Weak adaptive chosen ciphertext secure hybrid encryption scheme

Xianhui Lu[1], Xuejia Lai[2], Dake He[1], Guomin Li[1]
Email:luxianhui@gmail.com

1:School of Information Science & Technology, SWJTU, Chengdu, China
2:Dept. of Computer Science and Engineering, SJTU, Shanghai, China

Abstract. We propose a security notion named as weak adaptive chosen ciphertext security(IND-WCCA) for hybrid encryption schemes. Although it is weaker than adaptive chosen ciphertext security(IND-CCA), a IND-WCCA secure hybrid encryption scheme can be used in any situations that a IND-CCA secure hybrid encryption scheme used in. We show that IND-WCCA secure hybrid encryption scheme can be constructed from IND-CCA secure KEM and IND-PA secure DEM. Since IND-PA is the basic requirement of symmetric key encryption schemes, IND-WCCA hybrid encryption scheme is very flexible and can use most of the stream ciphers and block ciphers as the DEM part of the scheme. Use the new secure notion we can refine current IND-CCA secure hybrid encryption schemes and get more efficient IND-WCCA secure hybrid encryption schemes.

Keywords: hybrid encryption, KEM, DEM, IND-WCCA

1 Introduction

Public key encryption schemes(also called asymmetric encryption schemes) often limit the message space to a particular group, which can be restrictive when one wants to encrypt arbitrary messages. For this purpose hybrid schemes are devised. In these cryptosystems a symmetric encryption scheme is used to overcome the problems typically associated with encrypting long messages using "pure" asymmetric techniques. This is typically achieved by encrypting the message with a symmetric encryption scheme and a randomly generated symmetric key. This random symmetric key is then somehow encrypted using an asymmetric encryption scheme. This approach has been successfully used for many years [2–9]. One important advance in hybrid cryptography is the development of the KEM/DEM model for hybrid encryption algorithms [10]. This model splits a hybrid encryption scheme into two distinct components: an asymmetric key encapsulation mechanism (KEM) and a symmetric data encapsulation mechanisms (DEM). Whilst the KEM/DEM model does not model all possible hybrid encryption schemes, and there are several examples of hybrid encryption schemes that do not fit into the KEM/DEM model [3, 4, 17], it does have the advantage of allowing the security requirements of the asymmetric and symmetric parts of the scheme to be completely separated and studied independently. This approach has proven to be very popular and several emerging standards are strongly supporting its use, including the ISO/IEC standard on asymmetric encryption [11].

Security against adaptive chosen ciphertext attacks (IND-CCA security) [19–21] is a strong and useful notion of security for public key encryption schemes, and it is commonly accepted as the security notion of choice for encryption schemes that are to be plugged into a protocol running in an arbitrary setting [22]. As a kind of public key encryption scheme, hybrid encryption schemes are designed to be IND-CCA secure. Cramer and Shoup's work[10] shows that in order to obtain a IND-CCA secure hybrid encryption scheme, it is sufficient that both KEM and DEM are IND-CCA

secure. Kurosawa and Desmedt proposed an efficient hybrid scheme named as KD04[17]. Although the key encapsulation part of KD04(KD04-KEM) is not IND-CCA secure [25], the whole scheme can be proved to be IND-CCA secure. Thus Kurosawa-Desmedt's scheme points out that to obtain IND-CCA secure hybrid encryption, requiring both KEM/DEM to be IND-CCA secure, while being a sufficient condition, may not be a necessary one, and might indeed be an overkill.

1.1 Our contributions

We propose a security notion named as weak adaptive chosen ciphertext security(IND-WCCA) for hybrid encryption schemes. In an adaptive chosen ciphertext attack game the adversary is forbidden to query the decryption oracle with the challenge ciphertext. We notice that if one can refuse to decrypt the challenge ciphertext he can also refuse to decrypt a ciphertext whose KEM part is the same as that of the challenge ciphertext. So we define the weak adaptive chosen ciphertext attack game, in which the adversary is not allowed to query the decryption oracle with a ciphertext whose KEM part is the same as that of the the challenge ciphertext. We see that if we refuse to decrypt any ciphertext whose KEM part is the same as that of the challenge ciphertext, then a IND-WCCA secure hybrid encryption scheme can be used in any situations that a IND-CCA secure hybrid encryption scheme used in, although it is weaker than adaptive chosen ciphertext security.

