Revisit of CS98

Xianhui Lu[1], Xuejia Lai[2], Dake He[1], Guomin Li [1]
Email:lu_xianhui@sohu.com
1:School of Information Science & Technology, SWJTU, Chengdu, China
2:Dept. of Computer Science and Engineering, SJTU, Shanghai, China

May 21, 2007

Abstract

Cramer and Shoup proposed the first provably secure practical public-key encryption scheme in the standard model (CS98). We find new way to construct the secure reduction in which the decryption oracle is not needed yet. Thus we get a simplified version of CS98 which is more efficient than the original scheme, and also provably secure against chosen ciphertext attack in standard model.

Keywords: PKE, CCA, standard model

1 Introduction

Security against adaptive chosen cipher-text attacks (CCA secure) [2, 3, 4] is a strong and very useful notion of security for public-key encryption schemes. This notion is known to suffice for many applications of encryption in the presence of active attackers, including secure communication, auctions, voting schemes, and many others. CCA secure is commonly accepted as the security notion of choice for encryption schemes that are to be plugged in to a protocol running in an arbitrary setting [5, 6]. The random oracle model is a useful tool in constructing CCA secure public-key encryption schemes, but it does not rule out all possible attacks [7]. Schemes that can be proven to be CCA-secure in the standard model (without the use of heuristics such as random oracles) is more practical. Cramer and Shoup showed the first provably secure practical public-key encryption scheme in the standard model [1](CS98). It is CCA secure under the Decisional Diffie-Hellman(DDH) assumption. They further generalized their scheme to projective hash families [8]. Shoup presented a hybrid encryption scheme [9] which using [1] as a key encapsulation mechanism. In [11], Kurosawa and Desmedt introduced a hybrid encryption scheme which is a modification of the hybrid scheme presented in [9].

1.1 Our Contributions

We can prove that CS98 is secure in a different way. And we find that u_2 is not needed in our new secure reduction. So we get a simplified version of CS98. The simplified version of CS98 is more efficient than the original scheme, and also provably secure against chosen ciphertext attack in standard model.The proof of the security of the simplified scheme is different from that of Cramer

and Shoup [1, 10]. We first transit the IND-CCA2 game into a IND-CPA game. Finally it does not need to answer the decryption oracle queries in the following transitions.

2 Preliminaries

We first review CS98 . This is followed by the definition of DDH.

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 in put 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.

We write

$$Pr[x_1 \stackrel{R}{\leftarrow} X_1, x_2 \stackrel{R}{\leftarrow} X_2, \ldots, x_n \stackrel{R}{\leftarrow} X_n : \phi(x_1, \ldots, x_n)]$$

to denote the probability that when x_1 is drawn from a certain distribution X_1, and x_2 is drawn from a certain distribution $X_2(x_1)$, possibly depending on the particular choice of x_1, and so on, all the way to x_n, the predicate $\phi(x_1, ..., x_n)$ is true. We allow the predicate ϕ to involve the execution of probabilistic algorithms.

2.1 The CS98 scheme

We describe CS98 as follow:

- $\mathcal{G}(1^k)$: Assume that G is group of order q where q is large.

$$g_1, g_2 \stackrel{R}{\leftarrow} G; x_1, x_2, y_1, y_2, z \stackrel{R}{\leftarrow} Z_q; H \stackrel{R}{\leftarrow} TCR$$

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

$$PK = (g, h, c, d, H); SK = (x_1, x_2, y_1, y_2, z)$$

  Where TCR is target collision resistant hash function [10].

