基于Waters的ID加密的高效选择密文安全公钥密码体制

梅其祥[①②③] 何大可[①] 郑 宇[①]
[①](西南交通大学计算机与通信工程学院 成都 610031)
[②](中国科学院研究生院信息安全国家重点实验室 北京 100039)
[③](中南大学信息工程学院 长沙 410075)

摘 要 2004年的欧密会上，Canetti, Halevi和Katz提出了将Selective-ID安全的基于身份加密方案转化为选择密文安全(即, CCA安全)的公钥加密方案的方法。但由于该方法需要用到一次性签名，给所基于的方案增加了明显的通信和计算负载。该文由Waters提出的Adaptive-ID安全的基于身份加密(IDE)方案构造了一个新的CCA安全公钥加密方案。这里的“身份”由前两部分密文的hash值得到，密文合法性由双线性映射来验证。其效率比直接利用CHK的一般转化得到方案有明显提高。新方案的安全性在标准的决定性双线性Diffie-Hellman假设下被证明。

关键词 加密，选择密文安全性，基于身份加密，决定性双线性Diffie-Hellman问题
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1009-5896(2006)06-1141-04

Efficient Chosen Ciphertext Secure Public Key Cryptosystem from the ID-Based Encryption of Waters

Mei Qi-xiang[①②③] He Da-ke[①] ZhengYu[①]
[①](*School of Computer Science and Communication Engineering, Southwest Jiaotong University, Chengdu* 610031,*China*)
[②](*State Key Laboratory of Information Security , Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)
[③](*School of Information Science and Engineering, Central South University , Changsha* 410075, *China*)

Abstract In Eurocrypt 2004, Canetti, Halevi and Katz proposed a method for constructing Chosen Ciphertext secure (ie., CCA secure) public key encryption from any Selective-ID secure ID-Based Encryption (IBE). However, this method needs one time signature and thus adds noticeable overhead to the underling scheme. In this paper, a new CCA secure public key cryptosystem is constructed from the Adaptive-ID secure IBE scheme proposed by Waters. Here, the “identity” is the hash of the first two parts of the ciphertext, and the bilinear map is used to test the ciphertext validity. The proposal is much more efficient than those obtained from the general CHK method. The security of the new scheme is proved under the standard Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Key words Encryption, Chosen ciphertext security, ID-Based Encryption(IBE), Decisional bilinear Diffie-Hellman problem

1 引言

选择密文安全性[1](Chosen Ciphertext security, 即CCA-security)[1)]是公钥密码中很强的安全性概念，这个概念对存在主动攻击的许多加密应用中都是充分的。构造CCA安全的公钥密码体制具有重要的意义，如Bellare 和Rogaway提出的OAEP体制[2]就成为SET协议的加密标准。

长期以来，只有很少的加密方案能在标准模型中被证明是抗选择密文攻击的，而实用的方案更少。第一个实用的方案由Cramer和Shoup 1998年[3]提出，他们后来把该方案的构造方法推广成平滑hash证明系统[4](Smooth Hash Proof Systems，SHPS)。长时间以来，利用SHPS是构造标准模型中实际可行的CCA方案的唯一方法。2004年，Canetti, Halevi和Katz[5]提出将任意Selective-ID 安全[6]的基于身份加密(ID-Based Encryption，IBE)方案[6,7]转化为CCA安全公钥加密方案的一般方法。为了加密 m，加密者利用接收者的公钥PK，产生一次性签名密钥对(vk,sk)，将密文 $(vk, \mathrm{Enc}_{\mathrm{PK}}(\mathrm{vk}, m), \sigma)$ 发送到接收者，其中 $Enc_{\mathrm{PK}}(\mathrm{vk}, m)$ 可以看作是对 m 以PK为主公开参数和vk为身份的加密，σ 表

2004-11-08 收到, 2005-06-30 改回
国防科技重点实验室资助项目(51436050404QT2202)和信息安全国家重点实验室2004年第1批开放课题(01-01)资助课题

1)之所以称为CCA安全性是因为该概念的完整意思是在选择密文攻击下是安全(或者翻译为抗选择密文攻击)的(secure against Chosen Ciphertext Attacks)。而一般的文献中直接称该安全性为选择密文安全性(Chosen Ciphertext security)，并特别说明该概念是指CCA 安全性。

