Improved efficiency of Kiltz07-KEM

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. Kiltz proposed a practical key encapsulation mechanism(Kiltz07-KEM) which is secure against adaptive chosen ciphertext attacks(IND-CCA2) under the gap hashed Diffie-Hellman(GHDH) assumption[8]. We show a variant of Kiltz07-KEM which is more efficient than Kiltz07-KEM in encryption. The new scheme can be proved to be IND-CCA2 secure under the same assumption, GHDH.

Keywords: KEM, IND-CCA2, GHDH

1 Introduction

Security against adaptive chosen ciphertext attacks (IND-CCA2 security) [1–3] is now commonly accepted as the standard security notion for public key encryption schemes. Currently, most of the practical IND-CCA2 secure public key encryption schemes in standard model are variants of ElGamal[4] scheme. Cramer and Shoup[5, 6] proposed the first provably IND-CCA2 secure practical public key encryption scheme based on the decisional Diffie-Hellman(DDH) assumption in the standard model. This was further improved by Kurosawa and Desmedt and yield a more efficient scheme(KD04)[7]. Kiltz proposed a IND-CCA2 secure KEM(key encapsulation mechanism) under the Gap Hashed Diffie-Hellman(GHDH) assumption[8]. Combined with a redundancy-free DEM(data encapsulation mechanism) it will yield a IND-CCA2 secure hybrid encryption scheme more efficient than KD04.

1.1 Our Contributions

We show a variant of Kiltz07-KEM which can be proved to be IND-CCA2 secure under the same assumption, GHDH. The new scheme is similar to Kiltz07-KEM, while the only difference is that the second item of the ciphertext $u^{rt}v^r$ is replaced with $u^r v^{rt}$. Thus, the encryption of the new scheme only need three exponentiations. Compared with Kiltz07-KEM, the efficiency of the encryption is improved by 14.3%.

2 Definitions

In this section we describe the definitions of KEM, GHDH assumption and target collision resistant hash function. In describing probabilistic processes, we write $x \stackrel{R}{\leftarrow} X$ 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 $s \stackrel{R}{\leftarrow} S$ 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 $y \stackrel{R}{\leftarrow} A(x)$ 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:

$$b \stackrel{R}{\leftarrow} \{0,1\}; (K_0, \psi^*) \leftarrow \text{PKE.Encrypt(PK)}; K_1 \stackrel{R}{\leftarrow} K_D;$$

   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 Gap Hashed Diffie-Hellman Assumption

Now we review the definition of gap hashed Diffie-Hellman assumption[8]. Let G be a group of large prime order q, $H : G \rightarrow \{0,1\}^l$ be a cryptographic hash function and consider the following two experiment:

experiments $\text{Exp}^{ghdh}_{G,H,A}(l)$:

$$x, y \stackrel{R}{\leftarrow} Z_q^*; W_1 \leftarrow \{0,1\}^l; W_0 \leftarrow H(g^{xy}); b \stackrel{R}{\leftarrow} \{0,1\}$$

$$b' \leftarrow A^{\mathcal{O}_{ddh}()}(g^x, g^y, W_b); \text{If } b = b' \text{ return 1 else return 0;}$$

Here the oracle $\mathcal{O}_{ddh}(g, g^a, g^b, g^c)$ returns 1 if $ab = c$ otherwise return 0; We define the advantage of the A in violating the gap hashed Diffie-Hellman assumption as

$$Adv_{G,H,A}^{ghdh}(l) = |\Pr[\text{Exp}_{G,H,A}^{ghdh}(l) = 1] - 1/2|$$

We say that the GHDH assumption holds if $Adv_{G,H,A}^{ghdh}(l)$ is negligible for all polynomial-time adversaries A.

2.3 Target collision resistant hash function

A (t, ϵ) target collision resistant hash function (TCR) family is a collection $\mathcal{F}$ of functions $f_K : \{0,1\}^n \to \{0,1\}^m$ indexed by a key $K \in \mathcal{K}$ (where $\mathcal{K}$ denotes the key space), and such that any attack algorithm A running in time t has success probability at most ϵ in the following game:

- Key Sampling: A uniformly random key $K \in \mathcal{K}$ is chosen (but not yet revealed to A).
- A Commits: A runs (with no input) and outputs a hash function input $s_1 \in \{0,1\}^n$.
- Key Revealed: The key K is given to A.
- A Collides: A continues running and outputs a second hash function input $s_2 \in \{0,1\}^n$.

We say that A succeeds in the above game if it finds a valid collision for f_K, i.e. if $s_1 \neq s_2$ but $f_K(s_1) = f_K(s_2)$. We define the advantage of A as $AdvTCR = |Pr[f_K(s_1) = f_K(s_2) : s_1 \neq s_2] - 1/2|$. We say H is target collision resistant hash function if $AdvTCR$ is negligible.

