathsf{IND\text{-}ME\text{-}CCA}$ (or $\mathsf{NM\text{-}ME\text{-}CCA}$), we obtain definition of the standard $\mathsf{IND\text{-}CCA}$ (or $\mathsf{NM\text{-}CCA}$).

4 Insecurity of Natural Constructions

Given each component $\mathsf{IND\text{-}CCA}$-secure, let's consider the following problem: Is the above "natural" construction $\mathsf{IND\text{-}ME\text{-}CCA}$-secure? Rather disappointing, the answer is negative. All "natural" constructions seem insecure without further treatments.

Basic Analysis. At the first glance, one may think all multiple encryption schemes from such construction should be secure, since each component is chosen independently from each other and satisfies strong security notion $\mathsf{IND\text{-}CCA}$, then all outputs will be indistinguishable from random sequence. However, this reasoning is fallacious. The flaw is in that this does not consider the case that the adversary can make use of $\mathcal{DO}$. In this case $\mathcal{DO}$ can be very helpful because every ciphertext different from the original can be decrypted and returned according to the definition of CCA attack. Then all the adversary needs to do is to modify the challenge ciphertext to a "new" one but decrypt to the same message, and submit it to the Decryption Oracle $\mathcal{DO}$. In the (standard) CCA setting, the adversary cannot do this easily because the secret key is kept privately. However, in $\mathsf{ME\text{-}CCA}$ setting, partial key can be exposed by the Key Exposure Oracle $\mathcal{KE}$, moreover, since every component is semantically secure, as it must be probabilistic, where there exist at least two valid ciphertexts $C_0, C_1 \in \mathcal{C}$ with $\mathsf{MDec}(C_0) = \mathsf{MDec}(C_1) = M$, where $M \in \mathcal{M}$ is any valid plaintext. Furthermore, we have the following theorem (The proof can be found in the full version of this paper [**?**].).

Theorem 1. There exists *insecure* multiple encryption in the sense of $\mathsf{IND\text{-}ME\text{-}CCA}$, even if it contains only independent $\mathsf{IND\text{-}CCA}$-secure component ciphers.

Discussion. The theorem shows only the case of indistinguishability under ME-CCA attack. We briefly explain the case of *onewayness* against chosen ciphertext attack for multiple encryption, denoted as OW-ME-CCA. Onewayness can be informally described as: given ciphertext C, output the plaintext M. It is a strictly weaker notion than indistinguishability. However, the proof of Theorem 1 tells us that not only IND-ME-CCA, but also onewayness may *not* be maintained in ME-CCA model, even if all the components are CCA-secure. On the other hand, we can see such natural schemes are malleable because the adversary can easily produce a "new" ciphertext with a proper key exposure query and simulates the Encryption Oracle. NM-ME-CCA-security better explains why the adversary can launch that attack: it actually has produced a ciphertext with relation that it contains the same plaintext to the challenge ciphertext. NM-ME-CCA-security is not trivially obtainable in such situations, either.

5 A Generic Construction for Secure Multiple Encryption

We have shown that the simple modular design without further treatment of multiple encryption is not sufficient to yield ME-CCA-security. Then two questions arise naturally: First, does a ME-CCA-secure multiple encryption exit? Second, whether a generic construction with ME-CCA-security can be combined from component ciphers with weaker security, e.g., *onewayness against chosen plaintext attack* (OW-CPA) security? We answer both questions by giving a generic construction combining component ciphers of weak security (OW-CPA) to ME-CCA-secure multiple encryption.

For the "natural" constructions, ME-CCA-security is hard to achieve with simple connections of component ciphers because partial exposure of the secret keys will always cause malleability of ciphertexts. This prompts us the necessity to check the randomness used in encryption to ensure the validity of all parts of a ciphertext before outputting the plaintext. Suppose all randomness used in the encryption can be verified during decryption, then the Decryption Oracle in fact does not help the adversary: If the adversary can pass the randomness verification, with overwhelming probability, it has already known all the randomness used. This can further be achieved by embedding all randomness into the plaintext, then consistence of all randomness can be verified in the decryption phase, i.e., the adversary must be forced to have known the corresponding plaintext when it submits a valid ciphertext query. Then a multiple encryption will be secure if an adversary cannot break all underlying component ciphers.

