标准模型下安全的基于身份的加密方案 *

王天芹
(华北水利水电学院 信息工程系, 郑州 450011)

摘 要: 首先提出一个有效的多级基于身份的加密方案。在此基础上, 结合强一次签名方案, 构造一个具有较强安全性的基于身份的加密方案,并在标准模型下证明了方案的安全性可归约为双线性群中标准困难问题的难解性。该方案在自适应选择密文攻击下具有语义安全性, 这是目前关于基于身份的加密方案最强的安全模型。

关键词: 基于身份加密; 强一次签名; 判定 Diffie-Hellman 问题; 双线性映射
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0633-04
doi:10.3969/j.issn.1001-3695.2012.02.061

Secure identity-based encryption scheme without random oracles

WANG Tian-qin
(*Dept. of Information Engineering, North China University of Water Conservancy & Electric Power, Zhengzhou* 450011, *China*)

Abstract: This paper proposed an efficient hierarchical identity-based encryption scheme. Based on the scheme and a strong one-time signature scheme, it presented a secure identity-based encryption scheme, which was proved to be secure under the decisional bilinear Diffie-Hellman assumption without random oracles. It is secure against adaptive chosen-ciphertext attacks.
Key words: identity-based encryption; strong one-time signature; decisional Diffie-Hellman problem; bilinear map

0 引言

基于身份的密码体制(IBC)的概念是由 Shamir[1] 于 1984 年首次提出的。在此密码体制中, 用户的身份标志符(如姓名、e-mail 地址等)可以看做用户的公钥, 而相应的私钥由可信中心来产生。IBC 的主要优点是消除了对用户证书的需求和依赖, 因此极大地简化了密钥管理问题。应用 Weil 配对技术, Boneh 等人[2] 于 2001 年提出了第一个有效的基于身份的加密(IBE)方案。自此之后, IBC 引起了众多学者的广泛关注并得到了快速发展, 很多基于身份的加密和签名方案被提出[3~6]。其中大多方案的安全性或者基于强困难问题假定, 或者基于随机预言模型。虽然随机预言模型有其自身的优势, 但它是一理想的假设。不依赖于理想化的随机预言模型, 设计在标准模型下可证明安全的方案是本文研究工作的动机之一。

近年来, 基于标准模型下的安全性证明受到广泛关注。Waters[7] 于 2005 年首次创造性地提出了标准模型下能够抵抗选择明文攻击的基于身份的高效加密方案, 并且方案的安全性可归约为标准困难问题假定。此后, Waters 方法受到关注, 很多标准模型下安全的 IBE 方案被提出[8~10]。

本文应用 Waters 方法, 基于文献[8,9]的设计思想和安全模型, 首先提出一个 2 级 IBE(2-HIBE)方案。在此基础上, 结合强一次签名方案, 构造一个标准模型下能够抵抗选择密文攻击的 IBE 方案, 并且证明方案的安全性可归约为双线性群中判定 Diffie-Hellman(BDH)问题的难解性。与文献[7,8]中的类似方案相比较, 本文的方案具有更高的安全性能。

1 记号与定义

设 A 是随机算法, 以 $A(x_1, x_2, \cdots : O_1, O_2, \cdots)$ 表示 A 的输入为 $x_1, x_2, \cdots$, 在运行过程中可以对预言机 $O_1, O_2, \cdots$ 作询问。

1.1 基本定义

定义 1 双线性对。设 G 和 G_1 是两个 p 阶循环乘法群, 其中 p 为素数, g 是 G 的生成元。如果存在函数 $e: G \times G \to G_1$, 且满足下面的性质:

a)双线性性,对任意的 $u,v \in G$, $a,b \in Z_p$, 有 $e(u^a,v^b) = e(u,v)^{ab}$;

b)非退化性,$e(g,g) \neq 1$;

c)可计算性,对任意 $u,v \in G$, 存在有效算法计算 $e(u,v)$;