We show that a IND-WCCA secure hybrid encryption scheme can be constructed from a IND-CCA secure KEM and a IND-PA secure DEM. Since IND-PA is the basic requirement of symmetric key encryption schemes, IND-WCCA hybrid encryption scheme is very flexible and can use most of the stream ciphers and block ciphers as the DEM part of the scheme. Use the new security notion we can refine current IND-CCA secure hybrid encryption schemes and get more efficient IND-WCCA secure hybrid encryption schemes.

1.2 Related work

tag-KEM: Abe et al presented a new framework[23], which makes use of a new object called "tag-KEM". They defined an independent security criteria for the tag-KEM. The security criteria that they propose for the tag-KEM is stricter than for a KEM (a secure KEM will not be a secure tag-KEM) but allows for the use of a DEM that is only secure against passive attacks. Using this new framework they can refine several hybrid schemes including Fujisaki-Okamoto conversion[3],Ballare and Rogaway's scheme[2] and REACT-RSA[9].

Remove MAC from DHIES: M. Abdalla, M. Bellare and P. Rogaway proposed an efficient Diffie-Hellman Integrated Encryption Scheme(DHIES)[7]. DHIES is now embodied in three(draft) standards [13–15]. It is a natural extension of the ElGamal scheme[1], and enhanced ElGamal in a couple of ways important to cryptographic practice. First, it provides the capability of encrypting arbitrary bit strings while ElGamal requires that message be a group element. Second, it is secure against chosen ciphertext attack , while ElGamal is secure against chosen plaintext attack. Most importantly DHIES realized the above two goals without increasing the number of group operations for encryption and decryption, and without increasing key sizes relative to ElGamal. The CCA security of DHIES relies on the Oracle Diffie-Hellman assumption(ODH). Kurosawa and Matsuo[18] showed that MAC can be eliminated from DHIES if the underlying symmetric-key encryption(SKE) scheme is secure in the sense of IND-CCA(secure against adaptive chosen ciphertext attacks). Their scheme offers the first secure public-key encryption scheme with no redundancy in the standard model.

Secure hybrid encryption from weakened KEM: Hofheinz and Kiltz[26] put forward a new paradigm for building hybrid encryption schemes from constrained chosen ciphertext secure (CCCA) KEMs plus authenticated symmetric encryption scheme. CCCA has less demanding security requirements than standard adaptive chosen ciphertext security, it requires the adversary to have a certain plaintext knowledge when making a decapsulation query. CCCA can be used to express the kurosawa-Desmedt hybrid encryption scheme its generalizations to hash-proof systems in an abstract KEM/DEM security framework.

Tight security without redundancy: Boyen[27] presents a minimalist public key encryption scheme, as compact as ElGamal, but with adaptive chosen-ciphertext security under the gap Diffie-Hellman assumption in the random oracle model. Boyen uses a dual-hash device that provides tight redundancy-free implicit validation. The system is very simple and compact: on elliptic curves with 80-bit security, a 160-bit plaintext becomes a 320-bit ciphertext.

1.3 Outline

In section 2 we review the basic definitions of KEM, DEM, hybrid encryption scheme, Oracle Diffie-Helmman assumption and decisional Diffie-Hellman assumption. In section 3 we propose the new security notion for hybrid encryption scheme:weak adaptive chosen ciphertext security(IND-WCCA security) and showed that IND-WCCA secure hybrid encryption scheme can be construct from IND-CCA secure KEM and IND-PA(secure against passive attack) secure DEM. In section 4 we show that using the new security notion the existing hybrid encryption scheme can be refined and yield more efficient scheme. Finally we give the conclusion in section 5.

2 Preliminaries

In this section we review the definitions of KEM, DEM,hybrid encryption scheme, Oracle Diffie-Hellman assumption.

In describing probabilistic processes, we write $x \xleftarrow{R} X$ to denote the action of assigning to the variable x a value sampled according to the distribution X. If S is a finite set, we simply write $s \xleftarrow{R} S$ to denote assignment to s of an element sampled from uniform distribution on S. If A is a probabilistic algorithm and x an input, then $A(x)$ denotes the output distribution of A on input x. Thus, we write $y \xleftarrow{R} A(x)$ to denote of running algorithm A on input x and assigning the output to the variable y.

