Research Seminar in Cryptography

Report on 'KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption'

Mart Simisker
Supervised by: D. Unruh

December 20, 2018

Abstract

The aim of this report is to give an overview of the work done by J. Herranz, D. Hoefheinz and E. Kiltz. The paper looks at the KEM/DEM hybrid encryption paradigm. A composition theorem states that if both KEM and DEM have the highest level of security, then so does the hybrid PKE scheme. This paper studies the necessary and sufficient conditions on the security of the KEM and DEM to guarantee a hybrid PKE scheme with a certain level of security. In more detail, they study combinations of nine different security notions for KEMs, ten for DEMs and six for PKE schemes, to completely characterize which combinations lead to a secure hybrid PKE scheme (by providing a composition theorem) and which do not (by providing counter examples).

1 Introduction

This report will give an overview of the article 'KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption' by J. Herranz, D. Hoefheinz and E. Kiltz [1]. The report first begins with an introduction to the topic, covering also the introduction section of the article. It tries to provide some general definitions or explanations. Then the high level results are examined. After that, the definitions and theorems are examined.

1.1 General introduction to the topic

In modern networks, large number of parties wish to communicate without restrictions but at the same time they wish to preserve the privacy of the messages. A well known solution is to use public key encryption (PKE) schemes, which give the possibility for a user to communicate with multiple parties using one key pair for all the channels while the contents are kept secret from third parties. The main restriction of basic PKE schemes in contrast to symmetric encryption schemes is the restricted message space. A way to solve this is to use hybrid encryption schemes.

- Data encapsulation mechanism (DEM) - a highly efficient symmetric encryption scheme used to encapsulate large messages.
- Key encapsulation mechanism (KEM) - used for encapsulating short messages used as keys. The scheme uses asymmetric public key encryption.
- Hybrid encryption scheme - a combination of KEM and DEM, where the KEM is used to provide one with a random symmetric key, which is then used with the DEM to encrypt the actual message.

The hybrid encryption approach is often referred to as "KEM/DEM paradigm" and was first formalized by Cramer and Shoup [2, 3]. This paradigm can be used to construct efficient and practical public key encryption (PKE) schemes.

1.2 Introduction to attacks

The following will give a short overview of the attack part in security notions referred to in the paper. The attacks can differ slightly on the scheme they are used in (for an example KEM vs DEM).

Names of commonly used attacks are:

- CPA – chosen-plaintext attack

  Adversary gets to pick messages which the challenger encrypts.

  In the DEM setting it involves using an encryption oracle.

  In the public key setting, this is the weakest case, because the adversary can just create ciphertexts using the public-key.

- CCA1 – (non-adaptive) chosen-ciphertext attack

  Adversary gets access to a decryption oracle before receiving challenge ciphertext.

  In other words, the adversary gets access to some previous ciphertexts and the messages they decrypt to.

- CCA2 – adaptive chosen-ciphertext attack (with multiple queries)

  In addition to CCA1, adversary gets access to a decryption oracle after receiving challenge ciphertext. (CCA2 is stronger than CCA1).

- OT – one-time, correspond to passive attacks from [3].

  In such an attack, adversary picks two messages, the encryption oracle generates a random key and encrypts one of the messages (based on random choice). Adversary has to output which message was encrypted.

- OTCCA – one-time adaptive chosen-ciphertext attack (Comparable to CCA2)

Compares to adaptive chosen-ciphertext attacks from [3, Sec 7.2.1]. Such attacks, in addition to OT, allow the adversary to query a decryption oracle after receiving the challenge ciphertexts (with the exception of querying the challenge ciphertext).

All five are considered for data encapsulation mechanism, however only the first 3 are considered for key encapsulation mechanism and the combined hybrid scheme.

A good introduction to notions of symmetric encryption is given in the introduction of [4, p.3-4]. It gives a brief look at history and brings out important differences, which must be considered when modelling an attack on symmetric encryption schemes compared to asymmetric ones.