则称 e 为双线性对或双线性映射, G 为双线性群。

定义 2 (t,ε)-BDH 假定。设双线性群 G 的阶为 p, 生成元为 g。对于随机数 $a,b,c \in Z_p$, 随机取 $\gamma \in \{0,1\}$。如果 $\gamma = 1$, 令 $T = e(g,g)^{abc}$;否则,随机选取 $z \in Z_p$, 令 $T = e(g,g)^z$。G 中的 BDH 问题是指对于 (g,g^a,g^b,g^c,T), 判断是否有 $T = e(g,g)^{abc}$。敌手 A 以至少 ε 的概率解决 G 中的 BDH 问题是指

$$|Pr[A(g,g^a,g^b,g^c,e(g,g)^{abc}) = 1] - Pr[A(g,g^a,g^b,g^c,e(g,g)^z) = 1]| \geqslant \varepsilon$$

如果不存在任何概率多项式时间(PPT)敌手在时间 t 内以至少 ε 的概率解决 G 中的 BDH 问题, 则称 G 中的 (t,ε)-BDH 假定成立。

1.2 *l*-HIBE 方案及安全模型

定义 3 *l*-HIBE 方案。设用户身份标志是长度 n 的位串。

收稿日期: 2011-06-23; **修回日期**: 2011-08-04 **基金项目**: 国家自然科学基金资助项目(11071070)
作者简介: 王天芹(1968-),女,河南南阳人,教授,博士,主要研究方向为数论、密码学(wangtq@amss.ac.cn).

一个 l-HIBE 方案是一个四元组(Setup, Derivation, Encryption, Decryption)。其中:

Setup 输入安全参数 k, 输出系统公开密钥 PK 和主密钥 mk。

Derivation 输入用户身份向量 $v\in(\{0,1\}^n)^{<l}$, 对应的私钥 SK_v 和位串 $r\in\{0,1\}^n$, 输出对应于身份向量(v,r)的私钥 $SK_{v,r}$,记为 $SK_{v,r}=\mathrm{Der}_{SKv}(v,r)$ 。

Encryption 输入用户身份向量 $v\in(\{0,1\}^n)^{\leqslant l}$和消息 M, 输出密文 C,记为 $C=E(v,M)$。

Decryption 输入用户身份向量 $v\in(\{0,1\}^n)^{\leqslant l}$, 对应的私钥 SK_v 和密文 C, 输出消息 M 或符号 $\perp$ (表示解密失败), 记为 $M=D_{SKv}(v,C)$。

满足:

对于 Setup 所输出的所有 PK 和 mk, 对任意 v, SK_v, M, 有 $D_{SKv}(v,E(v,M))=M$。

在下面的描述中, 设 k 为安全参数。以 O_{Der}表示模拟用户密钥产生算法的预言机, 以 O_{Dec}表示模拟解密算法的预言机。

定义 4 IBE 方案在选择密文攻击下的安全性。如果任何 PPT 敌手 A 在下面试验中的优势是可忽略的, 则称方案在选择密文攻击(CCA)下是安全的:

a)模拟者 O 执行 Setup, 将输出值 PK 发送给 A。

b)A 进行多次用户私钥询问或解密询问, 分别由 O_{Der}或 O_{Dec}给出相应回答。

c)A 给出挑战身份向量 v^* 和消息 M_0、M_1。O 随机选取 $\gamma\in\{0,1\}$, 计算 $C^*=E(v^*,M_\gamma)$并发送给 A。

d)A 继续进行多次用户私钥询问或解密询问(但要求私钥询问向量 v不是 v^* 的前缀), 由相应的预言机给出回答。

最后,A 输出 $\gamma'\in\{0,1\}$ 作为对 γ 的猜测。A 的优势定义为

$$\mathrm{Adv}_A=\left|Pr[\gamma=\gamma']-\frac{1}{2}\right|$$

注:如果在试验中要求敌手不能进行解密询问,则称方案在选择明文攻击(CPA)下是安全的。

2 2-HIBE 方案

令 G 为阶为素数 p 的双线性群, g 是 G 的生成元, 双线性映射为 e: $G\times G\to G_1$。用户身份标志 $\mathrm{ID}\in\{0,1\}^n$ 或 $\mathrm{ID}=(\mathrm{ID}_1,\mathrm{ID}_2)\in(\{0,1\}^n)^2$, 待加密的信息 $M\in G_1$。