5.1 Secure Construction of Multiple Encryption

ME-CCA constructions based on any public key encryption components with OW-CPA security that is satisfied by most practical public key encryption schemes. Recall $\mathcal{E}_i$ is the i-th component cipher of the multiple encryption, $\mathsf{Enc}_i(m_i, pk_i; \mathtt{COIN}_i)$ and $\mathsf{Dec}_i(c_i, sk_i)$ are the encryption algorithm and decryption algorithm for $\mathcal{E}_i$ (in short $\mathsf{Enc}_i(m_i; \mathtt{COIN}_i)$ and $\mathsf{Dec}_i(c_i)$, respectively), where pk_i is the public key and sk_i is the secret key of $\mathcal{E}_i$ (see section 2). We further design the following construction. Denote $H_i : \{0,1\}^* \to \{0,1\}^{k_i}$ (k_i is the length of necessary random coin for $\mathcal{E}_i$) and $G_i : \{0,1\}^* \rightarrow \{0,1\}^{l_i}$ (l_i is the length of c_{i2}) as random functions. For parallel multiple, one can consider the following construction:

Key-Generation $\mathsf{MGen\text{-}Enc}(1^k)$**:** $(pk_i, sk_i) \leftarrow \mathsf{Gen\text{-}Enc}_i$, for $1 \leq i \leq n$; $PK = (pk_1, ..., pk_n)$, $SK = (sk_1, ..., sk_n)$.

Encryption $\mathsf{MEnc}(M, PK)$**:** $(m_1, ..., m_n) \overset{\mathsf{AONT}}{\longleftarrow} \mathcal{T}(M)$. $r_i \in_R \{0,1\}^*$, for $1 \leq i \leq n$. For i-th component cipher: $c_{i1} \leftarrow \mathsf{Enc}_i(r_i; H_i(M, r_1, ..., r_n))$, $c_{i2} \leftarrow G_i(r_i) \oplus m_i$, $c_i = (c_{i1}, c_{i2})$, $1 \leq i \leq n$. Outputs $C = (c_1, ..., c_n)$ as ciphertext.

Decryption $\mathsf{MDec}(C, SK)$**:** $r_i \leftarrow \mathsf{Dec}_i(\bar{c}_{i1})$, $\bar{m}_i = G(\bar{r}_i) \oplus \bar{c}_{i2}$, $1 \leq i \leq n$. Outputs $\bar{M} \leftarrow \mathcal{I}(\bar{m}_1, ..., \bar{m}_n)$ as plaintext if $\bar{c}_{i1} = \mathsf{Enc}_i(\bar{r}_i; H_i(\bar{M}, \bar{r}_1, ..., \bar{r}_n))$, otherwise "$\perp$".

We prove the following theorem holds for above construction, whose proof can be found in the full version of this paper [**?**]. Based on the same idea, one can design a secure construction for sequential multiple encryption, of which an example can be found in [**?**].

Theorem 2. *Multiple encryptions from above constructions are secure* IND-ME-CCA*-secure in the random oracle model.*

Discussion. One complementary remark should be addressed on the *uniformity* of underlying primitives. What we have considered so far is mainly non-deterministic component ciphers. For deterministic primitive public key encryption, e.g., RSA, above construction is not sufficient, however, it can be modified to fit this transform. Furthermore, if all the component ciphers are deterministic, the task is easier: just connect them together and set proper padding schemes as pre-procession of the message, like OAEP+ [**?**], and form the whole multiple encryption with parallel construction with compatible input domain, or sequential connecting one after another. AONT can be even replaced by OAEP+. This construction should also be secure because if the encryption primitive is deterministic, an adversary cannot re-encrypt the corresponding parts of a ciphertext into valid new part to produce another ciphertext even if it seizes corresponding secret keys. We shall give formal analysis regarding the deterministic encryption primitive in the forthcoming work.

