MAC-free variant of KD04

Xianhui Lu[1], Xuejia Lai[2], Dake He[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. Kurosawa and Desmedt proposed an efficient hybrid encryption scheme(KD04) which is secure against adaptive chosen ciphertext attacks(IND-CCA) although the underlying KEM(key encapsulation mechanism) is not IND-CCA secure[11]. We show a variant of KD04 which is IND-CCA secure when the the underlying DEM part is IND-CCA secure. We need a DEM built from one-time symmetric encryption scheme and a MAC in the security reduction to check if the KEM part of a ciphertext is valid. However in the real situation we can check if the KEM part of the ciphertext is valid without the help of the MAC. So the hybrid encryption scheme can also use redundancy-free IND-CCA secure DEMs that avoid the overhead due to the MAC. When using redundancy-free(MAC-free) IND-CCA secure DEMs, the new scheme will be more efficient than KD04 in bandwidth.

Keywords: hybrid encryption, IND-CCA, DEM, MAC-free

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. 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). 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[11]. Although the key encapsulation part of KD04(KD04-KEM) is not IND-CCA secure [16], 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.

A IND-CCA secure DEM can be built from any one-time symmetric encryption scheme and a MAC(MAC-DEM)[10]. Phan and Pintcheval showed that strong pseudorandom permutations(PRPs) directly imply redundancy-free IND-CCA secure DEMs that avoid the usual overhead due to the MAC[15]. It seems reasonable to believe that known block-ciphers(such as AES) are strong PRPs[13, 12, 14].

1.1 Our Contributions

We show a variant of KD04 which is IND-CCA secure when the the underlying DEM part is IND-CCA secure. In the security reduction the simulator only hold part of the private key and can not check whether the KEM part of a ciphertext is valid. So we need a DEM built from one-time symmetric encryption scheme and a MAC[10] in the security reduction to check if the KEM part of a ciphertext is valid. However in the real situation we have the whole private key and can check if the KEM part of the ciphertext is valid without the help of the MAC. So the hybrid encryption scheme can also use redundancy-free chosen ciphertext secure DEMs that avoid the overhead due to the MAC[13, 12, 14, 15]. When using redundancy-free IND-CCA secure DEMs, the new scheme will be more efficient than KD04 in bandwidth.

1.2 Related work

Kiltz07-KEM: Kiltz proposed a practical KEM(Kiltz07-KEM) which is proved to be secure against adaptive chosen ciphertext attacks in the standard model under a new assumption, the Gap Hashed Diffie-Hellman(GHDH) assumption[18]. Using a redundancy-free IND-CCA secure DEM, Kiltz07-KEM will yield a hybrid encryption scheme(Kiltz07-Hybrid) that is more efficient than KD04 in bandwidth. Although it is the same efficient as our new scheme Kiltz07-Hybrid is IND-CCA secure under the GHDH assumption which is less popular than the DDH assumption.

Secure hybrid encryption from weakened KEM: Hofheinz and Kiltz[17] 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.

MAC-free KD04 variant with πPRF: Okamoto proposed a variant of KD04-KEM using a πPRF(pseudo-random function with pairwise-independent random sources) is IND-CCA secure[19, 20]. Combining with a redundancy-free DEM it will yield a redundancy-free(MAC-free) IND-CCA secure hybrid encryption scheme. Although it is the same efficient as our new scheme the hybrid encryption scheme of Okamoto need a πPRF.

2 Definitions

In this section we describe the definitions of hybrid encryption scheme, DEM and DDH. 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 Hybrid Encryption Scheme

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

- HE.KeyGen(1^l): 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^l) and outputs a public key/secret key pair (PK,SK). We write (PK,SK) $\leftarrow$ HE.KeyGen(1^l).
- 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^l) 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:

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

   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 γ'.

We say the adversary succeeds if $\gamma' = \gamma$, 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.

2.2 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 $l \in N$, for all $k \in \{0,1\}^l$, here l denotes the length of the key of DEM, and for all $m \in \{0,1\}^*$,we have:

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

We recall the standard definition of security for data encapsulation mechanisms against adaptive chosen ciphertext attacks and passive attacks.

Definition 1. *A DEM scheme is secure against adaptive chosen ciphertext attacks if the advantage of any PPT adversary A in the following game is negligible in the security parameter k:*

1. The challenger randomly generates a key $k \in \{0,1\}^l$.
2. The adversary may make polynomial queries to a decryption oracle with ciphertext χ. The decryption oracle responds with DEM.Decrypt(k, χ).
3. At some point, A queries an encryption oracle with two messages m_0, m_1 , $|m_0| = |m_1|$. A bit γ is randomly chosen and the adversary is given a "challenge ciphertext" $\chi^* \leftarrow DEM.Encrypt(k, m_\gamma)$.
4. A may continue to query its decryption oracle except that it may not request the decryption of χ^*. The decryption oracle responds with DEM.Decrypt(k, χ).
5. Finally, A outputs a guess γ' .