2.1 方案描述

方案 Π' = (Setup, Extract, Derive, Encrypt, Decrypt) , 各算法描述如下:

1)Setup

随机选择 $\alpha\in Z_p^*$, 令 $g_1=g^\alpha$。随机选择 $g_2\in G$, 令 $v=e(g_1,g_2)$。随机选择 $u',v'\in G$, n 维向量 $\mathsf{u}=(u_i)$,$\mathsf{v}=(v_j)$,其中 $u_i,v_j\in G$。系统参数 $\mathrm{params}=(G,G_1,p,e,g,g_1,g_2,u',\mathsf{u},v',\mathsf{v},v)$,主密钥 $mk=(g_2^\alpha)$。

2)Extract(ID)

对于身份标志 $\mathrm{ID}=(k_1,k_2,\cdots,k_n)\in\{0,1\}^n$ 的用户(即第一级用户), 令 v 表示 ID 中 $k_i=1$ 的所有下标 i 的集合。随机选取 $r\in Z_p^*$, 计算并返回 $d_{\mathrm{ID}}=(d_0,d_1)=\left(g_2^\alpha\left(u'\prod_{i\in V}u_i\right)^r,g^r\right)$ 。

对于 $\mathrm{ID}=(\mathrm{ID}_1,\mathrm{ID}_2)=((k_1,k_2,\cdots,k_n),(l_1,l_2,\cdots,l_n))\in(\{0,1\}^n)^2$ 的用户(即第二级用户), 令 V_1 表示 ID 中 $k_i=1$ 的所有下标 i 的集合, V_2 表示 ID 中 $l_j=1$ 的所有下标 j 的集合(要求 $V_1\neq V_2$, 下同)。随机选取 $r_1\in Z_p^*$, $r_2\in Z_p^*$, 计算并返回 $d_{\mathrm{ID}}=(d_0,d_1,d_2)=\left(g_2^\alpha\left(u'\prod_{i\in V_1}u_i\right)^{r_1}\left(v'\prod_{j\in V_2}v_j\right)^{r_2},g^{r_1},g^{r_2}\right)$。

3)Derive(d_{ID_1},(ID_1,ID_2))

设 $d_{\mathrm{ID}_1}=(d'_0,d'_1)$,$\mathrm{ID}_1=(k_1,k_2,\cdots,k_n)\in\{0,1\}^n$,$\mathrm{ID}_2=(l_1,l_2,\cdots,l_n)\in\{0,1\}^n$。令 V_1 表示 ID_1 中 $k_i=1$ 的所有下标 i 的集合,V_2 表示 ID_2 中 $l_j=1$ 的所有下标 j 的集合。随机选取 $r_1\in Z_p^*$, $r_2\in Z_p^*$, 计算并返回 $d_{\mathrm{ID}}=(d_0,d_1,d_2)=\left(d'_0\left(u'\prod_{i\in V_1}u_i\right)^{r_1}\left(v'\prod_{j\in V_2}v_j\right)^{r_2},d'_1g^{r_1},g^{r_2}\right)$。

4)Encrypt(ID, M)

若 $\mathrm{ID}=(k_1,k_2,\cdots,k_n)\in\{0,1\}^n$, 令 V 表示 ID 中 $k_i=1$ 的所有下标 i 的集合。随机选取 $s\in Z_p^*$, 计算并返回密文

$$C=\left(Mv^s,g^s,\left(u'\prod_{i\in V}u_i\right)^s\right)。$$

若 $\mathrm{ID}=(\mathrm{ID}_1,\mathrm{ID}_2)=((k_1,k_2,\cdots,k_n),(l_1,l_2,\cdots,l_n))\in(\{0,1\}^n)^2$,令 V_1 表示 ID_1 中 $k_i=1$ 的所有下标 i 的集合,V_2 表示 ID_2 中 $l_j=1$ 的所有下标 j 的集合。随机选取 $s\in Z_p^*$, 计算并返回密文 $C=\left(Mv^s,g^s,\left(u'\prod_{i\in V_1}u_i\right)^s,\left(v'\prod_{j\in V_2}v_j\right)^s\right)$。