- $\mathcal{E}_{PK}(m)$: Given a message $m \in G$, the encryption algorithm runs as follows.

$$r \stackrel{R}{\leftarrow} Z_q$$

$$u_1 \leftarrow g_1^r; u_2 \leftarrow g_2^r; e \leftarrow h^r m; a \leftarrow H(u_1, u_2, e); v \leftarrow c^r d^{ra}$$

$$C \leftarrow (u_1, u_2, e, v)$$

- $\mathcal{D}_{SK}(C)$: Given a cipher-text $\mathcal{C} = (u, e, v)$, the decryption algorithm runs as follows.

$$a \leftarrow H(u_1, u_2, e); m \leftarrow e/u^z$$

$$if v = u_1^{x_1 + y_1 a} u_2^{x_2 + y_2 a} \ return \ m \ else \ return \ \perp$$

2.2 The Decision Diffie-Hellman Problem

There are several equivalent formulations of the decision Diffie-Hellman problem. 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 A simplified version of CS98

CS98 is the first practical public key encryption scheme that provably secure against chosen ciphertext attack in standard model. We find a simplification of CS98 which is also provably secure against chosen ciphertext attack in standard model. The simplified version of CS98 is described as bellow:

- $\mathcal{G}(1^k)$: Assume that G is group of order q where q is large.

$$g \xleftarrow{R} G; x, y, z \xleftarrow{R} Z_q; H \xleftarrow{R} TCR$$

$$c \leftarrow g^x; d \leftarrow g^y; h \leftarrow g^z$$

$$PK = (g, h, c, d, H); SK = (x, y, z)$$

  Where TCR is target collision resistant hash function [10].

- $\mathcal{E}_{PK}(m)$: Given a message $m \in G$, the encryption algorithm runs as follows.

$$r \xleftarrow{R} Z_q$$

$$u \leftarrow g^r; e \leftarrow h^r m; a \leftarrow H(u, h^r, m); v \leftarrow c^r d^{ra}$$

$$C \leftarrow (u, e, v)$$

- $\mathcal{D}_{SK}(C)$: Given a cipher-text $\mathcal{C} = (u, e, v)$, the decryption algorithm runs as follows.

$$m \leftarrow e/u^z; a \leftarrow H(u, u^z, m);$$

$$if v = u^{x+ya} \ return \ m \ else \ return \ \perp$$

Remark: The proof of the security of the new scheme is different from that of Cramer and Shoup [10]. We first transit the IND-CCA2 game into a IND-CPA game. And then it does not need to answer the decryption oracle queries when transiting from Game2 to Game3.

Now we prove that the simplified CS98 is secure against chosen cipher-text attack in standard model:

Theorem 1 *The simplified CS98 is secure against adaptive chosen cipher-text attack assuming that (1) the decision Diffie-Hellman problem is hard in group G, (2) H is a target collision resistant hash function[1].*

Let game G_0 be the original attack game, let $b' \in \{0,1\}$ denote the output of A, and let T_0 be the event that $b = b'$ in G_0, so that $AdvCCA_A = |Pr[T_0] - 1/2|$.

We will define a sequence $G_1, G_2, \ldots, G_l$ of modified attack games. Each of the games operates on the same underlying probability space. In particular, the public key and secret key of the cryptosystem, the coin tosses $Coins$ of A, and the hidden bit b take on identical values across all games. For any $1 \leq i \leq l$, we let T_i be the event that $b = b'$ in game G_i.

Game G_0

1. The key generation oracle work as follow:

   I1: $g \stackrel{R}{\leftarrow} G; x, y, z \stackrel{R}{\leftarrow} Z_q; H \stackrel{R}{\leftarrow} TCR$

   I2: $PK \leftarrow (g, h, c, d, H); SK \leftarrow (x, y, z)$

   Finally PK is given to A.

2. A make a sequence of calls to the decryption oracle with $C_1 \cdots C_{Q_{A1}}$. The decryption oracle computes:

   D1: $m_i \leftarrow e_i / u_i^{z_i}$

   D2: $a_i \leftarrow H(u_i, u_i^{z_i}, m_i)$

   D3: If $v_i = u_i^{x+ya_i}$ responds m to A; else responds $\perp$.