3 Variant of Kiltz07-KEM

In this section we describe the new scheme as follow:

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

$$g \stackrel{R}{\leftarrow} G; x, y \stackrel{R}{\leftarrow} Z_q^*; u \leftarrow g^x; v \leftarrow g^y; PK = (g, u, v, H, TCR); SK = (x, y)$$

  Where $H : G \to \{0,1\}^l$ is the hash function used in the GHDH assumption, l is the length of the key, TCR is a target collision resistant hash function.
- Encrypt: Given PK, the encryption algorithm runs as follow:

$$r \stackrel{R}{\leftarrow} Z_q^*; c_1 \leftarrow g^r; t \leftarrow TCR(c_1); c_2 \leftarrow u^r v^{rt}; k \leftarrow H(u^r); \psi \leftarrow (c_1, c_2)$$

- Decrypt: Given a ciphertext $\psi = (c_1, c_2)$ and SK, the decryption algorithm runs as follow:

$$t \leftarrow TCR(c_1); \text{if } (c_2 = c_1^{x+yt})\ k \leftarrow H(c_1^x); \text{else return } \perp$$

Now we prove that the KEM above is secure against adaptive chosen ciphertext attacks:

Theorem 1. *The key encapsulation above is secure against adaptive chosen ciphertext attack assuming that: (1)GHDH problem is hard in the group G, (2)TCR is a target collision resistant hash function.*

To prove the theorem, we will assume that there is an adversary A that can break the hybrid encryption scheme above, TCR is a target collision resistant hash function and show how to use this adversary to construct an adversary B to break the GHDH problem.

Given (g, u, g^r, W), B runs the following key generation algorithm:

$$y \xleftarrow{R} Z_q^*; t \leftarrow TCR(g^r); v \leftarrow g^y u^{-1/t}$$

The public key that A sees is (g, u, v, TCR, H), $H : G \rightarrow \{0,1\}^l$ is the hash function used in the GHDH assumption, l is the length of the key, TCR is a target collision resistant hash function. B knows y.

First we describe the simulation of the encryption oracle. In step 3, B sends $(c_1 = g^r, c_2 = c_1^{yt}, k = W)$ to A. Since $c_2 = c_1^{yt} = g^{yrt} = u^r(g^y u^{-1/t})^{rt} = u^r v^{rt}$, we have that the simulation of the encryption oracle is perfect.

We now describe the simulation of the decryption oracle. Given (c_{1i}, c_{2i}), B works as follow:

$$t_i \leftarrow TCR(u_{1i}); \text{if } \mathcal{O}_d dh(g, uv^{t_i}, c_{1i}, c_{2i}) = 1 \ k \leftarrow H((c_{2i}/(c_{1i}^{yt_i}))^{t/(t-t_i)}); \text{else return } \perp$$

Let $c_{1i} = g^{r_i}$, if $\mathcal{O}_d dh(g, uv^{t_i}, c_{1i}, c_{2i}) = 1$ we have that $c_{2i} = u^{r_i} v^{r_i t_i}$. Consider k:

$$k = H((c_{2i}/(c_{1i}^{yt_i}))^{t/(t-t_i)}) = H((u^{r_i} v^{r_i t_i}/(g^{r_i y t_i}))^{t/(t-t_i)})$$

$$= H((u^{r_i}(g^y u^{-1/t})^{r_i t_i}/(g^{r_i y t_i}))^{t/(t-t_i)}) = H((u^{r_i((t-t_i)/t)})^{t/(t-t_i)}) = H(u^{r_i})$$

It is clear that the simulation of the decryption oracle is perfect. Finally, when A return b', B also output b'. Let $u = g^x$, if $b' = 0$ it means that $k = W = H(g^{xr})$. So, if A breaks the scheme successfully, then B breaks the GHDH problem successfully. That's complete the proof of theorem 1.

4 Efficiency Analysis

The efficiency of the new scheme and Kiltz07-KEM is listed in table 1.

Table 1. Efficiency comparison

schemes	Encryption(exp)	Decryption(exp)	Cipher-text overhead(bit)	Assumption
Kiltz07-KEM	3.5(2exp+1mexp)	1.5(0exp+1mexp)	$2\|q\|$	GHDH
NEW	3 (3exp+0mexp)	1.5(0exp+1mexp)	$2\|q\|$	GHDH

When tabulating computational efficiency hash function is 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. It is clear that the encryption of the new scheme is about 14.3% faster than that of Kiltz07-KEM.

5 Conclusion

We showed a variant of Kiltz07-KEM. The new scheme is similar to Kiltz07-KEM, while the only difference is that the second item of the ciphertext $u^{rt}v^r$ is replaced with $u^r v^{rt}$. Thus, the efficiency of the encryption is improved by 14.3%.

References

1. 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;
2. 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;
3. D. Dolev, C. Dwork, and M. Naor, Non-Malleable Cryptography, SIAM J. Computing, 30(2): 391-437, 2000;
4. T. ElGamal. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31:469C472, 1985.
5. 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;
6. 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.
7. K. Kurosawa and Y. Desmedt, A New Paradigm of Hybrid Encryption Scheme, Adv. in Cryptology - Crypto 2004, LNCS vol. 3152, Springer-Verlag, pp. 426-442, 2004;
8. 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