5)Decrypt(d_{ID}, C)

若 $d_{\mathrm{ID}}=(d_0,d_1)$,记做 $C=(A,B,C_1)$, 计算并返回 $M'=A\cdot e(d_1,C_1)/e(d_0,B)$。

若 $d_{\mathrm{ID}}=(d_0,d_1,d_2)$,记做 $C=(A,B,C_1,C_2)$,计算并返回 $M'=A\cdot e(d_1,C_1)\cdot e(d_2,C_2)/e(d_0,B)$。

2.2 安全性分析

根据定义 4 给出的 IBE 方案的安全性定义, 有如下结论。

定理 1 方案 Π'在选择明文攻击下是安全的。确切地说, Π' 能够抵抗 (t,q,ε)-选择明文攻击, 如果 $\left(t+\Theta((nq)^2(\varepsilon)^{-2}),\frac{\varepsilon}{O((nq)^2)}\right)$-BDH 假定成立。

证明 假定敌手 A'以 CPA 方式攻击方案 Π', 成功的概率至少为 ε。下面说明, 由 A'可以构造一个算法 A 解决 BDH 问题。

对于给定的元素$(g,A=g^a,B=g^b,C=g^c,T)\in G^4\times G_1$, 其中 T 或者为 $e(g,g)^{abc}$, 或者为 G_1 中的随机元素。A 的目标是输出 1 或 0, 作为对 T 值的猜测。若输出 1,则猜测 $T=e(g,g)^{abc}$;否则, 猜测 T 为 G_1 中的随机元素。

A 描述如下:

参数设置:令 $m=4q$, A 随机选取

$$k,k'\in\{0,\cdots,n\}$$
$$x',x_1,\cdots,x_n,w',w_1,\cdots,w_n\in\{0,\cdots,(m-1)\}$$
$$y',y_1,\cdots,y_n,z',z_1,\cdots z_n\in Z_p$$

令

$$g_1=A,\ g_2=B,$$
$$u'=g_2^{p-mk+x'}g^{y'},u_i=g_2^{x_i}g^{y_i},i=1,\cdots,n,$$
$$v'=g_2{}^{p-mk'+w'}g^{z'},v_j=g_2{}^{w_j}g^{z_j},\ j=1,\cdots,n$$

g_1,g_2,u',u_i,v',v_j 作为 A'的公开参数, 主密钥为 g^{ab}(对 A 未知)。

定义

$$F(\mathrm{ID})=(p-mk)+x'+\sum_{i\in V_{\mathrm{ID}}}x_i,J(\mathrm{ID})=y'+\sum_{i\in V_{\mathrm{ID}}}y_i$$
$$W(\mathrm{ID})=(p-mk')+w'+\sum_{i\in V_{\mathrm{ID}}}w_i,H(\mathrm{ID})=z'+\sum_{i\in V_{\mathrm{ID}}}z_i$$

$$K(\mathrm{ID})=\begin{cases}0 & \text{if } x'+\sum_{i\in V_{\mathrm{ID}}}x_i\equiv 0(\bmod m)\\ 1 & \text{otherwise}\end{cases}$$

$$L(\mathrm{ID})=\begin{cases}0 & \text{if } w'+\sum_{i\in V_{\mathrm{ID}}}w_i\equiv 0(\bmod m)\\ 1 & \text{otherwise}\end{cases}$$

其中:V_{ID}表示 $\mathrm{ID}=(k_1,k_2,\cdots,k_n)\in\{0,1\}^n$ 中 $k_i=1$ 的所有下标 i 的集合(下同)。