1.3 Main questions

When we consider all the possible combinations of KEMs and DEMs, an important question is how does the security of the individual KEM and DEM parts relate to the security of the resulting hybrid PKE scheme? This knowledge becomes useful when constructing hybrid PKE schemes. Due to the large number of different security notions for the components of the scheme, this question becomes quite broad. The strongest security notion is denoted as *indistinguishability under chosen-ciphertext attacks*(IND-CCA2) [5]. Cramer and Shoup have proved in [3] that chosen-ciphertext security for the KEM and the DEM part is a sufficient condition to obtain a chosen-ciphertext secure hybrid PKE scheme. The two questions following this are, whether one could still get chosen-ciphertext secure hybrid PKE scheme after relaxing the notion of KEM or DEM part. And more generally, what are the necessary and sufficient conditions for the KEM and the DEM part to obtain a hybrid PKE scheme, which is secure with respect to possibly weaker notions.

2 First look at the results

The authors of the paper characterize the necessary and sufficient conditions, which the KEM and the DEM must satisfy in order to lead to a secure hybrid PKE scheme. The characterization is said to be complete with respect to the considered security notions for KEMs, DEMs and PKE schemes and the hierarchies implied by these notions. They also show the guaranteed security level of the hybrid PKE scheme for fixed security levels of the KEM and the DEM.

Considered security notions for KEMs, DEMs and PKE schemes Next, they describe, which security notions will be included in the comparison. They give a new notion of non-malleability for KEMs, which they call *weak non-malleability* (wNM). In combination with three standard attack forms, this leads to respective notions of wNM-CPA, wNM-CCA1, wNM-CCA2. They also

DEM KEM	IND-{OT, CPA, CCA1}	NM-{OT, CPA, CCA1}	IND-{OTCCA, CCA2}
{IND-CPA, wNM-CPA}	$\geq$ IND-CPA (5.1) $<$ IND-CCA1, NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1, NM-CPA	$\geq$ IND-CPA $<$ IND-CCA1, NM-CPA
sNM-CPA	$\geq$ IND-CPA $<$ IND-CCA1, NM-CPA	$\geq$ NM-CPA (5.3) $<$ IND-CCA1	$\geq$ NM-CPA $<$ IND-CCA1 (5.7)
{IND-CCA1, wNM-CCA1, wNM-CPA2}	$\geq$ IND-CCA1 (5.1) $<$ NM-CPA	$\geq$ IND-CCA1 $<$ NM-CPA	$\geq$ IND-CCA1 $<$ NM-CPA (5.4)
sNM-CCA1	$\geq$ IND-CCA1 $<$ NM-CPA	$\geq$ NM-CCA1 (5.2) $<$ IND-CCA2	$\geq$ NM-CCA1 $<$ IND-CCA2 (5.8)
IND-CCA2	$\geq$ IND-CCA1 $<$ NM-CPA (5.5)	$\geq$ NM-CCA1 $<$ IND-CCA2 (5.6)	$\geq$ IND-CCA2 [3]

Figure 1: Sufficient and necessary conditions for hybrid encryption. Results given in set-notation: all positive results hold with respect to the weakest possible combination of KEM/DEM in the set, whereas negative results hold with respect to the strongest combination[1] The $\geq$ is used for positive and $<$ for negative result.

denote by *strong non-malleability* (sNM) a stronger notion of non-malleability independently proposed by Nagao, Manabe and Okamoto [6]. In total, they consider nine notions for KEMs, {wNM, sNM, IND}-{CPA, CCA1, CCA2}. The difference between wNM and sNM is compared later.

They consider ten notions for DEMs - {NM, IND}-{OT, OTCCA, CPA, CCA1, CCA2}. Out of these, the OT (one-time) and OTCCA (the one-time chosen-ciphertext attack) security notions originate from [3]. Motivated by the hybrid PKE approach, in the OT and OTCCA security games, the adversary is not given access to an encryption oracle.

They provide a complete characterization of the relations between the notions, revisiting and extending existing results by Katz and Yung [7]. This is done by considering a stronger notion of non-malleability and by adding the attack form of OTCCA.