2.1 Key Encapsulation Mechanism

A key encapsulation mechanism consists the following algorithms:

- KEM.KeyGen(1^k): A probabilistic polynomial-time key generation algorithm takes as input a security parameter (1^k) and outputs a public key PK and secret key SK. We write (PK,SK) $\leftarrow$ KEM.KeyGen(1^k)
- KEM.Encrypt(PK): A probabilistic polynomial-time encryption algorithm takes as input the public key PK, and outputs a pair (K, ψ), where $K \in K_D (K_D$ is the key space) is a key and ψ is a ciphertext. We write $(K, \psi) \leftarrow$ KEM.Encrypt(PK)

– KEM.Decrypt(SK, ψ): A decryption algorithm takes as input a ciphertext ψ and the secret key SK. It returns a key K. We write $K \leftarrow$ KEM.Decrypt(SK, ψ).

We require that for all (PK,SK) output by KEM.KeyGen(1^k), all $(K, \psi) \in$ [KEM.Encrypt(PK)], we have KEM.Decrypt(SK, ψ)=K.

A KEM scheme is secure against adaptive chosen ciphertext attacks if the advantage of any adversary in the following game is negligible in the security parameter k:

1. The adversary queries a key generation oracle. The key generation oracle computes (PK,SK) $\leftarrow$ KEM.KeyGen(1^k) and responds with PK.
2. The adversary makes a sequence of calls to the decryption oracle. For each decryption oracle query the adversary submits a ciphertext ψ, and the decryption oracle responds with KEM.Decrypt(SK, ψ).
3. The adversary queries an encryption oracle. The encryption oracle computes:
$$b \xleftarrow{R} \{0,1\}; (K_0, \psi^*) \leftarrow \text{PKE.Encrypt}(\text{PK}, m_b); K_1 \xleftarrow{R} K_D;$$
and responds with (K_b, ψ^*).
4. The adversary continues to make calls to the decryption oracle except that it may not request the decryption of ψ^*.
5. Finally, the adversary outputs a guess b'.

The adversary's advantage in the above game is $\text{AdvCCA}_{\text{KEM},A}(k) = |\Pr[b = b'] - 1/2|$. If a KEM is secure against adpative chosen ciphertext attack defined in the above game we say it is IND-CCA secure.

2.2 Data Encapsulation Mechanism

A data encapsulation mechanism DEM consists of two algorithms:

– DEM.Encrypt(k, m): The deterministic, polynomial-time encryption algorithm takes as input a key k, and a message m, and outputs a ciphertext χ. We write $\chi \leftarrow DEM.Encrypt(k, m)$
– DEM.Decrypt(k, χ): The deterministic, polynomial-time decryption algorithm takes as input a key k, and a ciphertext χ, and outputs a message m or the special symbol $reject$. We write $m \leftarrow DEM.Decrypt(k, \chi)$

We require that for all $kLen \in N$, for all $k \in \{0,1\}^{kLen}$,$kLen$ denotes the length of the key of DEM, and for all $m \in \{0,1\}^*$,we have:

$$DEM.Decrypt(k, DEM.Encrypt(k, m)) = m.$$

A DEM is secure against passive attacks if the advantage of any probabilistic, polynomial-time adversary A in the following game is negligible in the security parameter kLen:

1. The challenger randomly generates an appropriately sized key $k \in \{0,1\}^{kLen}$.
2. A queries an encryption oracle with two messages m_0, m_1 , $|m_0| = |m_1|$. A bit b is randomly chosen and the adversary is given a "challenge ciphertext" $\chi^* \leftarrow DEM.Encrypt(k, m_b)$.
3. Finally, A outputs a guess b' .

The adversary's advantage in the above game is defined as $AdvPA_{DEM,A}(kLen) = |\Pr[b = b'] - 1/2|$. If a DEM is secure against passive attack defined in the above game we say it is IND-PA secure.

2.3 Hybrid Encryption Scheme

A hybrid encryption scheme is a combination of KEM and DEM consists the following algorithms:

- HE.KeyGen(1^k): Hybrid encryption scheme use the key generation algorithm of KEM as it's key generation algorithm which is a probabilistic polynomial-time algorithm takes as input a security parameter (1^k) and outputs a public key/secret key pair (PK,SK). We write (PK,SK) $\leftarrow$ HE.KeyGen(1^k).
- HE.Encrypt(PK,m): Given plaintext m and the public key PK, the encryption algorithm of hybrid encryption scheme works as follow:

  $$(k, \psi) \leftarrow \text{KEM.Encrypt(PK)}; \chi \leftarrow DEM.Encrypt(k, m); C \leftarrow (\psi, \chi)$$

  First, the encryption algorithm use the encryption algorithm of KEM produce a key k and it's ciphertext ψ, using key as the key it use the encryption algorithm of DEM to encrypt the plaintext m and get the ciphertext χ. Finally it get the ciphertext of the hybrid encryption scheme including ψ and χ.
- HE.Decrypt(SK,C): Given ciphertext $C = (\psi, \chi)$ and private key SK, the decryption algorithm of hybrid encryption works as follow.

  $$k \leftarrow \text{KEM.Decrypt(SK}, \psi); m \leftarrow DEM.Decrypt(k, \chi)$$

  First, the decryption algorithm use the decryption algorithm of KEM to decrypt ψ and get the key k, then using k as the key it use the decryption algorithm of DEM to decrypt χ and get the plaintext m.