We call the game above IND-CCA game. Define $AdvCCA_{DEM,A}(l)$ to be $|Pr[\gamma = \gamma'] - 1/2|$ in the above attack game. We say that DEM is secure against adaptive chosen ciphertext attack if for all probabilistic, polynomial-time oracle query machines A, the function $AdvCCA_{DEM,A}(l)$ grows negligibly in l.

2.3 Decisional Diffie-Hellman assumption

There are several equivalent formulations of the decisional Diffie-Hellman assumption. The one that we shall use is the following.

Let G be a group of large prime order q, and consider the following two distributions:

The distribution R of random quadruples $(g_1, g_2, u_1, u_2) \in G^4$

The distribution D of quadruples $(g_1, g_2, u_1, u_2) \in G^4$, where g_1, g_2 are random, and $u_1 = g_1^r, u_2 = g_2^r$ for random $r \in Z_q$.

An algorithm that solves the decision Diffie-Hellman problem is a statistical test that can effectively distinguish these two distributions. That is, given a quadruple coming from one of the two distributions, it should output 0 or 1, and there should be a non-negligible difference between (a) the probability that it output a 1 given an input from R, and (b) the probability that it output a 1 given an input from D. The decision Diffie-Hellman problem is hard if there is no such polynomial-time statistical test.

3 MAC-free variant of KD04

Our new scheme is very similar with KD04. Now we describe it as following:

- KeyGen: Assume that G is group of order q where q is a large prime number.

$$g_1 \overset{R}{\leftarrow} G; x, y, z \overset{R}{\leftarrow} Z_q^*; g_2 \leftarrow g_1^x; c \leftarrow g_1^y; d \leftarrow g_1^z$$

$$PK = (g_1, g_2, c, d, TCR, H, DEM); SK = (x, y, z)$$

  Where TCR is a target collision resistant hash function [10], $H : G \rightarrow \{0,1\}^l$ is a hash function, l is the length of the key, DEM is a IND-CCA secure data encapsulation mechanism.
- Encrypt: Given PK and m, the encryption algorithm runs as follows.

$$r \overset{R}{\leftarrow} Z_q^*; u_1 \leftarrow g_1^r; u_2 \leftarrow g_2^r; a \leftarrow TCR(u_1, u_2); k \leftarrow H(c^r d^{ra});$$

$$\psi \leftarrow (u_1, u_2); \chi \leftarrow DEM.Encrypt(k, m); C \leftarrow (\psi, \chi)$$

- Decrypt: Given a ciphertext $C = (u_1, u_2, \chi)$ and SK, the decryption algorithm runs as follows.

$$a \leftarrow TCR(u_1, u_2);$$

$$\text{if } (u_2 = u_1^x)\ k \leftarrow H(u_1^{y+az}); m \leftarrow DEM.Decrypt(k, \chi) \text{ return } m$$

$$\text{else return } \perp$$

Notice that if we use a IND-CCA secure MAC-DEM, m will be a rejecting symbol $\perp$ when the DEM part of the ciphertext is invalid. Now we prove that the hybrid encryption scheme above is secure against adaptive chosen ciphertext attacks:

Theorem 1. *The hybrid encryption scheme above is secure against adaptive chosen ciphertext attack assuming that (1)hash function TCR is chosen from target collision resistant hash function family (2) DDH problem is hard in the group G, (3) DEM is IND-CCA secure.*

To prove the theorem, we will assume that there is an adversary that can break the hybrid encryption scheme, and TCR is a target collision resistant hash function, DEM is a IND-CCA secure MAC-DEM and show how to use this adversary to construct a statistical test for the DDH problem. Then will show that in the real situation there will be no difference between MAC-DEM and redundancy-free DEMs.

For the statistical test, we are given (g_1, g_2, u_1, u_2) coming from either the distribution R or D. We will show that if the input comes from D, the simulation will be perfect, and so the adversary will have a non-negligible advantage in guessing the hidden bit b, 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 D run the simulator and adversary together, and if the simulator outputs γ and the adversary outputs γ', the distinguisher outputs 1 if $\gamma = \gamma'$, and 0 otherwise.

