无证书门限部分盲签名方案 *

宋程远, 张串绒, 曹 帅
(空军工程大学 电讯工程学院, 西安 710077)

摘 要: 结合无证书公钥密码体制、部分盲签名和秘密共享技术,首次提出了无证书门限部分盲签名方案,使得签名方案既无密钥托管的弊端,又具有部分盲签名的特性,更加避免了单个管理者的权力滥用。然后对其安全性和性能进行了证明分析。分析表明,该方案具有部分盲性、安全性、强壮性等特性,是安全、有效的。

关键词: 无证书签名; 秘密共享; 部分盲签名; 双线性对
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0630-03
doi:10.3969/j.issn.1001-3695.2012.02.060

Certificateless threshold partially blind signature scheme

SONG Cheng-yuan, ZHANG Chuan-rong, CAO Shuai
(*Telecommunication Engineering Institute, Air Force Engineering University, Xi'an* 710077, *China*)

Abstract: This paper first proposed certficateless threshold partially blind signature scheme with certificateless signature, partially blind signatures and secret sharing. So this signature didn't have disadvantage of the key trusteeship, owned the advantage of partially blind signature and avoided abusing the right. Thenit proved and analysised the security and capability. Analysis shows that the proposed scheme is secure and effective. It has provable security properties of blindness, security, robustness.
Key words: certificateless signature; secret sharing; partially blind signatures; bilinear pairings

盲签名思想最早是由 Chaum[1] 于 1982 年提出的。由于盲签名具有保护用户隐私的性质,使得盲签名在电子现金、电子选举、不经意传输等领域有着广泛的应用。但是,在盲签名中签名者完全不知道最终签名的任何信息,可能造成签名被非法使用以及在电子现金系统中造成数据库的无限增长等问题。为了解决这些问题 Abe 等人[2] 提出了部分盲签名的概念,即允许签名人在签名中嵌入与用户事先协商的公共信息,并且这些信息不能被删除或非法修改。例如,签名者可以添加签名时间、签名有效期、对签署消息性质的说明性信息等。这样,可以对接收者有所限制,在签名者不知所签署消息的具体内容的情况下,有效保护了签名者的合法权益。

为了解决基于身份公钥密码体制中存在的密钥托管问题和基于证书密码体制中存在的证书管理问题。Al-Riyami 等人[3] 在 2003 年的亚洲密码学会议上提出了无证书密码学。在无证书公钥密码系统中,用户的私钥不再由密钥生成中心(KGC)单独生成,而是由密钥生成中心生成的部分私钥和用户自己选取的秘密值两部分结合产生,这就有效地避免了基于身份密码系统的密钥托管问题。同时又不需要任何证书的使用,解决了基于证书公钥系统的证书管理问题。2007 年 Hu 等人[4] 定义了一个无证书签名的安全模型。2007 年 Choi 等人[5] 提出了两个可证安全的无证书签名方案。

在基于部分盲签名方案的选举系统或者电子支付系统中,通常设置单个管理者进行管理,而这个管理者总是被赋予了选举或者消息签名的权利。这样,如果这个管理者不诚实,那么他可以滥用权力,为了自身的利益进行欺骗性行为。为了防止这种单个管理者的权力滥用,需要使用门限方案让多个管理者一起进行消息签名。曹珍富等人[6] 基于改进的 RSA 密码系统提出了一个可证安全的强壮门限部分盲签名方案,其安全性基于分解问题。随后陆洪文等人[7] 基于双线性对提出一种新型的门限部分盲签名方案。

本文首次将部分盲签名、无证书签名、秘密共享三者的优势充分地结合起来,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。

1 相关基础

1.1 双线性对

假设有 2 个 q 阶的循环群(其中 G_1 为加法群,G_2 为乘法群),如果有双线性对 $e: G_1 \times G_1 \to G_2$ 满足以下特性:

a)双线性性。$\forall P, Q \in G_1, \forall a, b \in F_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$。

b)非退化性。对于任意一点 $P \in G_1$, $e(P, P) \neq 1$。

c)可计算性。对于所有 $P, Q \in G_1$,总存在有效的方法计算 $e(P, Q)$。

双线性对能通过对椭圆曲线或超椭圆曲线中的 Weil 对或 Tate 对的变形得到[7]。基于椭圆曲线的密码方案的安全性主要依托于以下问题的难解性。给定 2 个 q 阶的循环群(其 G_1 为加法群,G_2 为乘法群),1 个双线性对 $e: G_1 \times G_1 \to G_2$ 和 G_1 的