A hybrid encryption scheme is secure against adaptive chosen ciphertext attacks if the advantage of any adversary in the following game is negligible in the security parameter k:

1. The adversary queries a key generation oracle. The key generation oracle computes (PK,SK) $\leftarrow$ HE.KeyGen(1^k) and responds with PK.
2. The adversary makes a sequence of calls to the decryption oracle. For each decryption oracle query the adversary submits a ciphertext C, and the decryption oracle responds with HE.Decrypt(SK, C).
3. The adversary submits two messages m_0, m_1 with $|m_0| = |m_1|$. On input m_0, m_1 the encryption oracle computes:

   $$b \xleftarrow{R} \{0,1\}; C^* \leftarrow \text{HE.Encrypt(PK}, m_b)$$

   and responds with C^*.
4. The adversary continues to make calls to the decryption oracle except that it may not request the decryption of C^*.
5. Finally, the adversary outputs a guess b'.

We say the adversary succeeds if $b' = b$, and denote the probability of this event by $\Pr_{\text{A}}[\text{Succ}]$. The adversary's advantage is defined as $\text{AdvCCA}_{\text{HE,A}} = |\Pr_{\text{A}}[\text{Succ}] - 1/2|$. If a hybrid encryption scheme is secure against adaptive chosen ciphertext attack defined in the above game we say it is IND-CCA secure.

2.4 Oracle Diffie-Hellman Assumption

Now we review the definition of oracle Diffie-Hellman assumption[7]. Let G be a group of large prime order q, $H : \{0,1\}^* \to \{0,1\}^{hLen}$ be a cryptographic hash function and consider the following two experiments:

experiments $\mathrm{Exp}^{odh-real}_{G,H,A}$:

$$u \overset{R}{\leftarrow} Z_q^*; U \leftarrow g^u; v \overset{R}{\leftarrow} Z_q^*; V \leftarrow g^v; W \leftarrow H(g^{uv})$$

$$\mathcal{H}_v(X) \overset{def}{=} H(X^v); b \leftarrow A^{\mathcal{H}_v(\cdot)}(U,V,W); \text{return } b$$

experiments $\mathrm{Exp}^{odh-rand}_{G,H,A}$:

$$u \overset{R}{\leftarrow} Z_q^*; U \leftarrow g^u; v \overset{R}{\leftarrow} Z_q^*; V \leftarrow g^v; W \leftarrow \{0,1\}^{hLen}$$

$$\mathcal{H}_v(X) \overset{def}{=} H(X^v); b \leftarrow A^{\mathcal{H}_v(\cdot)}(U,V,W); \text{return } b$$

Now define the advantage of the A in violating the oracle Diffie-Hellman assumption as

$$Adv^{odh}_{G,H,A} = \Pr[\mathrm{Exp}^{odh-real}_{G,H,A} = 1] - \Pr[\mathrm{Exp}^{odh-rand}_{G,H,A} = 1]$$

Here A is allowed to make oracle queries that depend on the g^u with the sole restriction of not being allowed to query g^u itself. When it is the $\mathrm{Exp}^{odh-rand}_{G,H,A}$ experiment we say (g,U,V,W) comes from the random distribution R, otherwise we say (g,U,V,W) comes from the ODH distribution O.

3 Weak chosen ciphertext security

In this section we describe the new security notion named as weak adaptive chosen ciphertext security(IND-WCCA) for hybrid encryption schemes. In an adaptive chosen ciphertext attack game the adversary is forbidden to query the decryption oracle with the challenge ciphertext. Different with pure asymmetric encryption scheme there are two independent part in the ciphertext of a hybrid encryption scheme, ciphertext of the KEM part and ciphertext of the DEM part. We notice that if one can refuse to decrypt the challenge ciphertext he can also refuse to decrypt a ciphertext whose KEM part is the same as that of the challenge ciphertext. In fact checking only the KEM ciphertext part is more efficient than checking the whole ciphertext. So we define the weak adaptive chosen ciphertext attack game, in which the adversary is not allowed to query the decryption oracle with any ciphertext whose KEM part is the same as that of the challenge ciphertext. It is clear that if we reject all the ciphertext whose KEM part is the same as that of the challenge ciphertext then there will be no difference between IND-WCCA and IND-CCA. We see that although IND-WCCA is weaker than IND-CCA, a IND-WCCA secure hybrid encryption scheme can be used in any situations that a IND-CCA secure hybrid encryption scheme used in. Now we give the detail description of IND-WCCA security.