1)私钥询问　A 与 A'进行交互, 回答 A'所提出的私钥询问。

考虑对应于用户身份为 $\mathrm{ID}=(I_1,I_2)$ 的私钥询问(对应于 $\mathrm{ID}=(I_1)$ 的私钥询问同文献[7])。

如果 $K(I_1)\neq 0$, 则随机选取 $r\in Z_p$, 计算

$$d_{I_1}=(d'_0,d'_1)=\left(g_1^{\frac{-J(I_1)}{F(I_1)}}\left(u'\prod_{i\in V_{I_1}}u_i\right)^r,\ g_1^{\frac{-1}{F(I_1)}}g^r\right)$$

然后计算 $d_{\mathrm{ID}}=\mathrm{Derive}(d_{\mathrm{ID}_1},\mathrm{ID})$ 作为对 A'的回答。

否则(即 $K(I_1)=0$), 如果 $L(I_2)=0$, 则 A 输出随机数 $\beta'\in\{0,1\}$, 失败退出;否则, 随机选取 $r_1,r_2\in Z_p$, 计算

$$d_{\mathrm{ID}}=(d_0,d_1,d_2)=$$

$$\left(g_1^{\frac{-H(I_2)}{W(I_2)}}g^{J(I_1)r_1}\left(v'\prod_{j\in V_{I_2}}v_j\right)^{r_2},\ g^{r_1},\ g_1^{\frac{-1}{W(I_2)}}g^{r_2}\right)$$

作为对 A'的回答。

2)挑战　A'向 A 发送挑战信息 $M_0,M_1\in G_1$ 及 $\mathrm{ID}^*=(I_1^*,I_2^*)$。

如果 $x'+\sum_{i\in V_{I_1^*}}x_i\neq km\vee w'+\sum_{j\in V_{I_2^*}}w_j\neq k'm$, 则 A 输出随机数 $\beta'\in\{0,1\}$, 失败退出;否则, 随机选取 $\gamma\in\{0,1\}$, 计算 $C^*=(TM_\gamma,C,C^{J(I_1^*)},C^{H(I_2^*)})$作为对 A'的回答。

3)询问　A'继续向 A 提出私钥询问, A 同步骤 1)一样对 A'的询问进行回答。

4)猜测　A'输出 $\gamma'\in\{0,1\}$作为对步骤 2)中 γ 的猜测。

5)强制退出　类似文献[7],A 根据需要(由到目前为止 A'所作的私钥询问的性质所决定)强制失败退出。

最后(到目前为止 A 未失败退出), 如果 $\gamma'=\gamma$, 则 A 输出 $\beta'=1$ 并成功结束; 否则, 输出 $\beta'=0$ 并成功结束。

令 abort 表示事件 A 失败退出。

当 T 为 G_1 中的随机元素时, A'不能从 C^* 中获得有关 γ 的任何信息。此时, 无论事件 abort 是否发生, 都有

$$Pr[\beta'=1]=\frac{1}{2}\tag{1}$$

当 $T=e(g,g)^{abc}$时, 有

$$Pr[\beta'=1]=Pr[\beta'=1\mid\mathrm{abort}]\cdot Pr[\mathrm{abort}]+Pr[\beta'=1\mid\overline{\mathrm{abort}}]\cdot Pr[\overline{\mathrm{abort}}]$$

此时, 在 A 成功结束的情况下, 如果 A'对 γ 的猜测正确, 则 A 对 T 的猜测也正确,即 $Pr[\beta'=1\mid\overline{\mathrm{abort}}]=Pr[\gamma'=\gamma\mid\overline{\mathrm{abort}}]$;而当 A 失败退出时, 有 $Pr[\beta'=1\mid\mathrm{abort}]=\frac{1}{2}$。因此有

$$Pr[\beta'=1]=$$

$$\frac{1}{2}\cdot Pr[\mathrm{abort}]+Pr[\gamma'=\gamma\mid\overline{\mathrm{abort}}]\cdot Pr[\overline{\mathrm{abort}}]=$$

$$\frac{1}{2}-\frac{1}{2}\cdot Pr[\overline{\mathrm{abort}}]+Pr[\gamma'=\gamma\mid\overline{\mathrm{abort}}]\cdot Pr[\overline{\mathrm{abort}}]\tag{2}$$