For PKE schemes, they considered six standard notions of {NM, IND}-{CPA, CCA1, CCA2}, classified in [8].

2.1 Sufficient and necessary conditions for hybrid encryption

In Figure 1, they gave a characterization of the necessary and sufficient conditions required from the KEM and the DEM in order to achieve secure hybrid PKE schemes. They use a notation, in which the symbol $\geq$ denotes the positive implication, meaning that any combination of KEM and DEM with the stated levels of security leads to a hybrid PKE scheme with the level of security stated

after the symbol. The $<$ symbol denotes negative results, meaning that there exists some combination of KEM and DEM with the stated security notions, but the resulting hybrid PKE does not satisfy the security notion after the symbol.

Eight results in the table contain a theorem number from the paper [1] in brackets. The rest of the results are deduced from these eight results by using security hierarchies of KEMs, DEMs and PKE schemes. In the figure, positive results propagate to the right and down, negative results to the top and left.

The authors were surprised that it was possible to group notions, which achieve exactly the same security level for the resulting hybrid scheme, even though the primitives can be separated. As an example, with an IND-OT secure DEM one can reach the same level of security as with an IND-CCA1 DEM.

Additionally, they point out that the proof of [3] does not always carry over to show that an X-Y secure KEM in combination with an X-Y secure DEM also yields an X-Y secure hybrid scheme. This only holds for X $\in$ {IND, sNM} (Theorems 5.1, 5.2 and 5.3 of the main paper) but is wrong for X = wNM (Theorems 5.6 and 5.4 of the main paper). The table also shows the necessity of the sufficient conditions on the KEM and the DEM in the composition theorem from [3] - an IND-CCA2 secure hybrid scheme can only be guaranteed when both, the KEM and DEM have the highest security level. Theorems 5.4, 5.8 and 5.6 prove that by weakening the KEM to wNM-CCA2/sNM-CCA1 or the DEM to NM-CCA1, the hybrid PKE scheme is no longer guaranteed to be IND-CCA2. Moreover, a combination of the strongest possible KEM with a weak DEM or vice versa, only provides a relatively weak hybrid PKE scheme (from theorems 5.5 and 5.7).

On the positive side, IND-CCA1 KEM and an IND-OT DEM already yield an IND-CCA1 hybrid scheme (Theorem 5.1). A sNM-CCA1 KEM and a NM-OT DEM implies a NM-CCA1 hybrid scheme (Theorem 5.2).

The techniques used when proving the theorems contain new as well as well-established ones.

2.2 Security notions for Key Encapsulation Mechanisms and their relation

The paper revisits attempts to define non-malleability of KEMs [9, 10] (which they denote NM'), and argues that there are certain problems with the treatment of the key space. Furthermore, they prove that one of the main theorems of [9, 10] about the equivalence between the notions of IND-CCA2 and NM'-CCA2 is wrong. They do this by showing that the Cramer-Shoup KEM [3] serves an example of a KEM, which is IND-CCA2 but not NM'-CPA. They also reviewed

[11, 8]. Based on these reviews, they defined non-malleability for KEMs, which they call wNM.

A stronger definition of non-malleability, denoted here as sNM, was proposed in [6] (correcting [9, 10]). The difference from previous is that in the non-malleability experiment of sNM, the adversary is given additional information containing the challenge key in clear.

In the paper, a complete characterization of the KEM hierarchy is given, implications and separations between the different security notions {IND, wNM, sNM}-{CPA, CCA1, CCA2} are provided. The resulting hierarchy was depicted in [1, Figure 2]. For an example, IND-CCA2 implies sNM-CCA2 as well as the other way around (as proved in [6]). IND-CCA2 also implies IND-CCA1, which does not necessarily imply wNM-CPA (According to theorem 3.3). However, sNM-CCA2 implies sNM-CCA1, which implies sNM-CPA, which implies wNM-CPA. The authors have pointed out, that although sNM always implies wNM, wNM-CCA2 does not even imply sNM-CPA. Another result is that wNM-ATK strictly implies IND-ATK for ATK $\in$ {CPA, CCA1}.