A hybrid encryption scheme is secure against weak adaptive chosen ciphertext attacks if the advantage of any adversary in the IND-WCCA game defined in the following is negligible in the security parameter k:

1. The adversary queries a key generation oracle. The key generation oracle computes (PK,SK) $\leftarrow$ HE.KeyGen(1^k) and responds with PK.
2. The adversary makes a sequence of calls to the decryption oracle. For each decryption oracle query the adversary submits a ciphertext $C_i = (\psi_i, \chi_i)$, and the decryption oracle responds with HE.Decrypt(SK, C_i).
3. The adversary submits two messages m_0, m_1 with $|m_0| = |m_1|$. On input m_0, m_1 the encryption oracle computes:

$$b \overset{R}{\leftarrow} \{0,1\}; (\psi^*, \chi^*) \leftarrow \text{HE.Encrypt}(\text{PK}, m_b)$$

   and responds with $C^* = (\psi^*, \chi^*)$.
4. The adversary continues to make calls to the decryption oracle except that it may not request the decryption of ciphertext $C_i = (\psi_i, \chi_i)$ that $\psi_i = \psi^*$.
5. Finally, the adversary outputs a guess b'.

We say the adversary succeeds if $b' = b$, and denote the probability of this event by $\Pr_{\text{A}}[\text{Succ}]$. The adversary's advantage is defined as $\text{AdvWCCA}_{\text{HE,A}} = |\Pr_{\text{A}}[\text{Succ}] - 1/2|$. If a hybrid encryption scheme is secure against weak adaptive chosen ciphertext attack defined in the above game we say it is IND-WCCA secure.

We will show that a IND-WCCA secure hybrid encryption scheme can be constructed from a IND-CCA secure KEM and a IND-PA secure DEM.

Theorem 1. *The KEM/DEM hybrid encryption scheme is secure against weak adaptive chosen ciphertext attacks assuming that (1) KEM is secure against adaptive chosen ciphertext attack, (2) DEM is secure against passive attack.*

Suppose there is an adversary can break the KEM/DEM hybrid encryption scheme in the IND-WCCA attack game. From the definition we see that the IND-WCCA game can be seen as the IND-CCA game of KEM. If KEM is IND-CCA secure, then the key that DEM uses to encrypt the challenge plaintext is independent from the adversary's view except a negligible probability $AdvCCA_{KEM,A}$. So the IND-WCCA game can be seen as the IND-PA attack game of DEM. Since DEM is IND-PA secure, b is independent from the adversary's view except a negligible probability $AdvPA_{DEM,A}$. Finally we get that:

$$AdvWCCA_{HE,A} \leq AdvPA_{DEM,A} + AdvCCA_{KEM,A}$$

Since $AdvPA_{DEM,A}$ and $AdvCCA_{KEM,A}$ are negligible values we have that $AdvPA_{DEM,A} + AdvCCA_{KEM,A}$ is also a negligible value. So $AdvWCCA_{HE,A}$ is negligible and the hybrid encryption scheme is IND-WCCA secure.

That completes the proof of theorem 1.

4 IND-WCCA secure hybrid encryption scheme

In section 3 we showed that IND-WCCA secure hybrid encryption schemes can be constructed from IND-CCA secure KEM and IND-PA secure DEM. So use the new security notion we can refine current IND-CCA secure hybrid encryption schemes and get more efficient IND-WCCA secure hybrid encryption schemes. In this section we give an efficient hybrid scheme from DHIES[7] as an example. Finally we compare the new scheme with the most efficient existing schemes and show that the new scheme is more efficient.