The input to the simulator is (g_1, g_2, u_1, u_2). The simulator runs the following key generation algorithm, using the given (g_1, g_2, u_1, u_2). The simulator chooses

$$x_1, x_2, y_1, y_2 \stackrel{R}{\leftarrow} Z_q^*$$

and sets

$$c \leftarrow g_1^{x_1} g_2^{x_2}; d \leftarrow g_1^{y_1} g_2^{y_2}$$

The simulator also chooses a target collision resistant hash function TCR, a hash function $H : G \rightarrow \{0,1\}^l$ and a IND-CCA secure MAC-DEM, where l is the length of the key. The public key that the adversary sees is $(g_1, g_2, c, d, H, TCR, DEM)$. The simulator knows (x_1, x_2, y_1, y_2).

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

$$a \leftarrow TCR(u_1, u_2), k \leftarrow H(u_1^{x_1+ay_1} u_2^{x_2+ay_2}), \chi \leftarrow DEM.Encrypt(k, m_\gamma)$$

and outputs: (u_1, u_2, χ)

We now describe the simulation of the decryption oracle. Given (u_{1i}, u_{2i}, χ_i), the simulator calculates:

$$a_i \leftarrow TCR(u_{1i}, u_{2i}), k_i \leftarrow H(u_{1i}^{x_1+a_i y_1} u_{2i}^{x_2+a_i y_2}); m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$$

The simulator returns m_i. If χ_i is invalid then m_i will be a rejecting symbol $\perp$.

That completes the description of the simulator. The theorem now follows immediately from the following two lemmas.

Lemma 1. *If the simulator's input comes from D, the joint distribution of the adversary's view and the hidden bit γ is the same as that in the actual attack.*

Consider the joint distribution of the adversary's view and the bit γ when the input comes from the distribution D, say $u_1 = g_1^r, u_2 = g_2^r$. First we show that the output of the encryption oracle has the right distribution:

$$u_1 = g_1^r; u_2 = g_2^r; a = TCR(u_1, u_2); k = H(u_1^{x_1+y_1 a} u_2^{x_2+y_2 a}) = H(c^r d^{ra})$$

We see that the output of the encryption oracle has the right distribution. Now we show that the output of the decryption oracle has the right distribution: Given $C_i = (u_{1i}, u_{2i}, \chi_i)$, we say the KEM part of C_i is valid if $u_{1i} = g_1^{r_i}, u_{2i} = g_2^{r_i}$, else if $u_{1i} = g_1^{r_i}, u_{2i} = g_2^{r_i'}, r_i \neq r_i'$ we say the KEM part of C_i is invalid. If the KEM part of C_i is valid we have:

$$a_i \leftarrow TCR(u_{1i}, u_{2i}), k_i \leftarrow H(u_{1i}^{x_1+a_i y_1} u_{2i}^{x_2+a_i y_2}) = H(g_1^{r_i(x_1+a_i y_1)} g_2^{r_i(x_2+a_i y_2)}) = H(c^{r_i} d^{a_i r_i})$$

It is clear that when the KEM part of C_i is valid the decryption oracle has the right distribution just the same as that in the actual attack. Now let's consider the case that the KEM part of C_i is invalid:

$$a_i \leftarrow TCR(u_{1i}, u_{2i}), k_i \leftarrow H(u_{1i}^{x_1+a_i y_1} u_{2i}^{x_2+a_i y_2}) = H(g_1^{r_i(x_1+a_i y_1)} g_2^{r_i'(x_2+a_i y_2)})$$

Let $log_{g_1} g_2 = w, \epsilon_i' = g_1^{r_i(x_1+a_i y_1)} g_2^{r_i'(x_2+a_i y_2)}$, consider the distribution of (x_1, x_2, y_1, y_2), we have:

$$\log_{g_1} c = x_1 + w x_2 \tag{1}$$

$$\log_{g_1} d = y_1 + w y_2 \tag{2}$$

$$\log_{g_1} \epsilon_i' = r_i(x_1 + a_i y_1) + r_i'(x_2 + a_i y_2) \tag{3}$$

It is clear that (1)(2) and (3) are linearly independent, therefore, the adversary can not get enough information to determine the distribution of (x_1, x_2, y_1, y_2) and can not denote (3) by (1) and (2) either. So $k_i = H(\epsilon_i')$ is independent from the adversary's view. Since DEM is a IND-CCA secure MAC-DEM[10, 11] the probability that the adversary construct a valid DEM part is negligible. So $m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$ will be a rejecting symbol $\perp$. Now we have that the decryption oracle will output a rejecting symbol $\perp$ just as in the actual attacks when the KEM part of C_i is valid.