About the preference of wNM and sNM The authors think that wNM follows closer to the original [11, 8]. The sNM from [6] is said to seem more useful in practice. One argument is, that the NM of KEM and NM of DEM implies NM of hybrid PKE scheme only in case of sNM but not with wNM.

2.3 Security notions for Data Encapsulation Mechanisms and their relation

In this article, they consider eight of the 18 different security notions defined by Katz and Yung [7], the ({IND, NM})-{OT, CPA, CCA1, CCA2}, and additionally ({IND, NM})-OTCCA, where IND-OTCCA was originally introduced in [3]. The notion of non-malleability used here is considered to be stronger than the one used in [7] and therefore the hierarchy obtained looks different. This stronger notion had already been mentioned but not used in [7].

The full characterization of the DEM hierarchy, providing implications and separations between different security notions, is presented in [1, Figure 3].

2.4 Further results

In the article, they have considered a stronger definition of non-malleability for PKE schemes, in which the vector of ciphertexts may also contain invalid ciphertext. This is compared to the definition from [8], and has been used in an update [12] of [13].

3 Security Definitions

In this section, the paper gives the formal security definitions for PKE, KEM and DEM schemes.

3.1 Public Key Encryption

They define *public key encryption* scheme $\mathcal{PKE}$ consisting of three polynomial-time algorithms, PKE.Kg (the key generation algorithm), PKE.Enc (the encryption algorithm) and PKE.Dec (the decryption algorithm). The key generation algorithm is a randomized key generation algorithm dependent on a security parameter $k \in \mathbb{N}$ and produces a random key pair (pk, sk). The encryption algorithm takes the public key pk and a message m, and outputs a uniformly random ciphertext C. The decryption algorithm takes the private key sk and ciphertext C, and outputs either the message m or a rejection symbol.

For consistency, they require that the decryption of an encryption using the same keypair always returns the original message for all values of the security parameter and for all messages.

PKE Indistinguishability They give the definition of the adversaries advantage in a security experiment, for $\mathcal{PKE}$ scheme, with security parameter k against a given $atk \in$\{CPA, CCA1, CCA2\}. The $\mathcal{PKE}$ scheme is said to be *indistinguishable* against ATK attacks (IND-ATK) if the advantage function from the definition is a negligible function in the security parameter k for all polynomial time adversaries.

PKE Non-Malleability They define relations of arity t (polynomial in the security parameter k) between an element of a field and a vector of $t-1$ elements of the field (the elements are either ciphertexts or messages). The goal of the adversary in the non-malleability experiment is, given a ciphertext C, to come up with a vector of ciphertexts, where the vector of their decryptions is meaningfully related to the key K - that is there is some relation, which maps the ciphertext to the vector of ciphertexts.

They use a definition from [8], which describes the adversaries advantage in the Non-malleability experiment for attacks in {CPA, CCA1, CCA2}, with some differences, namely allowing the adversary to provide invalid ciphertext or none at all, making the definition stronger. The use of the relation is explained in more detail. Similarly to the previous, the $\mathcal{PKE}$ scheme is said to be *non-malleable against* ATK *attacks* (NM-ATK) if the advantage function from the definition is a negligible function in the security parameter k for all polynomial time adversaries. They also stress, that the results of [8] are still valid with respect to the modified definition.

3.2 Public Key Encapsulation Mechanisms

A *public-key encapsulation mechanism* $\mathcal{KEM}$ consists of three polynomial time algorithms (KEM.Kg, KEM.Enc, KEM.Dec), and is associated with key-space *KeySp* (affected by a security parameter k, which decides the key length). The KEM.Kg generates randomized keypairs for security parameter k. The KEM.Enc function is the encryption algorithm, which produces a key K (assuming the role of a message) and a ciphertext of K, for public key pk (encrypts K using pk) and the security parameter k, such that K belongs to the key-space *KeySp*. The KEM.Dec takes a secret key sk and a ciphertext C, and returns either a key in the key-space or rejection symbol. In this case, they require that for all $k \in \mathbb{N}$ and all key, ciphertext pairs produced by the KEM.Enc for a given public key, given the related secret key, the KEM.Dec will always produce the correct key.