4.1 IND-WCCA secure hybrid encryption scheme from DHIES

Remove the MAC from DHIES[7] we can get a IND-WCCA secure hybrid scheme WDHIES as follow:

- $HE.KeyGen(1^k)$: Assume that G is group of order q where q is a large prime.

$$g \overset{R}{\leftarrow} G; x \overset{R}{\leftarrow} Z_q^*; h \leftarrow g^x$$

$$PK = (g, h, H, DEM); SK = (x)$$

  Here $H : \{0,1\}^* \rightarrow \{0,1\}^{kLen}$ is a cryptographic hash function used in ODH oracle, DEM is secure against passive attack.
- $HE.Encrypt(PK, m)$: Given a message m, the encryption algorithm runs as follows.

$$r \overset{R}{\leftarrow} Z_q^*; \psi \leftarrow g^r; k \leftarrow H(h^r); \chi \leftarrow DEM.Encrypt(k, m);$$

$$C \leftarrow (\psi, \chi)$$

- $HE.Decrypt(SK, C)$: Given a ciphertext $C = (\psi, \chi)$, the decryption algorithm runs as follows.

$$k \leftarrow H(\psi^x); m \leftarrow DEM.Decrypt(k, \chi);$$

Before the formal security proof we give some intuition to show that the new scheme is secure against weak active attacks. The ODH(Oracle Diffie-Hellman)[7] assumption guarantees that different KEM ciphertexts(c_1) will yield different keys independent to each other. So the adversary can not get the information of b from the decryption oracle. The ODH assumption also assures that the adversary can not get the information of b from the challenge ciphertext(the output of the encryption oracle). Finally we have that the new scheme is IND-WCCA secure based on the ODH assumption.

Now we give the formal proof of the new scheme.

Theorem 2. *WDHIES is secure against weak adaptive chosen ciphertext attack assuming that (1) the oracle Diffie-Hellman problem is hard in group G,(2)DEM is IND-PA secure.*

To prove the theorem, we will assume that there is an adversary that can break the cryptosystem, and DEM is IND-PA secure and show how to use this adversary to construct a statistical test for the ODH problem.

For the statistical test, we are given $(\hat{g}, U, V, W)$ coming from either the random distribution R or the ODH distribution O. At a high level, our construction works as follows. We build a simulator that simulates the joint distribution consisting of adversary's view in its attack on the cryptosystem, and the hidden bit b generated by the generated oracle (which is not a part of the adversary's view). We will show that if the input comes from O, the simulation will be nearly perfect, and so the adversary will have a non-negligible advantage in guessing the hidden bit b. We will also show that if the input comes from R, then the adversary's view is essentially independent of b, and therefore the adversary's advantage is negligible. This immediately implies a statistical test distinguishing R from O: run the simulator and adversary together, and if the simulator outputs b and the adversary outputs b', the distinguisher outputs 1 if $b = b'$, and 0 otherwise.

We now give the details of the simulator. The input to the simulator is (g, U, V, W). The simulator sets $h \leftarrow V$. The public key that the adversary sees is (g, h, H, DEM), where $H : \{0,1\}^* \rightarrow \{0,1\}^{kLen}$ is a cryptographic hash function used in ODH oracle, DEM is secure against passive attack.

First we describe the simulation of the encryption oracle. Given m_0, m_1, the simulator chooses $b \in \{0,1\}$ at random, and computes

$$k \leftarrow W; \psi \leftarrow U; \chi \leftarrow DEM.Encrypt(k, m_b);$$

and outputs (ψ, χ)

We now describe the simulation of the decryption oracle. Given (ψ_i, χ_i), the simulator runs as follow:

$$k_i \leftarrow \mathcal{H}_v(\psi_i)$$

$$m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$$

here $\mathcal{H}_v(X) = H(X^v)$ is the ODH oracle. Finally the simulator outputs m_i.

That completes the description of the simulator. As we will see the theorem now follows immediately from the following two lemmas.

Lemma 1. *If the simulator's input comes from O, the joint distribution of the adversary's view and the hidden bit b is statistically indistinguishable from that in the actual attack.*

Consider the joint distribution of the adversary's view and the bit b when the input comes from the distribution O. Say $U = g^u, V = g^v, W = H(g^{uv})$.

It is clear in this case that the output of the encryption oracle has the right distribution, since:

$$k = W = H(g^{uv}) = H(h^u); \psi = U = g^u$$

To complete the proof, we need to argue that the output of the decryption oracle has the right distribution. Given (ψ_i, χ_i), since the adversary is not allowed to query the decryption oracle with ciphertext that $\psi_i = \psi = U$ we have:

$$\mathcal{H}_v(\psi_i) = \mathcal{H}_v(g^{r_i}) = H(g^{vr_i}) = H(V^{r_i}) = H(h^{r_i}) = k_i$$

$$DEM.Decrypt(k_i, \chi_i) = m_i$$

therefore, the decryption oracle outputs m_i just as it should. So the joint distribution of the adversary's view and the hidden bit b is just the same as that in the actual attack.