示以用私钥 sk 对前两个部分密文的签名，解密时，先验证签名的合法性，若合法，再利用“主” 密钥提取“身份” vk 的私钥 d_{vk}，并用 d_{vk} 进行解密。可以看出，该方案相应于原来的IBE方案有明显的通信和计算负载，因为加密时，需要产生一次性签名的密钥对，以及用所产生的私密钥对IBE的密文进行签名，解密时还要先验证签名的合法性，再进行解密。

我们构造了一个新的CCA方案，安全性基于标准的决定性双线性Diffie-Hellman (Decisional Bilinear Diffie-Hellman, DBDH)假设。该方案由转化最近Waters提出[8]的高效的Adaptive-ID 安全的IBE方案[8,9]而得到。相应于所基于的IBE方案，该方案没有任何密文扩展，加密计算量相同，只有解密多了一次pairing运算。我们能实现这种极低负载是因为Waters方案是Adaptive-ID安全的，即攻击者可以是适应性地选择身份攻击，但Canetti , Halevi和Katz转化的是Selective-ID安全的，即攻击者在只能非适应性地选择身份(所攻击的身份在参数产生之前就已决定)攻击。由于Waters的Adaptive-ID安全IBE方案和基于同样假设的目前最好的Selective-ID 安全IBE方案的效率非常接近，所以我们所得到方案与利用Canetti等的一般转化得到的同样假设的方案相比，效率有明显的提高。这也说明了Adaptive-ID 安全IBE方案的转化有其自身特点，直接用Selective-ID 安全IBE方案对转化方法来转化Adaptive-ID安全IBE方案不是最优的。

2 预备知识

2.1 选择密文安全性(Chosen Ciphertext security, 即CCA-security)[1]

在下面的游戏中，攻击者获得的优势可以忽略: (1)挑战者执行参数产生算法和密钥产生算法，并将公共参数Param、加密公钥 PK 给攻击者A；(2) 攻击者A用若干个密文询问解密预言机，挑战者按照解密算法进行解密，并将解密结果给攻击者A；(3) 攻击者A选出两个等长消息 m_0 和 m_1，挑战者随机地选取一个比特值 γ，并对 m_γ 进行加密形成挑战密文 $C^* = E_{\mathrm{PK}}(m_\gamma)$ 给攻击者；(4) 攻击者A可以继续选择密文询问解密预言机，唯一的限制是不能用挑战密文 C^* 本身进行询问；(5) 最后，攻击者A输出一个猜测 γ'。当 $\gamma' = \gamma$ 时，称攻击者A获得成功，并用 $\mathrm{Pr}_{\mathrm{A,PKE}}(\mathrm{Succ})$ 表示该事件成功的概率。攻击者的优势定义为 $|\mathrm{Pr}_{\mathrm{A,PKE}}(\mathrm{Succ}) - 1/2|$。

2.2 双线性映射

设 G 和 G_1 为阶次为大素数 p 的循环群，g 为 G 上随机的生成元，双线性映射 $e: G \times G \to G_1$ 是表示具有如下性质的映射：

(1)双线性 对于所有的 $u,v \in G$，$a,b \in Z_p$，都有 $e(u^a, v^b) = e(u,v)^{ab}$，如 $e(u^2, v^3) = e(u,v)^6$。

(2)不退化性 $e(g,g) \neq 1$。如果 G 上的群操作可以有效地计算，并且存在群 G_1 和有效计算的双线性映射 $e: G \times G \to G_1$，则称 G 为双线性群(参见文献[6,7])。

2.3 决定性双线性Diffie-Hellman假设[7]

设 G 和 G_1 为阶次为大素数 p 的循环群，g 为 G 上随机的生成元，且存在由 G 到 G_1 中的双线性映射 $e: G \times G \to G_1$。对于随机选取的 $a,b,c,z \in Z_p$，多项式时间攻击者被给定 $(g, A = g^a, B = g^b, C = g^c, Z)$，它猜中 $Z = e(g,g)^{abc}$ 还是 $Z = e(g,g)^z$ 的概率偏离 0.5 的优势可以忽略。

3 方案描述

参数产生 设 G 和 G_1 为阶次为大素数 p 的循环群，g 为 G 上随机的生成元，且存在由 G 到 G_1 中的双线性映射 $e: G \times G \to G_1$。假设存在免碰撞hash函数 $H: G_1 \times G \to \{0,1\}^n$。设 g_2，u'，$u_1, u_2, \cdots, u_n$ 为在 G 中随机选取的若干元素。公共参数为 $G, G_1, g, g_2, u', u_1, u_2, \cdots, u_n$，$H$，$e$。