另外, 由假设条件有

$$\left|Pr[\gamma'=\gamma]-\frac{1}{2}\right|\geqslant\varepsilon\tag{3}$$

由式(1)(2)(3)可得,A 成功解决 BDH 问题的概率为

$$\tilde{\varepsilon}=\left|Pr[\gamma'=\gamma\mid\overline{\mathrm{abort}}]\cdot Pr[\overline{\mathrm{abort}}]-\frac{1}{2}\cdot Pr[\overline{\mathrm{abort}}]\right|=$$

$$\left|Pr[\overline{\mathrm{abort}}\mid\gamma'=\gamma]\cdot Pr[\gamma'=\gamma]-\frac{1}{2}\cdot(Pr[\overline{\mathrm{abort}}\mid\gamma'=\gamma]\cdot Pr[\gamma'=\gamma]+Pr[\overline{\mathrm{abort}}\mid\gamma'\neq\gamma]\cdot Pr[\gamma'\neq\gamma])\right|=$$

$$\left|\frac{1}{2}\cdot Pr[\overline{\mathrm{abort}}\mid\gamma'=\gamma]\cdot(\frac{1}{2}+\varepsilon)-\frac{1}{2}\cdot Pr[\overline{\mathrm{abort}}\mid\gamma'\neq\gamma]\cdot(\frac{1}{2}-\varepsilon)\right|$$

类似文献 7 定理 1 中的方法对 $\tilde{\varepsilon}$ 进行估计, 可得 $\tilde{\varepsilon}\geqslant\frac{\varepsilon}{O((nq)^2)}$。定理 1 证完。

3　IBE 方案

基于 HIBE 方案, 结合强一次签名方案, 可以构造具有高安全性的 IBE 方案。

3.1　方案描述

设强一次签名方案 $S=(\mathrm{Gen},\mathrm{Sig},\mathrm{Vf})$, 其中:Gen 为参数生成算法, 所生成的验证密钥 $vk\in\{0,1\}^{n-1}$;Sig 为签名算法, Vf 为验证算法。基于 2.1 节的方案 $\Pi'=(\mathrm{Setup},\mathrm{Extract},\mathrm{Derive},\mathrm{Encrypt},\mathrm{Decrypt})$, 构造如下 IBE 方案 $\Pi=(\mathrm{Init},\mathrm{Ext},\mathrm{Enc},\mathrm{Dec})$, 其中用户身份 $\mathrm{ID}\in\{0,1\}^{n-1}$。

a)Init。同 Π'中的算法 Setup。

b)Ext(ID)。令$\hat{\mathrm{ID}}=0\parallel\mathrm{ID}$, 返回 $d_{\mathrm{ID}}=d_{\hat{\mathrm{ID}}}=\mathrm{Extract}(\hat{\mathrm{ID}})$。

c)Enc(ID,M)。首先调用算法 Gen, 生成签名验证密钥对(sk,vk), 其中 $vk\in\{0,1\}^{n-1}$。令$\hat{\mathrm{ID}}=(0\parallel\mathrm{ID},1\parallel vk)$。计算$\hat{C}=\mathrm{Encrypt}(\hat{\mathrm{ID}},M)$,$\sigma=\mathrm{Sig}(sk,\hat{C})$, 返回 $C=(vk,\hat{C},\sigma)$。

d)Dec(d_{ID}, ID, C)。假定 $C=(vk,\hat{C},\sigma)$。首先调用算法 Vf, 验证对于$\hat{C}$的签名 σ 的有效性。如果签名无效, 则返回 $\perp$;否则, 令$\hat{\mathrm{ID}}=0\parallel\mathrm{ID}$,$\hat{vk}=1\parallel vk$。计算$\hat{d}=\mathrm{Derive}(d_{\mathrm{ID}},(\hat{\mathrm{ID}},\hat{vk}))$, 返回 $\mathrm{Decrypt}(\hat{d},\hat{C})$。