So both the encryption oracle and the decryption oracle has the right distribution 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 γ is independent from the adversary's view.*

When the input comes from the distribution R, say $u_1 = g_1^r, u_2 = g_2^{r'}, r \neq r'$, The lemma follows immediately from the following two propositions.

Proposition 1. *If the decryption oracle reject all the ciphertext whose KEM part is invalid, then the distribution of the hidden bit γ is independent of the adversary's view.*

Consider the output of the encryption oracle:

$$a = TCR(u_1, u_2); k = H(u_1^{x_1+y_1 a} u_2^{x_2+y_2 a}) = H(g_1^{r(x_1+a_i y_1)} g_2^{r'(x_2+a_i y_2)})$$

Let $\epsilon = g_1^{r(x_1+a_i y_1)} g_2^{r'(x_2+a_i y_2)}$, consider the distribution of (x_1, x_2, y_1, y_2) we have:

$$\log_{g_1} \epsilon = r(x_1 + a_i y_1) + r'(x_2 + a_i y_2) \tag{4}$$

Consider the output of the decryption oracle when the KEM part of the ciphertext is valid, let $\epsilon_i = g_1^{r_i(x_1+a_i y_1)} g_2^{r_i(x_2+a_i y_2)}$, we have:

$$\log_{g_1} \epsilon_i = r_i(x_1 + a_i y_1) + r_i(x_2 + a_i y_2) \tag{5}$$

It is clear that (4) is linearly independent of (1)(2) and (5), therefore, the adversary can not get enough information to determine the distribution of (x_1, x_2, y_1, y_2) and can not denote (4) by (1) (2) and (5) either. So $k = H(\epsilon)$ is independent from the adversary's view. Since DEM is IND-CCA secure, we have that γ is independent from the adversary's view.

Proposition 2. *The decryption oracle will rejection all ciphertext whose KEM part is invalid except negligible probability.*

Now we show that the decryption oracle will rejection all ciphertext whose KEM part is invalid except negligible probability. There are two cases we need to consider:

Case 1: $(u_{1i}, u_{2i}) = (u_1, u_2), \chi \neq \chi_i$: In this case we have $k_i = k$ is independent from the adversary's view. Since DEM is a IND-CCA secure MAC-DEM, the probability that the adversary construct a valid DEM part is negligible. So $m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$ will be a rejecting symbol $\perp$ except negligible probability.

Case 2: $(u_{1i}, u_{2i}) \neq (u_1, u_2)$: Since TCR is a target collision resistant hash function we have that $a_i \neq a$. It is clear that (3) is linearly independent of (1) (2) (4) (5), therefore, the adversary can not get enough information to determine the distribution of (x_1, x_2, y_1, y_2) and can not denote (3) by (1) (2) (4) and (5) either. So $k_i = H(\epsilon_i')$ is independent from the adversary's view. Since DEM is a IND-CCA secure MAC-DEM the probability that the adversary construct a valid DEM part is negligible. So $m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$ will be a rejecting symbol $\perp$ except negligible probability.

Now we proved that when DEM is a IND-CCA secure MAC-DEM the new hybrid scheme above will be IND-CCA secure. Let's consider the difference between a MAC-DEM and a redundancy-free DEM in the real situation. If we use a MAC-DEM, $m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$ will be a rejecting symbol $\perp$ when the KEM part of the ciphertext(u_{1i}, u_{2i}) is invalid. Otherwise, if we use a redundancy-free DEM $m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$ will not be a rejecting symbol $\perp$ when the KEM part of the ciphertext(u_{1i}, u_{2i}) is invalid. That's the only difference between a MAC-DEM and a redundancy-free DEM from the KEM's view. We notice that in the real situation we have the whole private key (x, y, z) and can check if the KEM part of the ciphertext is valid or not. That's to say, when the KEM part of the ciphertext is invalid, the decryption oracle will output a rejecting symbol $\perp$ before execute $m_i \leftarrow DEM.Decrypt(k_i, \chi_i)$. It yield that there will be no difference between a MAC-DEM and redundancy-free DEM in the real situation. So we have that when DEM is a IND-CCA secure redundancy-free DEM the new hybrid scheme above will also be IND-CCA secure.

That's complete the proof of theorem 1.

4 Efficiency Analysis

The efficiency of the new scheme, KD04, Kiltz07 and Okamoto07 is listed in table 1.