收稿日期: 2011-07-04; **修回日期**: 2011-08-13 **基金项目**: 国家自然科学基金资助项目(60873233);陕西省科技攻关项目(2008-k04-21);西安市产学研结合项目(cxy08016)

作者简介:宋程远(1987-),女,山东东营人,硕士研究生,主要研究方向为信息安全(scy19871120929@126.com);张串绒(1965-),女,陕西眉县人,副教授,主要研究方向为信息安全、移动自组网;曹帅(1987-),男,甘肃平凉人,硕士研究生,主要研究方向为信息安全、移动自组网.

生成元 P,则(G_1, G_2, e)中的双线性 Diffie-Hellman 问题(BDHP)就是在给定(P,aP,bP,cP)的情况下计算 $e(P,P)^{abc}$;而判断双线性 Diffie-Hellman 问题(DBDHP)则是在已知(P,aP,bP,cP),$h\in G_2$ 的情况下判断 $h=e(P,P)^{abc}$ 是否成立。

1.2　门限签名体制

Shamir[8] 首先提出了门限方案。在(t,n)门限方案中,秘密 D 被分为 n 份子秘密 D_1,D_2,…,D_n,分配给 n 个人,该方案满足下列条件:

a)知道任意 t 个或者更多子秘密 D_i,则容易计算出秘密 D。

b)只知道 $t-1$ 个或者更少子密钥 D_i,则无法计算出秘密 D。

这种门限签名体制的提出克服了只有一个主密钥的两个缺点:a)若主密钥偶然地或蓄意地被暴露,整个系统就容易受攻击;b)若在主密钥丢失或毁坏,系统中的所有信息就用不成了。目前门限方案有多种形式,本文中主要采用的是拉格朗日内插多项式法[9]。

2　无证书门限部分盲签名方案

2.1　系统初始化

设 G_1 为 p 生成的循环加法群,阶为 q, G_2 为具有相同阶 q 的循环乘法群,$e:G_1\times G_1\rightarrow G_2$ 为一个双线性映射。定义三个安全的哈希函数 $H_0:\{0,1\}^*\rightarrow Z_q^*$, $H:\{0,1\}^*\rightarrow Z_q^*$, $H_1:\{0,1\}^*\rightarrow G_1^*$。PKG 随机选择 $s\in Z_q^*$,并计算 $P_{\text{pub}}=sP$。系统公开参数 params=$\{G_1,G_2,e,q,P,P_{\text{pub}},H_0,H,H_1\}$,主密钥 s 由 KGC 保管。

2.2　部分私钥提取

设签名者身份为 ID,输入参数 params 和主密钥 s 进行以下计算:a)计算 $Q_{\text{ID}}=H(\text{ID})$;b)计算出签名者的部分私钥为 $D_{\text{ID}}=sQ_{\text{ID}}$,并将 D_{ID} 通过安全认证信道发送给签名者,通过验证等式 $e(D_{\text{ID}},P)=e(Q_{\text{ID}},P_{\text{pub}})$,以检验其私钥的合法性。

2.3　秘密值生成

随机选择 $x_i\in_R Z_q^*$,并把 x_i 作为用户的部分私钥。

2.4　群签名者私钥生成

签名者产生自己完全的密钥,计算 $S_{\text{ID}}=x_iD_{\text{ID}}=x_isQ_{\text{ID}}$。

2.5　群签名者公钥计算

签名者产生自己的公钥 $Y=x_iP$。

2.6　密钥分发

设 t,n 门限方案满足 $n\geqslant 2t-1$,且满足 $q\geqslant t$,群体中的 n 个成员为 P_1,…,P_n,群公钥为 Y,群私钥为 S_{ID},每个成员 P_i 的分享公钥为 Y_i,个人分享私钥为 S_{ID_i}。