3.2　安全性分析

根据定义 4 给出的 IBE 方案的安全性定义, 有如下结论:

定理 2　方案 Π 能够抵抗(t,q,ε)-选择密文攻击。

证明　假设敌手 B 以 CCA 方式攻击 Π。下面说明, 由 B 可以构造 B', 以 CPA 方式攻击 Π'。

对于给定的参数 params,B'的目标是通过与其私钥询问预言机交互(进行私钥询问)破坏方案 Π'的语义安全性。

B'调用 B, 模拟 B 的预言机与 B 进行交互, 回答 B 所提出的各类询问(包括私钥询问和解密询问):

a)B'调用算法 Gen, 得到(vk^*,sk^*)。

b)B'将参数 params 发送给 B 作为 B 的公开参数。

c)对于 B 关于身份 ID 的私钥询问,B'向其预言机作关于$\hat{\mathrm{ID}}=0\parallel\mathrm{ID}$ 的私钥询问, 并将询问结果发送给 B。

d)对于 B 关于(ID,(vk,C,σ))的解密询问(不妨假设 $\mathrm{Vf}_{vk}(C,\sigma)=1$), 如果 $vk=vk^*$,B'输出随机位 $\gamma'\in\{0,1\}$并失败退出, 否则,B'首先向其预言机作关于$\hat{\mathrm{ID}}=(0\parallel\mathrm{ID},1\parallel vk)$的

私钥询问，然后根据询问结果 d_{ID} 解密 C，并将解密结果发送给 B。

e)对于 B 的挑战消息(ID^*,M_0,M_1),B'首先构造自己的挑战消息($\hat{ID}^* = (0 \| ID^*, 1 \| vk^*), M_0, M_1$)，然后对于收到的密文 C^*，计算 $\sigma^* = Sig_{sk^*}(C^*)$ 并将(vk^*,C^*,σ^*)发送给 B。

f)B 继续进行私钥询问和解密询问,B'如同 c)d)方式进行回答。

g)对于 B 的输出位 $\gamma' \in \{0,1\}$,B'输出 γ'。

令 Forge 表示事件 B 对(ID,(vk^*,C,σ))进行过解密询问。注意到，在 Forge 不发生时,B'对 B 的预言机的模拟是完善的，而在 Forge 发生时,B'成功的概率为 1/2。因此有

$$\left| Pr_{B'}[Succ] - \frac{1}{2} \right| = \left| Pr_B[Succ \wedge \overline{Forge}] + \frac{1}{2} Pr_B[Forge] - \frac{1}{2} \right|$$

另一方面,有

$$\left| Pr_B[Succ] - \frac{1}{2} \right| = \left| Pr_B[Succ \wedge Forge] + Pr_B[Succ \wedge \overline{Forge}] - \frac{1}{2} \right| \leqslant$$

$$\left| Pr_B[Succ \wedge Forge] - \frac{1}{2} Pr_B[Forge] \right| +$$

$$\left| Pr_B[Succ \wedge \overline{Forge}] + \frac{1}{2} Pr_B[Forge] - \frac{1}{2} \right| \leqslant$$

$$\frac{1}{2} Pr_B[Forge] + \left| Pr_B[Succ \wedge \overline{Forge}] + \frac{1}{2} Pr_B[Forge] - \frac{1}{2} \right|$$

因此，由签名方案 S 的安全性及定理 1 知，方案 Π 是安全的。定理 2 证完。

说明　与文献[7]中的 IBE 方案相比较，本文方案的优势是能够抵抗选择密文攻击的；与文献[8]中的 IBE 方案相比较，本文方案能够抵抗适应性身份攻击。

4　结束语

本文首先提出了一个 2-HIBE 方案，该方案在自适应选择明文攻击下具有语义安全性，并在标准模型下证明了方案的安全性可归约为双线性群中判定 Diffie-Hellman(BDH)问题。然后结合强一次签名方案，构造了一个标准模型下能够抵抗选择密文攻击的 IBE 方案，并证明了 IBE 方案的强安全性可由签名方案的安全性和 2-HIBE 方案的安全性来保证。这是目前构造高安全性 IBE 方案的一条有效途径。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology-Crypto. Berlin: Springer-Verlag, 1984: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology-Crypto. Berlin: Springer-Verlag, 2001: 213-229.