密钥生成 随机选取 $a \in Z_p$，计算 $g_1 = g^a$，$h = g_2^a$，保密私钥 h，公开公钥 g_1。

加密 为了给公钥为 g_1 的用户发送消息 M，发送者随机选取 $t \in Z_p$，计算 $c_1 = e(g_1, g_2)^t M$，$c_2 = g^t$，$V = H(c_1, c_2)$，$c_3 = \left(u' \prod_{i \in \langle V \rangle} u_i^t \right)$，密文为 $C = (c_1, c_2, c_3)$，($\langle V \rangle \subseteq \{0,1,\cdots,n\}$ 表示所有 $v_i = 1$ 的 i 的集合，而 v_i 是 V 的第 i 个比特)。

解密 公钥为 g_1 的用户收到密文 $C = (c_1, c_2, c_3)$ 后，首先计算 $V = H(c_1, c_2)$；验证等式 $e\left(c_2, \left(u' \prod_{i \in \langle V \rangle} u_i\right)\right) = e(g, c_3)$ 是否成立，若成立，则计算 $M = c_1 / e(c_2, h)$，并输出 M；否则输出“reject”表示密文不合法。

4 效率分析

该方案的主要负载是由于解密时需要验证密文的合法性，验证需要 2 次pairing运算，解密总共需 3 次pairing运算。而所基于的IBE方案解密只需两次pairing运算。但是相对于Canetti等的一般转化仍然有计算优势，因为若为了缩短密文长度，他们的一次性签名用短签名[10]，目前最好的标准模型中短签名需要计算一次pairing来进行验证，而该短签名所基于的假设已经更强，即强-Diffie-Hellman假设，而且此时的密文扩展为 $4|p|$ ($2|p|$ 为一次性签名验证公钥，$2|p|$ 为签名)，而由Waters方案派生出来的短签名则需要 2 次pairing运算进行验证。相应于所基于的IBE方案，本文方案没有密文扩展。

5 安全性分析

定理 在决定性双线性 Diffie-Hellman 假设下，本方案可以抗适应性选择密文攻击。

证明 假设存在一个攻击者 A 可以对本方案进行选择密文攻击，我们将证明存在攻击者 B，可以解决决定性双线

性 Diffie-Hellman 问题，从而导致矛盾。B 被给定 $g, A=g^a$，$B=g^b, C=g^c, Z$，他的目标是借助于 A 来以不可忽略的优势猜中 $Z=e(g,g)^{abc}$ 还是 $Z=e(g,g)^z$，为此，它需模仿解密 Oracle, 应答 A 的解密询问。

B 按照 Waters 方案中的模仿者的方法，选取 m，$X=(x_i)$，$Y=(y_i)$，取 $g_1=A$，$g_2=B$，$u'=g_2^{p-km+x'}g^{y'}$，$u_i=g_2^{x_i}g^{y_i}$。

定义　$F(V)=(p-mk)+x'+\sum_{i\in\langle V\rangle}x_i$；　$J(V)=y'+\sum_{i\in\langle V\rangle}y_i$

$$K(V)=\begin{cases}0, & \text{if}\quad x'+\sum_{i\in\langle V\rangle}x_i\equiv 0 \bmod m\\ 1, & \text{其它}\end{cases}$$

当攻击者 A 用密文 $C=(c_1,c_2,c_3)$ 询问解密预言机时，B 计算“身份” $V=H(c_1,c_2)$，验证等式 $e\left(c_2,\left(u'\prod_{i\in\langle V\rangle}u_i\right)\right)=e(g,c_3)$ 是否成立，若不成立，输出“reject”表示密文不合法；否则，按照 Waters 方案中的私钥提取模仿算法模仿关于“身份” V 的私钥 $d=(d_1,d_2)$：如果 $K(V)=0$，则停止，随机输出 β'；否则，随机选取 $r\in Z_p$，计算 $d_1=g_1^{\frac{-J(V)}{F(V)}}\left(u'\prod_{i\in\langle V\rangle}u_i^r\right)$，$d_2=g_1^{\frac{-1}{F(V)}}\cdot g^r$ 关于“身份” V 私钥为 $d=(d_1,d_2)$。设 $\bar r=r-a/(F(V))$，则 $d_1=g_2^a\left(u'\prod_{i\in\langle V\rangle}u_i\right)^{\bar r}$，$d_2=g^{\bar r}$，即当 $K(V)=0$ 时，B 可以模仿关于“身份” $V=H(c_1,c_2)$ 的私钥 $d=(d_1,d_2)$，再利用 $d_V=(d_1,d_2)$ 进行解密：$M=c_1\frac{e(d_2,c_3)}{e(d_1,c_2)}$，并将 M 给 A。