成员 P_i 通过以下步骤产生一个分享私钥 S_{ID_i}:

a)随机选取 $a_{i0}\in Z_q^*$ 将其保密,并广播 $a_{i0}P$。

b)随机选取系数在 Z_q 中,次数为 $t-1$ 的多项式 $f_i(x)$,满足 $f_i(0)=a_{i0}$,令 $f_i(x)=a_{it-1}x^{t-1}+a_{it-2}x^{t-2}+\cdots+a_{i0}$。

c)计算并广播 $a_{ij}P(j=1,2,\cdots,t-1)$,将 $f_i(j)$ 秘密地发送给其他签名成员 $P_j(j=1,2,\cdots,n;j\neq i)$。

d)P_i 在收到其他 P_j 发送的 $f_j(i)$ $(j=1,2,\cdots,n;j\neq i)$后,验证 $f_j(i)P=\sum_{k=0}^{t-1}i^k a_{jk}P$ 是否成立来验证 $f_j(i)$ 的有效性。

e)计算分享私钥 $S_{\text{ID}_i}=\sum_{k=1}^{n}f_k(i)$。设 $f(x)=\sum_{i=1}^{n}f_i(x)$,则 $S_{\text{ID}_i}=f(i)$;分享公钥为 $Y_i=S_{\text{ID}_i}P$。

在执行完密钥生成过程后,群公钥为 $Y=sP$,这里 $s=\sum_{i=1}^{n}a_{i0}$ 由全体成员共同生成,不需要另外的密钥管理,且每个群成员都无法获知群私钥。最后系统返回的公钥为 $pk=(Y_A,Y_{A_1},\cdots,Y_{A_n},P,G_1,G_2,H_0,H,H_1)$,私钥为 $sk=(S_{\text{ID}_1},\cdots,S_{\text{ID}_n},S_{\text{ID}})$。

2.7　签名过程

假设用户想要获得签名群体对消息 M 的部分盲签名,并且已经与其中至少 t 个成员事先商定 c 作为消息 M 的附加信息。不妨设 t 个签名者为 P_1,…,P_t 签名过程如下:

a)每个签名成员 P_i 随机选取 $r_i\in Z_q^*$,计算 $U_i=r_iH_1(c)Q_{\text{ID}}$,并将 U_i 发送给用户。

b)用户计算 $U=\sum_{i=1}^{t}U_i$。随机选 $\alpha,\beta\in Z_q^*$,计算 $U'=\alpha U+\alpha\beta Q_{\text{ID}}$,$h=\alpha^{-1}H_0(M\|c,U')+\beta$,将 h 发给每个签名成员 P_i。

c)每个签名成员 P_i 计算 $S'_i=w_ir_iH(c)S_{\text{ID}_i}+w_ihS_{\text{ID}_i}$。其中 $w_i=\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}$,并将 S'_i 发送给用户。

d)用户在收到 S'_i 后验证 $e(s'_i,P)=e((w_iU+w_ihH_1(c))Q_{\text{ID}},P_{\text{pub}})$是否成立,判断成立后计算 $S'=\sum_{i=1}^{t}S'_i$,并进行脱盲变换 $S=\alpha S'$;最后得到签名为(U',S,M,c)。

3　无证书门限部分盲签名方案分析

3.1　正确性

任何验证者可以通过以下的等式是否成立来验证签名的合法性:

$$e(S,P)=e(U'+H_0(m\|c,U')Q_{\text{ID}},P_{\text{pub}})$$

签名验证过程的正确性如下:

$$e(S,P)=e(\alpha S',P)=e(\alpha\sum(w_ir_iH_1(c)S_{\text{ID}_i}+w_ihS_{\text{ID}_i}),P)=$$
$$e(\alpha U+\alpha\beta Q_{\text{ID}}+H_0(m\|c,U')Q_{\text{ID}},P_{\text{pub}})=$$
$$e(U'+H_0(m\|c,U')Q_{\text{ID}},P_{\text{pub}})$$

3.2　部分盲性

本文提出的改进的基于身份的盲签名具有部分盲性。

由签名算法,如果给定一个有效的部分盲签名(U',S',m,c)以及在签名发行过程中交换的数据(U,h,S),考虑下面的方程:

$$S'=\alpha S \tag{1}$$
$$h=\alpha^{-1}H_0(m\|c,U')+\beta \tag{2}$$
$$U'=\alpha U+\alpha\beta Q_{\text{ID}} \tag{3}$$