6 New Security Definitions for Multiple Encryption

It seems contradictive to our intuition that though component ciphers are independent, even onewayness may lose with just simple connection of independently chosen ciphers. However, if we follow the CCA-security, it is doomed to appear completely insecure. From another aspect, it suggests that CCA-security may be somehow excessively strong. In the real world, it is unreasonable that $\mathcal{DO}$ helps such obvious attacks. A well-known example states that a new cipher S' constructed from a CCA-secure cipher S, where a harmless bit is appended to the ciphertext of S and is discarded during decryption, is no longer secure in the sense of CCA. In fact such attack to S' should be easily judged and have "no significant difference" in most of interesting cases. When $\mathcal{DO}$ encounters such queries, it should easily determine whether this is really a "new" ciphertext, by just looking at the ciphertext.

6.1 Relaxing Security Definition Regarding Multiple Encryption

CCA-security might be too strong and is not always necessary, as pointed out in [?,?,?], among which, Shoup's "benign malleability" [?] and An, Dodis and Rabin's "gCCA" [?] are basically equivalent: a relation function $\mathcal{RF}$ helps the Decryption Oracle against obvious attacks. In gCCA definition, the relation function performs as follows: if $\mathcal{RF}(c, c') = \mathsf{TRUE} \Rightarrow \mathsf{Dec}(c) = \mathsf{Dec}(c')$. The opposite direction does not hold, otherwise, the relation function can be used as an oracle breaking the indistinguishability. There must be $\exists\ (c, c')$, such that $\mathcal{RF}(c, c') = \mathsf{FALSE}$, with $\mathsf{Dec}(c) = \mathsf{Dec}(c')$ (refer [?] for more details). Canetti, Krawczyk and Nielsen [?] recently propose another relaxation, called "replayable chosen ciphertext attack" (RCCA), with most of cases strictly weaker than gCCA.

To rule out the definitional limitation of CCA-security in multiple encryption setting, we also introduce a relaxed definition called "*weak chosen ciphertext attack for multiple encryption*" (ME-wCCA). In the definition of wCCA, there is a relation function $\mathcal{RF}^*$ is computed by invoking $\mathcal{RF}_i$ ($1 \leq i \leq n$) during the decryption process inside $\mathcal{DO}$, with initial value of each $\mathcal{RF}_i$ set to FALSE, where $\mathcal{RF}_i$ is the relation function defined according to gCCA-security for i-th component cipher $\mathcal{E}_i$. $\mathcal{RF}_i(c_i, c_i') = \mathsf{TRUE} \Rightarrow \mathsf{Dec}(c_i) = \mathsf{Dec}(c_i')$. Whenever $\mathcal{RF}_i = \mathsf{TRUE}$ for some i, $\mathcal{RF}^*$ halts and returns TRUE to $\mathcal{DO}$ immediately. Once receiving TRUE, $\mathcal{DO}$ outputs "$\perp$" to the adversary. Informally, if $\mathcal{RF}^*$ finds a part (may be the intermediate decryption result) of the query ciphertext looks "the same" as the corresponding part of the challenge ciphertext, it tells the Decryption Oracle to reject this decryption query. Since the rules for oracle access is the same, the definition of IND-ME-CCA only needs to be modified a little to adapt to IND-ME-wCCA.

We stress that ME-wCCA-security is a reasonable relaxation for CCA-security. This notion is basically an extension of gCCA-security. By restricting a multiple encryption to only one component cipher, IND-ME-wCCA becomes IND-gCCA.

Definition 3 (IND-ME-wCCA). *In this game, every thing is the same except the operation of the Decryption Oracle $\mathcal{DO}$. The Decryption Oracle $\mathcal{DO}$ is equipped with a Relation Function $\mathcal{RF}^*$ inside, which is computable in polynomial time. The scheme is secure if any probabilistic polynomial time adversary has success negligibly close to 1/2.*

$$\Pr\left[b = \tilde{b} \middle| \begin{array}{c} (PK, SK) \leftarrow \mathsf{MEnc\text{-}Gen}(1^k), (M_0, M_1, \alpha) \leftarrow \mathcal{A}_{\mathsf{find}}^{\mathcal{KE}, \mathcal{DO}^{\neg\mathcal{RF}^*}}(PK), \\ b \xleftarrow{R} \{0,1\}, C_b \leftarrow \mathsf{Enc}(M_b), \tilde{b} \leftarrow \mathcal{A}_{\mathsf{guess}}^{\mathcal{KE}, \mathcal{DO}\neg\mathcal{RF}^*}(C_b, \alpha) \end{array} \right] \leq \frac{1}{2} + \mathsf{neg}(k)$$

The following lemma shows that IND-ME-wCCA-secure multiple encryption can be acquired from IND-gCCA-secure component ciphers (for proof see [?]).