由于

$$\begin{aligned}&c_1\cdot e(c_3,d_2)/e(c_2,d_1)\\&=e(g_1,g_2)^sM\cdot e\left(\left(u'\prod_{i\in\langle ID\rangle}u_i\right)^s,g^r\right)\Big/e\left(g^s,g_2^a\left(u'\prod_{i\in\langle ID\rangle}u_i\right)^r\right)\\&=e(g_1,g_2)^sMe\left(\left(u'\prod_{i\in\langle ID\rangle}u_i\right)^s,g^r\right)\Big/\left(e\left(g^s,g_2^a\right)e\left(g^s,\left(u'\prod_{i\in\langle ID\rangle}u_i\right)^r\right)\right)\\&=e(g_1,g_2)^sMe\left(u'\prod_{i\in\langle ID\rangle}u_i,g\right)^{rs}\Big/\left(e\left(g^a,g_2\right)^se\left(g,u'\prod_{i\in\langle ID\rangle}u_i\right)^{rs}\right)=M\end{aligned}$$

所以，A 从 B 得到的解密明文与从真正解密者得到的解密明文是一致的。

当 A 选出两个等长明文 m_0 和 m_1 后，B 按照 Waters 方案中的模仿方法，进行挑战密文的模仿，只是“身份” $V'=H(c_1',c_2')$ 是在加密中形成的：随机取 $\gamma\in\{0,1\}$，先建立部分挑战密文 $(c_1',c_2')=(Zm_\gamma,C)$，计算“身份” $V'=H(c_1',c_2')$，当 $x'+\sum_{i\in\langle V'\rangle}x_i\neq km$ 时，B 停止，随机输出 β'；否则，建立完全挑战密文 $T=(c_1',c_2',c_3')=(Zm_\gamma,C,C^{J(V')})$。

与 Waters 方案中一样，若 $Z=e(g,g)^{abc}$，则

$$\begin{aligned}T&=\left(e(g,g)^{abc}m_\gamma,g^c,g^{cJ(V')}\right)\\&=\left(e(g_1,g_2)^cm_\gamma,g^c,\left(u'\prod_{i\in\langle V'\rangle}u_i\right)^c\right)\end{aligned}$$

即 T 是对 m_γ 的合法加密；而当 Z 为 G_1 中随机元素 $e(g,g)^z$ 时，挑战密文本身并未泄露 γ 的信息。

由于 A 用不合法的密文 $C=(c_1,c_2,c_3)$ 进行解密询问时，B 按照前面提及的方法可以检测出来。下面假设 A 总是用合法的密文 $C=(c_1,c_2,c_3)$ 进行解密询问。而当密文合法时，密文中的随机数、“身份” $V=H(c_1,c_2)$ 均由 c_1，c_2 确定，c_3 也由 c_1，c_2 确定，因此，若 $c_1=c_1'$，$c_2=c_2'$，则一定 $c_3=c_3'$。A 用来进行解密询问的密文 $C=(c_1,c_2,c_3)$ 一定满足 $(c_1,c_2)\neq(c_1',c_2')$，由于 hash 函数免碰撞性质，则一定有 $V'\neq V$，B 可以按照前面提及的方法模仿提取“身份” V 的“私钥” $d=(d_1,d_2)$，并进行解密。