The key difference between PKE and KEM is the definition of message space, which for PKE may contain all possible messages but for KEM has to be the *KeySp*, a subset of all possible messages.

KEM Indistinguishability The notion of indistinguishability of KEMs against CCA2 attacks was established in [3]. Similarly to the PKE indistinguishability, they define the advantage of adversary in ATK $\in$\{CPA, CCA1, CCA2\} and say that a key encapsulation mechanism $\mathcal{KEM}$ is said to be *indistinguishable against* ATK *attacks* (IND-ATK) if the advantage function is a negligible function in k for all polynomial-time adversaries.

KEM Non-Malleability The crucial need for care when defining non-malleability of KEMs can be seen from the problem in the existing definition from [9, 10]. In this case, they restricted the adversary from defining the key space and instead say that the key sampling algorithm returns a key uniformly distributed over $\{0,1\}^k$. They then define the adversary's advantage in the non malleability experiment and state, that a key encapsulation mechanism $\mathcal{KEM}$ is said to be *weakly non-malleable against* ATK *attacks* (wNM-ATK) if the advantage function is a negligible function in k for all polynomial-time adversaries.

Stronger Non-Malleability The stronger notion, denoted as sNM, proposed by Nagao, Manabe and Okamoto [6], is different from wNM as they give to the adversary additional information. This consists of two keys in a random order, where one is a random key, and the other is the output of the KEM.Enc. The resulting notion is called *strong non-malleability against* ATK *attacks* (sNM-ATK), for ATK $\in$ \{CPA, CCA1, CCA2\}.

3.3 Data Encapsulation Mechanisms

A (stateless) *data encapsulation mechanism* $\mathcal{DEM}$ consists of three polynomial-time algorithms (DEM.Kg, DEM.Enc and DEM.Dec). The key generation

(DEM.Kg) produces a random key K with length k, the security parameter. The encryption method (DEM.Enc) takes a key K and a message, and encrypts the message. The decryption function (DEM.Dec) takes a key K and a ciphertext, and returns a decrypted message or a rejection. It is assumed, that for a key K, generated using DEM.Kg (for any value of the security parameter), the decryption method applied to the output of the encryption method, will always return the original message.

DEM Indistinguishability The definitions of indistinguishability against CPA, CCA1 and CCA2 attacks for DEMs are given in [4]. They draw attention to the fact, that in the security definition of CPA for DEMs an adversary is also given access to an encryption oracle.

Additionally, one-time attacks (OT) and one-time (adaptive) chosen-ciphertext attacks (OTCCA) are considered. The OT attacks are said to correspond to *passive attacks* and OTCCA to *adaptive chosen-ciphertext attacks* in [3, Sec 7.2.1]. It is further explained, that OT attacks are CPA attacks where the adversary is not given an encryption oracle (there is only one call to the encryption oracle). OTCCA attacks are OT attacks where in the second stage the adversary is given access to a decryption oracle.

They then define the adversary advantage function for ATK$\in$\{OT, OTCCA, CPA, CCA1, CCA2\} and state that a data encapsulation mechanism $\mathcal{DEM}$ is said to be *indistinguishable against* ATK *attacks* (IND-ATK) if the advantage function is a negligible function in k for all polynomial-time adversaries.

DEM Non-Malleability They define an adversary advantage function for attack ATK$\in$ \{OT, OTCCA, CPA, CCA1, CCA2\} similarly to the KEM definition, that is they allow invalid ciphertexts or an empty vector of ciphertexts, which leads to a stricter definition. They compare their definition to [7, Proof of Theorem 7] and give an interesting example why a system should not be considered secure just because the adversary cannot come up with a valid encryption of anything. A data encapsulation mechanism $\mathcal{DEM}$ is said to be *non-malleable against* ATK *attacks* (NM-ATK) if the advantage function defined is a negligible function in k for all polynomial time adversaries.