Lemma 2. *If the simulator's input comes from R, the distribution of the hidden bit b is (essentially) independent from the adversary's view.*

Let $U = g^u, V = g^v, W = H(g^w), w \neq uv$. It is clear that the distribution of $k = W$ is independent from the adversary's view condition on $\psi = U = g^u$ and the adversary can not get the information of $k = W$ from the decryption oracle too. So the distribution of $k = W$ is independent from the adversary's view. Since DEM is IND-PA secure, it yield that the distribution of the hidden bit b is independent from the adversary's view.

This complete the proof of theorem 2.

Table 1. Efficiency comparison

Scheme	Encryption(exp)	Decryption(exp)	Cipher-text overhead(bit)	Assumption	DEM Security
DHIES	2(2exp+0mexp)	1(1exp+0mexp)	$\|q\| + \|t\|$	ODH	IND-CPA
KM04	2(2exp+0mexp)	1(1exp+0mexp)	$\|q\|$	ODH	IND-CCA
Boyen07	2(2exp+0mexp)	1(1exp+0mexp)	$\|q\|$	GDH,ROM	
WDHIES	2 (2exp+0mexp)	1(1exp+0mexp)	$\|q\|$	ODH	IND-PA

4.2 Efficiency Compare

The efficiency of our schemes, DHIES, KM04, Boyen07 is listed in table 1.

In table1 DHIES is the scheme in [7], KM04 is the scheme in [18], Boyen07 is the scheme in [27]. When tabulating computational efficiency hash function and block cipher evaluations are ignored, multi-exponentiation ($mexp$) is counted as 1.5 exponentiations (exp). Ciphertext overhead represents the difference between the ciphertext length and the message length, and $|q|$ is the length of a group element,$|t|$ is the length of the tag in DHIES.

It is clear that WDHIES is more efficient than DHIES in bandwidth and the same efficient as KM04 and Boyen07. WDHIES only need a IND-PA secure DEM , while KM04 need a IND-CCA secure DEM. Compared with Boyen07, WDHIES is more simple and secure in the standard model, while Boyen07 is secure in random oracle model.

5 Conclusion

Hybrid encryption scheme is a kind of public key encryption scheme that contains two independent part, the KEM part and the DEM part. Accordingly there are two independent part in the ciphertext of hybrid encryption schemes, ciphertext of the KEM part and ciphertext of the DEM part. In the traditional IND-CCA attack game on public key encryption scheme, the adversary is not allowed to query the decryption oracle with the challenge ciphertext. We notice that in the case of hybrid encryption scheme if one can reject to decrypt ciphertext which is the same as the challenge ciphertext, he can also reject to decrypt ciphertexts whose KEM part is the same as that of the challenge ciphertext. So we propose a security notion named as weak adaptive chosen ciphertext security(IND-WCCA) for hybrid encryption schemes. In the IND-WCCA attack game on a hybrid encryption scheme the adversary is not allowed to query the decryption oracle with ciphertexts whose KEM part is the same that of the challenge ciphertext. Although it is weaker than adaptive chosen ciphertext security(IND-CCA), a IND-WCCA secure hybrid encryption scheme can be used in any cases that a IND-CCA secure hybrid encryption scheme used in. We show that IND-WCCA secure hybrid encryption scheme can be constructed from IND-CCA secure KEM and IND-PA secure DEM. Since IND-PA is the basic requirement of symmetric key encryption schemes, IND-WCCA hybrid encryption scheme is very flexible and can use most stream ciphers and block ciphers as the DEM part of the scheme. Use the new secure notion we can refine current IND-CCA secure hybrid encryption schemes and get more efficient IND-WCCA secure hybrid encryption schemes.