最后，A 输出 γ'，若 $\gamma'=\gamma$，则 B 输出 $\beta'=1$，否则，输出 $\beta'=0$。

与 Waters 文中同样的分析知，以不可忽略概率， B 不中途停止。事实上，B 不中途停止的概率的分析和 Waters 方案中的分析几乎是相同的，唯一的区别是这里的“身份”是密文的第 1 部分和第 2 部分的 hash 值，但 Waters 方案的身份必须在加密之前确定。但是，由于以下原因，Waters 方案中计算模仿者不中途停止的概率的方法在这里仍然适用：首先，对于任何身份 ID，不管是否在加密之前决定，都有 $\Pr(K(\mathrm{ID})=0)=1/m$，因为，$X=(x_i)$ 中的任何元素都是在 1 至 m 中随机一致地选取的整数，$x'+\sum_{i\in\langle ID\rangle}x_i$ 等于 $0(\bmod m)$ 的概率为 $(1/m)$；其次，对于任意的两个不同的身份，(V,V')，至少存在一个下标值 j 满足 $v_j\neq v_j'$，这样，至少有一个 x_j 值，仅在 $x'+\sum_{i\in\langle V\rangle}x_i$ 与 $x'+\sum_{i\in\langle V'\rangle}x_i$ 其中的一个出现，而且由于 x_j 是在 1 至 m 中随机一致地选取的，所以 $x'+\sum_{i\in\langle V\rangle}x_i(\bmod m)$ 独立于 $x'+\sum_{i\in\langle V'\rangle}x_i(\bmod m)$；另外，由于 k 是在 0 至 n 之间随机一致地选取的整数，所以，对于任何身份 V，都有，$\Pr\pi\left(x'+\sum_{i\in\langle V\rangle}x_i=km\right)=\frac{1}{n+1}\Pr\left(x'+\sum_{i\in\langle V\rangle}x_i=0(\bmod m)\right)$。

当 B 不中途终止时，B 的模仿是完善的，若 A 以不可忽略的优势正确地区分出是对谁的加密，则 B 也可以相应的优势区分 $Z=e(g,g)^{abc}$ 还是 $Z=e(g,g)^z$。　　证毕

6　结束语

该文由Waters 的基于身份加密方案构造了一个高效的抗选择密文攻击的公钥密码方案。其安全性在标准的决定性 Diffie-Hellman 假设下被证明。与直接利用Canetti等的一般转化得到方案相比，新方案的效率有明显提高。

参 考 文 献

[1] Rackoff C, Simon D. Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attacks. Advances in Cryptology Crypto 1991, LNCS, Springer-Verlag, 1992, vol.576: 433−444.

[2] Bellare M, Rogaway P. Optimal asymmetric encryption. Advances in Cryptology Eurocrypt 1994, LNCS, Springer-Verlag, 1994, vol.950: 92−111.

[3] Cramer R, Shoup V. A practical public key cryptosystem provably secure againstchosen ciphertext attack. Advances in Cryptology Crypto 1998, LNCS, Springer-Verlag, 1998, vol.1462: 13−25.

[4] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. Advances in Cryptology Eurocrypt 2002, LNCS, Springer-Verlag, 2002,vol.2332: 45−64.

[5] Canetti R, Halevi S, Katz J. Chosen ciphertext security from identity-based encryption. Advances in Cryptology Eurocrypt 2004, LNCS, Springer-Verlag, 2004, vol.3027: 207−222.

[6] Boneh D, Boyen X. Efficient selective-id secure identity based encryption without random oracles. Advances in Cryptology Eurocrypt 2004, LNCS, Springer-Verlag, 2004, vol.3027: 223−238.

[7] Boneh D, Franklin M. Identity-based encryption from the weil pairing. Advances in Cryptology Crypto 2001, LNCS Springer-Verlag, 2001, vol.2139: 213 − 229.

[8] Waters B. Efficient identity-based encryption without random oracles. Advances in Cryptology Eurocrypt 2005, LNCS, Springer-Verlag,2005 , vol.3494, 114−127. Available at http://theory.stanford.edu/~bwaters/publications/publications.html

[9] Boneh D, Boyen X. Secure identity based encryption without random oracles. Advances in Cryptology Crypto 2004, LNCS, Springer-Verlag, 2004, vol.3152: 443−459.

[10] Boneh D, Boyen X. Short signatures without random oracles. Advances in Cryptology Eurocrypt 2004, LNCS, springer- Verlag, 2004, vol.3027: 56−73.

梅其祥： 男，1973 年生，博士生, 讲师，研究方向为可证明性安全、密码协议的分析与设计.

何大可： 男，1944 年生，教授，博士生导师, 研究方向为密码学、并行计算.

郑 宇： 男，1979 年生，博士生，研究方向为通信保密、信息系统安全工程.