Lemma 1. *A multiple encryption scheme $\mathcal{ME}$ is* IND-ME-wCCA*-secure w.r.t. $\mathcal{RF}^*$ by any of three basic constructions, if each component cipher $\mathcal{E}_i$ is* IND-gCCA*-secure w.r.t relation function $\mathcal{RF}_i$, $1 \leq i \leq n$. $\mathcal{RF}^*$ is defined as $\mathcal{RF}^*(C, C') = \mathsf{TRUE}$, such that $\mathcal{RF}_i(c_i, c_i') = \mathsf{TRUE}$ for some i, $1 \leq i \leq n$, where c_i, c_i' are two ciphertexts of $\mathcal{E}_i$, and C, C' are the corresponding ciphertexts for $\mathcal{ME}$.*

Since IND-CCA always implies IND-gCCA, we have the following theorem:

Theorem 3. *If all component ciphers are* IND-CCA*-secure and chosen independently according to above "natural" constructions, then the resulting multiple encryption is* IND-ME-wCCA*-secure.*

In fact, each attack per theorem 1 can construct a new ciphertext with the same plaintext. Since non-malleability is an arduous goal for multiple encryption, we define relaxed gNM-ME-CCA similar to IND-ME-wCCA. Informally, the definition limits that the adversary does not win as long as it outputs with a new ciphertext with the equivalence relation regulated by the relation function to the challenge ciphertext, where the relation function is defined analogously to that of IND-ME-wCCA.

Definition 4 (gNM-ME-CCA). *A multiple encryption scheme is generalized-non-malleable against* ME-CCA *attack if for any PPT adversary, which is assisted by Decryption Oracle $\mathcal{DO}$, and a Key Exposure Oracle $\mathcal{KE}$, it cannot produce a new ciphertext with relation other than what the Relation Function $\mathcal{RF}^*$ specifies with non-negligible probability, where $\mathcal{RF}^*$ is defined identical to* ME-wCCA*. Denote $\mathbb{M}, \mathbb{C}$ as sets of plaintexts and ciphertexts being empty initially, respectively.*

$$\Pr\left[b=1 \middle| \begin{array}{c} (PK, SK) \leftarrow \mathsf{MEnc\text{-}Gen}(1^k), (M_0, M_1, \alpha) \leftarrow \mathcal{A}_1^{\mathcal{KE},\mathcal{DO}}(PK), \\ C_b \leftarrow \mathsf{MEnc}(M_1), (R, \mathbb{C}) \leftarrow \mathcal{A}_2^{\mathcal{KE},\mathcal{DO}}(C_b, \alpha, M_0, M_1), \\ \mathbb{M} \leftarrow \mathsf{MDec}(\mathbb{C}), (C_b \notin \mathbb{C}) \wedge (\perp \notin \mathbb{M}) \wedge R(M_b, \mathbb{M}) \wedge (R \neq \mathcal{RF}^*) \end{array}\right] \leq \frac{1}{2} + \mathsf{neg}(k)$$

gNM-ME-CCA is a strictly weaker notion than NM-ME-CCA-security (cf. IND-ME-wCCA to IND-ME-CCA).

7 Relations among Security Definitions

In this section, we discuss the relations among security definitions of multiple encryptions. The good news is that in multiple encryption scenario indistinguishability and non-malleability are still equivalent under ME-CCA attacks (IND-ME-wCCA is equivalent to gNM-ME-CCA). The proofs of these theorems are left to the full version of this paper [?].