[3] HESS F. Efficient identity based signature schemes based on pairings [C]//Proc of the SAC. Berlin: Springer-Verlag, 2003: 310-324.

[4] BONEH D, BOYEN X. Secure identity based encryption without random oracles[C]//Advances in Cryptology-Crypto. Berlin: Springer-Verlag, 2004: 443-459.

[5] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model [C]//Proc of ACISP. Berlin: Springer-Verlag, 2006: 207-222.

[6] 李进,张方国,王燕鸣. 两个高效的基于分级身份的签名方案[J]. 电子学报, 2007,35(1):150-152.

[7] WATERS B. Efficient identity-based encryption without random oracles[C]//Proc of EUROCRYPT. Berlin: Springer-Verlag, 2005: 114-127.

[8] BONEH D, BOYEN X. Efficient selective identity-based encryption without random oracles[J]. Journal of Cryptology, 2011, 24(4): 659-693.

[9] CANETTI R, HALEVI S, KATS J. Chosen-ciphertext security from identity-based encryption[C]//LNCS, vol 3027. Berlin: Springer-Verlag, 2004: 207-222.

[10] GENTRY C, HALEVI S. Hierarchical identity based encryption with polynomially many levels[C]//LNCS, vol 5444. Berlin: Springer-Verlag, 2009: 437-456.

(上接第 632 页)

5　结束语

盲签名方案在电子现金、电子选举等领域有着重要的应用,而部分盲签名是一种克服了盲签名缺点的更实用的密码技术。无证书密码体制既消除了传统密码体制对证书的需求,又解决了基于身份密码体制的密钥托管问题。秘密共享又可以防止单个管理者的权力滥用。本文首次将部分盲签名、无证书签名、秘密共享三者结合起来,提出无证书门限部分盲签名方案,并对其安全性进行了证明。该方案具有很大的应用空间,特别适用于基于盲签名的多管理者选举系统和安全电子现金系统。并且这种具有特殊性质的部分盲签名的研究将是近期的热点研究问题。

参考文献

[1] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology-CRYPTO. New York:Spring-Verlag,1982:199-203.

[2] ABE M, FUJISAKI E. How to date blind signatures[C]// Proc of ASIACRYPT. London: Spring-Verlag,1996:244-251.

[3] Al-RIYARNI S,PATERSOA K. Certificateless public key eryptograp [C]//Proc of AsiaCRYPT. Berlin: Springer-Verlag, 2003: 452-473.

[4] HU B C,WONG D S,ZHANG Zhen-feng,*et al*. Certificateless signature:a new security model and an improved generic construction [J]. Designs,Codes and Cryptography,2007,42(2):109-126.

[5] CHOI K Y,PARK J H,HWANQ J Y,*et al*. Efficient cerificateless signature schemes[C]//Proc of the 5th International Conference on Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2007:443-458.

[6] 曹珍富,朱浩瑾,陆荣幸. 可证安全的强壮门限部分盲签名[J]. 中国科学 E 辑:信息科学,2005,35(12):1254-1265.

[7] 陆洪文,郑卓. 基于双线性对的门限部分盲签名方案[J]. 计算机应用,2005,25(9):2057-2059

[8] SHAMIR A. How to share a secret[J]. Communication of ACM, 1979,22(11):612-613.

[9] 王育民,肖国镇. 密码学与数据安全[M]. 北京:国防工业出版社, 1991:211-215

[10] ZHANG Zhen-feng,WONG D S,XU Jing,*et al*. Certificateless public-key signature security model and efficient construction[C]//LNCS, vol 3989. Berlin:Springer-Verlag,2006:293-308.