References

1. T. ElGamal. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31:469C472, 1985.

2. M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In 1st ACM CCCS, pages 62C73. Association for Computing Machinery, 1993.
3. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In M. Wiener, editor, Advances in Cryptol- ogy - Crypto '99, volume 1666 of Lecture Notes in Computer Science, pages 535-554. Springer-Verlag, 1999.
4. T. Okamoto, S. Uchiyama, and E. Fujisaki. EPOC: Efficient probabilistic public-key encryption. Submission to P1363a: Standard Specications for Public-Key Cryptography, Additional Techniques, 1999.
5. S. Lucks. A variant of the Cramer-Shoup cryptosystem for groups of unknown order. In Y. Zheng, editor, Advances in Cryptology - Asiacrypt 2002, volume 2501 of Lecture Notes in Computer Science, pages 27-45. Springer-Verlag, 2002.
6. M. Abdalla, M. Bellare, and P. Rogaway. DHAES: An encryption scheme based on the Diffie-Hellman problem. Submission to P1363a: Standard Specications for Public-Key Cryptography, Additional Techniques, 2000.
7. M. Abdalla, M. Bellare and P. Rogaway. DHIES: An encryption scheme based on the Diffie-Hellman Problem Extended abstract, entitled The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES, was in Topics in Cryptology - CT-RSA 01, Lecture Notes in Computer Science Vol. 2020, D. Naccache ed, Springer-Verlag, 2001
8. V. Shoup. Using hash functions as a hedge against chosen ciphertext attack. In B. Preneel, editor, Advances in Cryptology - Eurocrypt 2000, volume 1807 of Lecture Notes in Computer Science, pages 275-288. Springer-Verlag, 2000.
9. T. Okamoto and D. Pointcheval. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In RSA 2001, LNCS, Springer-Verlag, 2001.
10. 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.
11. International Organization for Standardization. ISO/IEC CD 18033- 2, Information technology – Security techniques – Encryption Algo- rithms – Part 2: Asymmetric Ciphers, 2003.
12. International Organization for Standardization. ISO/IEC 18033-1, Information technology – Security techniques – Encryption Algorithms – Part 1: General, 2003.
13. American National Standards Institute (ANSI) X9.F1 subcommittee. ANSI X9.63 Public key cryptography for the Financial Services Industry: Elliptic curve key agreement and key transport schemes, July 5 1998. Working draft version 2.0.
14. IEEE P1363a Committee. IEEE P1363a / D9 standard specifications for public key cryptography: Additional techniques. http://grouper.ieee.org/groups/1363/index.html/, June 2001. Draft Version 9.
15. Certicom research, standards for efficient cryptography group (SECG) sec 1: Elliptic curve cryptography. http://www.secg.org/secg_docs.htm, Sept. 20 2000. Version 1.0.
16. V. Shoup. ISO 18033-2: An emerging standard for public-key encryption (committee draft). Available at http://shoup.net/iso/, June 3 2004.
17. K. Kurosawa and Y. Desmedt. A new paradigm of hybrid encryp- tion scheme. In M. Franklin, editor, Advances in Cryptology - Crypto 2004, volume 3152 of Lecture Notes in Computer Sciene, pages 426-442. Springer-Verlag, 2004.
18. Kaoru Kurosawa and Toshihiko Matsuo. How to remove MAC from DHIES. In Proceedings of ACISP 2004, volume 3108 of LNCS, pages 236C47. Springer, 2004.
19. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations Among Notions of Security for Public-Key Encryption Schemes", *Adv. in Cryptology - Crypto 1998*, LNCS vol. 1462, Springer-Verlag, pp. 26-45, 1998;
20. D. Dolev, C. Dwork, and M. Naor, "Non-Malleable Cryptography", *SIAM J. Computing* , 30(2): 391-437, 2000;
21. C. Rackoff and D. Simon, "Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack", *Adv. in Cryptology - Crypto 1991*, LNCS vol. 576, Springer- Vrlag , pp. 433-444, 1991;
22. V. Shoup, "Why Chosen Ciphertext Security Matters", *IBM Research Report RZ 3076*, November , 1998. Available at http://www.shoup.net/papers;
23. Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup, Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM", by Abe, Gennaro, Kurosawa, and Shoup, in Proc. Eurocrypt 2005.
24. Victor Shoup, Sequences of games: a tool for taming complexity in security proofs, manuscript, Nov. 30, 2004. Revised, May 27, 2005; Jan. 18, 2006. http://shoup.net/papers/
25. D. Hofheinz, J. Herranz, and E. Kiltz. The Kurosawa-Desmedt key encapsulation is not chosen-ciphertext secure. Cryptology ePrint Archive, Report 2006/207, 2006. http://eprint.iacr.org
26. Dennis Hofheinz and Eike Kiltz. Secure Hybrid Encryption from Weakened Key Encapsulation. Advances in Cryptology – CRYPTO 2007, pp. 553–571 LNCS 4622 (2007).Springer-Verlag.

27. Xavier Boyen. Miniature CCA2 PK Encryption : Tight Security Without Redundancy. In Advances in Cryptology (ASIACRYPT 2007), volume 4833 of Lecture Notes in Computer Science, pages 485-501. Springer, 2007