Theorem 4. IND-ME-CCA $\Leftrightarrow$ NM-ME-CCA

Theorem 5. IND-ME-wCCA $\Leftrightarrow$ gNM-ME-CCA

Theorem 6. IND-ME-wCCA $\Rightarrow$ IND-ME-CPA*,* IND-ME-CPA $\not\Rightarrow$ IND-ME-wCCA*.*

8 Applications to Key-Insulated Cryptosystem

The key-insulated cryptosystem is proposed by [?] to protect cryptosystems against partial key exposure. In such system, encryption is done in an insecure user device. Additionally, there is a physically secure server that stores a master key. With the help of this server, user keys are updated periodically so that compromise of user keys in some periods does not affect the system in other periods. In [?], a generic construction is proposed based on arbitrary semantically secure public key encryption against *chosen plaintext attack*. Recall that the authors of [?] do not claim their generic construction CCA-secure.

At the first look, because of the property of cover-free family even if the secret keys are compromised in t periods, at most $t-1$ secret keys of a period other than these t are known to the adversary. Since the message is split into shares by AONT, we know it is computationally infeasible to break the indistinguishability even after viewing part of the sub-messages generated by AONT. However, an adversary actually can bypass the hard task and just needs to try to modify the challenge ciphertext using known secret keys in order to get help from the Decryption Oracle $\mathcal{DO}$. In fact, it can obtain any secret key sk_j by sending adaptive query to the Key Exposure Oracle $\mathcal{KE}$ for sk_j in some period i with $j \in S_i$. Then it can decrypt $c_j = \mathsf{Enc}_j(m_j)$, and re-encrypt it. It can always succeed to produce $c'_j = \mathsf{Enc}_j(m_j)$ with $c'_j \neq c_j$, since according to the system settings, all component ciphers are semantically secure. Now the adversary can replace c_j with c'_j and submit this "new" ciphertext C' to $\mathcal{DO}$, which will return the corresponding message M. This attack works for any period i.

The original generic construction of [?] does not satisfy chosen ciphertext attack security, actually if every component cipher is chosen IND-CCA-secure, this generic construction is actually IND-ME-wCCA-secure (Theorem 3). We note that this scheme still provides very practical security.

8.1 CCA-Secure Key-Insulated Cryptosystem

The feasibility of constructing a CCA-secure key-insulated cryptosystem (parallel multiple encryption) has already been shown in section 5.1. We are only fascinated at whether given IND-CCA-secure ciphers as building blocks, a parallel construction can be transformed to a CCA-secure key-insulated cryptosystem with minimum modification. Recall $\mathtt{coin}_i$ is the auxiliary randomness input for encryption component $\mathcal{E}_i$. Let $\mathtt{coin}_i = h(\mathtt{r}||Index_i)$, where $\mathtt{r}$ is a random number, $Index_i$ is the description of i-th component and h is a random function. The Encryption is $C = \mathsf{MEnc}(M||r; (\mathtt{coin}_1, ..., \mathtt{coin}_n))$, especially for IND-CCA component $\mathcal{E}_i$, $\mathsf{Enc}_i(m_i; \mathtt{coin}_i)$ where m_i is generated from AONT with input $M||r$. Decryption process becomes: for a ciphertext C', $M'||\mathtt{r}' = \mathsf{MDec}(C')$, output M' only if $c'_i = \mathsf{Enc}_i(m_i; h(\mathtt{r}'||Index_i))$ is well formed, for every $1 \leq i \leq n$. Whenever it is detected that a ciphertext has used invalid randomness, the Decryption Oracle rejects this query immediately.

It is easy to see this scheme satisfies the security definition of [?] under CCA attack. The proof is easy and will be omitted here. We point out this is actually the *first* generic construction of key-insulated cryptosystem enjoying CCA-security (Another generic construction for CCA-secure key-insulated cryptosystem will be given by Dodis and Katz in their upcoming work, whose security can be proven in the standard model.). In fact, this transform turns IND-ME-CPA secure multiple encryptions into IND-ME-CCA-secure ones.

Acknowledgement

The authors would thank Masayuki Abe, Yevgeniy Dodis, Yumiko Hanaoka, Jonathan Katz, Kazukuni Kobara and Moti Yung for fruitful discussions. The authors would also like to thank anonymous referees for invaluable comments.