Table 1. Efficiency comparison

	Encryption(exp)	Decryption(exp)	Cipher-text overhead(bit)	Assumption
KD04	3.5(2exp+1mexp)	1.5(0exp+1mexp)	$2\|q\| + \|t\|$	DDH
Kiltz07	3.5(2exp+1mexp)	1.5(0exp+1mexp)	$2\|q\|$	GHDH
Okamoto07	3.5(2exp+1mexp)	1.5(0exp+1mexp)	$2\|q\|$	DDH,πPRF
NEW	3.5(2exp+1mexp)	1.5(0exp+1mexp)	$2\|q\|$	DDH

In table1 NEW is the new hybrid encryption scheme when the underlying DEM is redundancy-free, KD04 is the scheme in [11], Kiltz07 is the hybrid encryption scheme from Kiltz07-KEM[18] and a redundancy-free IND-CCA secure DEM, Okamoto is the hybrid encryption scheme in [19, 20] when the underlying DEM is redundancy-free. 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 KD04.

It is clear that the new scheme is more efficient than KD04 in bandwidth. Compared to Kiltz07 and Okamoto07 the new scheme only need the DDH assumption, however Kiltz07 need the GHDH assumption, Okamoto07 need the DDH assumption and a πPRF.

5 Conclusion

We show a variant of KD04 which is IND-CCA secure when the the underlying DEM part is IND-CCA secure. We use a DEM built from one-time symmetric encryption scheme and a MAC in the security reduction to check if the KEM part of a ciphertext is valid. Then we show that there will be no difference between a MAC-DEM and a redundancy-free DEM in the real situation. So the hybrid encryption scheme can also use redundancy-free IND-CCA secure DEMs that avoid the overhead due to the MAC. When using redundancy-free IND-CCA secure DEMs, the new scheme will be more efficient than KD04 in bandwidth. Compared to Kiltz07 and Okamoto07 the new scheme only need the DDH assumption, however Kiltz07 need the GHDH assumption, Okamoto07 need the DDH assumption and a πPRF.

References

1. 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;
2. D. Dolev, C. Dwork, and M. Naor, "Non-Malleable Cryptography", *SIAM J. Computing* , 30(2): 391-437, 2000;
3. 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;
4. R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure Against Chosen Ciphertext Attack", *Adv. in Cryptology - Crypto 1998*, LNCS vol. 1462, Springer- Verlag , pp. 13-25, 1998;
5. 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.
6. 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.
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. International Organization for Standardization. ISO/IEC CD 18033- 2, Information technology – Security techniques – Encryption Algo- rithms – Part 2: Asymmetric Ciphers, 2003.
9. R. Cramer and V. Shoup, "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption", *Adv. in Cryptology - Eurocrypt 2002*, LNCS vol. 2332,Springer-Verlag, pp. 45-64, 2002;
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. K. Kurosawa and Y. Desmedt, "A New Paradigm of Hybrid Encryption Scheme", *Adv. in Cryp-tology - Crypto 2004, LNCS vol. 3152, Springer-Verlag*, pp. 426-442, 2004;
12. S. Halevi. EME*: Extending EME to handle arbitrary-length messages with associated data. In A. Canteaut and K. Viswanathan, editors, INDOCRYPT 2004, volume 3348 of LNCS, pages 315C327. Springer-Verlag, Berlin, Germany, Dec. 2004. 9
13. S. Halevi and P. Rogaway. A tweakable enciphering mode. In D. Boneh, editor, CRYPTO 2003, volume 2729 of LNCS, pages 482C499. Springer-Verlag, Berlin, Germany, Aug. 2003. 3, 9
14. S. Halevi and P. Rogaway. A parallelizable enciphering mode. In T. Okamoto, editor, CT- RSA 2004, volume 2964 of LNCS, pages 292C304. Springer-Verlag, Berlin, Germany, Feb. 2004. 3, 9

15. D. H. Phan and D. Pointcheval. About the security of ciphers (semantic security and pseudo- random permutations). In H. Handschuh and A. Hasan, editors, SAC 2004, volume 3357 of LNCS, pages 182C197. Springer-Verlag, Berlin, Germany, Aug. 2004. 3, 9
16. 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
17. 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.
18. Eike Kiltz. Chosen-Ciphertext Secure Key Encapsulation based on Hashed Gap Decisional Diffie-Hellman. Proceedings of the 10th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2007, pp. 282–297 LNCS 4450 (2007).Springer-Verlag. Full version available on Cryptology ePrint Archive: Report 2007/036
19. Tatsuaki Okamoto. Authenticated Key Exchange and Key Encapsulation in the Standard Model. Advances in Cryptology C ASIACRYPT 2007, pp. 474–484 LNCS 4833 (2007).Springer-Berlin / Heidelberg.
20. Tatsuaki Okamoto. Authenticated Key Exchange and Key Encapsulation Without Random Oracles. Cryptology ePrint Archive, Report 2007/473, 2007. http://eprint.iacr.org