3. At some point, A makes a call to the encryption oracle:

   E1: $M_0, M_1 \leftarrow A(Coins, PK, \vec{C_1}, \vec{m_1})$

   E2: $b \stackrel{R}{\leftarrow} \{0,1\}$

   E3: $r^* \stackrel{R}{\leftarrow} Z_q$

   E4: $u^* \leftarrow g^{r^*}$

   E5: $e^* \leftarrow h^{r^*} M_b$

   E6: $a^* \leftarrow H(u^*, h^{r^*}, M_b)$

   E7: $v^* \leftarrow c^{r^*} d^{r^* a^*}$

   E8: $C^* \leftarrow (u^*, e^*, v^*)$

   where $\vec{C_1} = (C_1, \cdots, C_{Q_{A1}}), \vec{m_1} = (m_1, \cdots, m_{Q_{A1}})$

4. A may continue to query its decryption oracle with $C_{Q_{A1}+1}, \cdots, C_{Q_{A1}+Q_{A2}}$ except that it may not request the decryption of C^*. The decryption oracle works as step 2.

5. Finally, A outputs a guess b'.
   $b' \leftarrow A(Coins, PK, \vec{C}, \vec{m}, C^*, M_0, M_1)$
   where $\vec{C} = (C_1, \cdots, C_{Q_{A2}+Q_{A1}}), \vec{m} = (m_1, \cdots, m_{Q_{A2}+Q_{A1}})$

Game G_1 We remove the decryption oracle in game G_0(step 2 and step 4) to obtain a new game G_1. Let R_1 be the event that $v_i = c^{r_i} d^{r_i a_i}$ and A does not know m_i. This is the only way A can get help from the simulator. When A knows m_i the decryption oracle will not help him. When $v_i \neq c^{r_i} d^{r_i a_i}$ the simulator will response $\perp$, that's a response A knows when he try to forge a ciphertext. There are three cases we consider when R_1 happens:

Case1: In step2, $1 \leq i \leq Q_{A1}$. Since A does not know m_i, he can not calculate $a_i \leftarrow H(u_i, u_i^{z_i}, m_i)$. The value of $c^{r_i} d^{r_i a_i}$ is uniform over G from A's view. So the probability of this case happens is $1/q$.

Case2: In step4,$(u_i, e_i) \neq (u^*, e^*), a_i = a^*$: This case is just a target collision attack on H. So the probability of this case happens is $AdvTCR$. Where $AdvTCR$ is the advantage of attack on target collision resistant hash function, see [10] for detail.

Case3: In step4,$(u_i, e_i) \neq (u^*, e^*), a_i \neq a^*$, Since A does not know m_i, there are two cases we need to consider:

   (a) A construct a ciphertext C_i without the help of C^*. This is the same as Case1. So the probability of this case happens is $1/q$.

   (b) A construct a ciphertext C_i with the help of C^*. We have:

$$\log_g v^* = (x + ya^*)r^*$$

$$\log_g v_i = (x + ya_i)r_i$$

   Since $a_i \neq a^*$, the two equations above are linear independent to each other. A can not get v_i from v^*. So the probability of this case happens is also $1/q$.

Now we get the probability of R_1:

$$Pr[R_1] \leq AdvTCR + Q_A/q$$

Where $Q_A = Q_{A1} + Q_{A2}$

Let's consider $\neg R_1$. If $v_i \neq c^{r_i} d^{r_i a_i}$ the decryption oracle will return $\perp$ to A. Now we see that when $\neg R_1$ happens, the decryption will not leak more information to A than he knows. And we have that:

$$Pr[T_0] = Pr[b = b' : b' \leftarrow A(Coins, PK, \vec{C}, \vec{m}, C^*, M_0, M_1)]$$

$$Pr[T_1] = Pr[b = b' : b' \leftarrow A(Coins, PK, C^*, M_0, M_1)]$$
$$Pr[T_0 \wedge \neg R_1] = Pr[b = b' : b' \leftarrow A(Coins, PK, C^*, M_0, M_1)] = Pr[T_1 \wedge \neg R_1]$$

According to [12] $lemma1$ we have:

$$|Pr[T_1] - Pr[T_0]| = Pr[R_1] \leq AdvTCR + Q_A/q \tag{1}$$

Game G_2 We modify the encryption oracle in game G_1 to obtain a new game G_2. Instead of using the original encryption algorithm, we modify the encryption algorithm, replacing step$E5$ with:

E5': $e^* \leftarrow g^{r^* x} M_b$

The change we have made is purely conceptual: the value of e^* is exactly the same in game $G2$ and $G1$. Therefore,

$$Pr[T_2] = Pr[T_1] \tag{2}$$

Game G_3 We modify the encryption oracle in game G_2 to obtain a new game G_3. Instead of using the original encryption algorithm, we modify the encryption algorithm, replacing step$E5'$ with:

E5": $r^+ \stackrel{R}{\leftarrow} Z_q; e^* \leftarrow g^{r^+} M_b$

Observe that, games $G2$ and $G3$ are the same except that in game $G2$, the quadruple $(g, h, u^*, g^{r^* z})$ is uniformly distributed in D, and in game $G3$, the quadruple (g, h, u^*, g^{r^+}) is uniformly distributed in R. Thus, any difference in behavior between these two games immediately yields a statistical test for distinguishing Diffie-Hellman quadruples from random quadruples. More precisely, we have

$$|Pr[T_3] - Pr[T_2]| \leq AdvDDH \tag{3}$$

To complete the proof, we need to argue that b' is independent of b. First observe that by construction, b is independent of $Conins, PK$. In the changed encryption oracle:

$$r^* \stackrel{R}{\leftarrow} Z_q; u^* \leftarrow g^{r^*}$$
$$r^+ \stackrel{R}{\leftarrow} Z_q; e^* \leftarrow g^{r^+} M_b;$$
$$a^* \leftarrow H(u^*, e^*, M_b); v^* \leftarrow c^{r^*} d^{r^* a^*}$$
$$C^* \leftarrow (u^*, e^*, v^*)$$

So we get that b is independent to $C^* = (u^*, e^*, v^*)$. Now we have that b is independent to $b' \leftarrow A(Coins, PK, C^*, M_0, M_1)$. Since $Pr[T_2] = Pr[b = b' : b' \leftarrow A(Coins, PK, C^*, M_0, M_1)]$, we have:

$$|Pr[T_3] - 1/2| = 0 \tag{4}$$

From $(1), (2), (3)$ we have

$$AdvCCA_A = |Pr[T_0] - 1/2| \leq AdvDDH + AdvTCR + Q_A/q \tag{5}$$

Now we've proved theorem 1.

4 Efficiency Analysis

The efficiency of our simplified schemes and CS98 is listed in table 1.

Table 1: Efficiency comparison

	Encryption(exp)	Decryption(exp)	Cipher-text overhead(bit)
CS98	4.5(3exp+1mexp)	2.5(1exp+1mexp)	$3\|q\|$
SCS98	3.5(2exp)	2.5(1exp+1mexp)	$2\|q\|$

Where SCS98 is the simplified CS98. When tabulating computational efficiency hash function and block cipher evaluations are ignored, multi-exponentiation (*mexp*) is counted as 1.5 exponentiations (*exp*). Cipher-text overhead represents the difference between the cipher-text length and the message length, and $|q|$ is the length of a group element. It is clear that the simplified scheme is efficient than the original scheme in both computation and ciphertext overhead.

5 Conclusion

Our new secure reduction is different from that of Cramer and Shoup [1, 10]. We first transit the adaptive chosen ciphertext attack game into a chosen plaintext attack game. And then it does not need to answer the decryption oracle queries in the following transitions. Finally we can get a simplified version of CS98.

References

[1] 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;

[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] 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;

[5] V. Shoup, "Why Chosen Ciphertext Security Matters", *IBM Research Report RZ 3076*, November , 1998. Available at http://www.shoup.net/papers;

[6] V. Shoup, "A Proposal for an ISO Standard for Public Key Encryption (version 2.1)", December, 2001. Available at http://www.shoup.net/papers;

[7] R. Canetti, O. Goldreich, and S. Halevi, "The Random Oracle Methodology Revisited" *30thACM Symp. on Theory of Computing (STOC), ACM*, pp. 209-218, 1998;

[8] 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;

[9] 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.

[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 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.

[12] 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/