On the existence of DEMs, they mention that a one-time pad [14] is an IND-OT DEM and therefore exists unconditionally. By adding a MAC to an arbitrary IND-OT DEM, one can obtain an IND-OTCCA DEM [3]. Note that using one-time pad as the DEM part for a hybrid encryption scheme would be inefficient, because it would require a KEM, which outputs long keys. The existence of IND-CPA/IND-CCA2 secure DEMs depends on the assumption that one-way functions exist, which was first explicitly noted in [11].

4 Internal relations of KEMs and DEMs

In the following sections, the summarised results are explained in more detail.

4.1 Relations among Key Encapsulation Mechanisms

The following covers theorems 3.1 to 3.5. The first theorem proves that a weak non-malleable KEM is also an indistinguishable KEM in respect to the same attack with an exception of CCA2. The other theorems have negative results. First, even the strongest wNM secure KEM does not imply the weakest (CPA) sNM secure KEM. Then they show that an IND-CCA1 secure KEM does not imply a weaker wNM secure KEM. Similarly a weak sNM KEM does not imply a stronger IND secure KEM. Finally, a stronger non-malleability CCA1 secure KEM does not imply a weak non-malleable stronger (CCA2) KEM.

Some proofs of the negative theorems use separation examples from theorems from [8].

4.2 Relations among Data Encapsulation Mechanisms

The following covers theorems 4.1 to 4.6. The first theorem shows, that a non-malleable scheme is strictly stronger than an indistinguishable scheme for all specified attacks.

The second theorem shows the two cases, when an indistinguishable scheme also implies a non-malleable scheme. This holds for two specific attacks, the OTCCA and CCA2.

The rest of the theorems show negative results, that is not implied cases. First, an indistinguishable OTCCA does not imply that the scheme is also indistinguishable under CPA. In the comparisons of indistinguishability to non-malleability, an IND-CCA1 scheme does not imply NM-OT. In the other direction, NM-CCA1 does not imply IND-OTCCA and NM-CPA does not imply IND-CCA1. With these theorems, the relations among DEMs have been covered.

Theorems 4.2, 4.4, 4.5 and 4.6 are closely connected to the works of Bellare *et. al* [8]. Theorem 4.3 follows from the works of Katz and Yung [7, Theorem 6].

5 Necessary and Sufficient Conditions for Hybrid Encryption

They begin by constructing the hybrid public key encryption scheme. Let $\mathcal{KEM}$ = (KEM.KG, KEM.Enc, KEM.Dec) be a public-key encapsulation mechanism (KEM), and $\mathcal{DEM}$ = (DEM.KG, DEM.Enc, DEM.Dec) be a data encapsulation mechanism (DEM. The compatibility of the schemes is assumed, such that for all security parameters k, the KEMs and DEMs key-space are equal. Then the hybrid public key encryption scheme $\mathcal{PKE}_{\mathcal{KEM},\mathcal{DEM}}$ = (PKE.KG,

PKE.Enc, PKE.Dec), which is constructed by combining $\mathcal{KEM}$ and $\mathcal{DEM}$ as follows:

- PKE.Kg - returns the KEM.Kg result (pk, sk) for the input security parameter k.
- PKE.Enc - uses KEM.Enc to create a key K and ciphertext of the key C_1 using public key pk. Then uses DEM.Enc to encrypt the message using K and gets C_2. Finally it returns (C_1, C_2).
- PKE.Dec - uses KEM.Dec to decrypt the key K from ciphertext C_1 using sk. Then uses DEM.Dec to decrypt the message from C_2 using K. Returns the decrypted message.

5.1 Theorems

The theorems about the hybrid schemes can be grouped as positive results and negative results. The first positive result describes how the security notion of the KEM propagates to the hybrid PKE scheme, even with a weaker notion for DEM. The CCA2 version of the proof is given in Theorem 5 of [3], and the others are said to be almost identical. The other positive theorems cover how the strong non-malleability notion PKE scheme propagates to the hybrid PKE scheme with a non-malleable weaker security notion.

The first negative results describe that a weak non-malleable KEM and an indistinguishable DEM both having the strongest security notion CCA2, do not imply a non-malleable CPA secure hybrid PKE scheme. The second negative result shows, that if the DEM is indistinguishable CCA1 secure, then the hybrid PKE scheme does not imply non-malleable chosen-plaintext attack security. The third negative theorem shows that a NM-CCA1 DEM does not imply IND-CCA2 secure hybrid PKE scheme. The fourth negative result shows how the sNM-CPA KEM holds down the IND-CCA2 DEM and does not imply IND-CCA1 secure hybrid PKE scheme. Similarly, the last negative result shows how the sNM-CCA1 secure KEM holds down the IND-CCA2 secure DEM and does not imply an IND-CCA2 secure hybrid PKE scheme.

Therefore, one can see how great an effect the KEMs security notion holds on the resulting scheme. However for a strong security, both components must have a strong security notion.

Acknowledgement

I would like to thank Professor Dominique Unruh for providing an interesting topic and for his guidance.

References

[1] J. Herranz, D. Hofheinz, and E. Kiltz, "KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption," 2006.

[2] V. Shoup, "A proposal for an ISO standard for public key encryption." http://shoup.net/papers/, 2001.

[3] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack." SIAM Journal on Computing, 33(1):167-226, 2003. 1, 2, 3, 4, 5, 9, 11, 13, 20.

[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption." In 38th Annual Symposium on Foundations of Computer Science, pages 394-403, Miami Beach, Florida, October 19-22, 1997. IEEE Computer Society Press. 11.

[5] C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack." In Joadn Feigenbaum, editor, Advances in Cryptology - CRYPTO'91, volume 576 of Lecture Notes in Computer Science, pages 433-444, Santa Barbara, CA, USA, August 11-15, 1992. Springer-Verlag, Berlin, Germany. 2.

[6] W. Nagao, Y. Manabe, and T. Okamoto, "On the equivalence of several security notions of key encapsulation mechanism." Cryptology ePrint Archive, Report 2006/268, 2006. http://eprint.iacr.org/2006/268.pdf. 2, 5, 11, 13, 15, 27.

[7] J. Katz and M. Yung, "Characterization of security notions for probabilistic private-key encryption." Journal of Cryptology, 19(1):67-96,2006. 2, 5, 12, 13, 18.

[8] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes." In Hugo Krawczyk, editor, Advances in Cryptology - CRYPTO'98, volume 1462 of Lecture Notes in Computer Science, pages 26-45, Santa Barbara, CA, USA, August 23-27, 1998. Springer-Verlag, Berlin, Germany. 2, 3, 4, 5, 6, 7, 8, 9, 13, 14, 18, 19, 23, 24, 25, 27.

[9] W. Nagao, Y. Manabe, and T. Okamoto, "A universally composable secure channel based on the KEM-DEM framework." In Joe Kilian, editor, TCC 2005: 2md Theory of Cryptography Conference, volume 3378 of Lecture Notes in Computer Science, pages 426-444, Cambridge, MA, USA, February, 10-12, 2005. Springer-Verlag. Berlin, Germany. 2, 4, 5, 10, 31.

[10] W. Nagao, Y. Manabe, and T. Okamoto, "A universally composable secure channel based on the KEM-DEM framework." IEICE Trans Fundamentals, E89-A(1):28-38, 2006. 2, 4, 5, 10, 31.

[11] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography." In 23rd Annual ACM Symposium on Theory of Computing, pages 542-552, New Orleans, Louisiana, USA, May 6-8, 1991. ACM Press. 4, 5, 6, 7, 13, 23.

[12] M. Bellare and A. Sahai, "Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization." IACR ePrint Archive, June 2006. Manuscript available online at http://eprint.iacr.org/2006/228.ps. 6, 8, 9, 29.

[13] M. Bellare and A. Sahai, "Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization." In Michael J. Wiener, editor, Advances in Cryptology - CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 519-536, Santa Barbara, CA, USA, August 15-19, 1999. Springer-Verlag, Berlin, Germany. 8, 8, 15.

[14] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications." Journal of the American Institue of Electrical Engineers, 45:109-115, 1926. 13.