一定能找到一个唯一的 $\alpha'\in_R Z_q^*$ 使得式(1)成立,而且进一步通过式(2)可得到一个唯一的 $\beta\in_R Z_q^*$,$\beta=h-(\alpha')^{-1}H_0(m\|c,U')$。因为($U'$,$S'$,$m$,$c$)是有效的部分盲签名,因此 $e(S,P)=e(U'+H_0(m\|c,U')Q_{\text{ID}},P_{\text{pub}})$成立。下面考虑 α'、β'是否满足式(3):

$$e(\alpha'U+\alpha'\beta'Q_{\text{ID}},P_{\text{pub}})=$$
$$e(\alpha'U+\alpha'(h-(\alpha')^{-1}H_0(m\|c,U'))Q_{\text{ID}},P_{\text{pub}})=$$
$$e(\alpha'rH_1(c)Q_{\text{ID}}+\alpha'hQ_{\text{ID}},P_{\text{pub}})e(S',P)^{-1}e(U',P_{\text{pub}})=$$
$$e(\alpha'S,P)e(S',P)^{-1}e(U',P_{\text{pub}})=$$
$$e(U',P_{\text{pub}})$$

3.3　安全性

本方案的安全性证明方法类似于文献[10]。由于用户的

私钥是由 KGC 生成的部分私钥和用户自己选择的秘密值共同构成,所以在无证书新型部分盲签名方案中有两种攻击模型。第一种模型(Type I)是攻击者知道 KGC 的主密钥,但是不能替换用户的公钥;第二种模型(Type II)是公钥替换攻击,攻击者可以替换任何用户的公钥,但不具有系统主密钥。

定理 1 在假设 hash 函数 H_1 和 H_2 是随机预言且在 Z_p^* 中 DLP 是难解的情况下,该方案的 Type I 攻击是安全的。

令 B 是问题 DLP 的解决者,假设敌手能伪造签名成功,则证明 B 可利用敌手的能力解决 DLP 问题。

构造一个算法,B 随机选取主密钥 $s \in Z_q^*$、$P_{pub} = sP$ 和系统参数 params $= \{G_1, G_2, e, q, P, P_{pub}, H_0, H, H_1\}$,然后交给敌手。由于敌手知道主密钥,所以它可以计算部分私钥 $D_{ID} = H(ID)$。B 保持一个表 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$,进行以下询问应答:

a)对随机预言机 H_1 的询问。B 保持一个列表 $L_1 = \{ID, Q\}$,初始为空,设 ID_i 是敌手对 H_1 的第 i 次访问。若 ID_i 在 L_1 列表中,返回 Q_i 值;如果 ID_i 不在 L_1 列表中,执行以下步骤:如果 $ID_i = ID^*$,B 选择 $Q^* \in Z_q^*$,且 $Q^* \notin (Q_1, Q_2, \cdots, Q_{q_h})$,将 Q^* 返回,并将 (ID_i, Q^*) 添加到表 L_1 中;否则将从 $(Q_1, Q_2, \cdots, Q_{q_h})$ 中返回一个值,返回敌手并将 (ID_i, Q^*) 添加到表 L_1 中。

b)公钥询问。当敌手想要查询的 ID 已在 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 表中,B 直接给予应答;当敌手想要查询的 ID 不在 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 表中,B 随机选取 $T \in \{0,1\}$ 和 $w \in Z_q^*$。如果 $T = 1$,则令 $Y_{ID} = wY \in G_1$,并令 $S_{ID} = w$,把值 $Y_{ID} = wP$ 返回给敌手,将 (ID, Y_{ID}, s_{ID}, T) 添加到 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 中,以跟踪敌手对公钥的询问。

c)私钥询问。若表 L 中有 (ID, Y_{ID}, s_{ID}, T),B 直接将 $S_{ID} = x_i D_{ID}$ 返回给敌手;若表 L 没有 (ID, Y_{ID}, s_{ID}, T),B 对 ID 进行公钥询问,并将 (ID, Y_{ID}, s_{ID}, T) 添加到 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 中,以跟踪敌手对私钥的询问。

d)签名询问。如果敌手进行 (ID, Y_{ID}, s_{ID}, T) 的签名询问,其中 M_i 表示消息,Y_i 表示由敌手选择的公钥,ID_i 表示身份,B 按照如下步骤新建签名:假设 $ID_i \neq ID^*$。随机选取 $x_i \in_R Z_p^*$,计算 $S_i = r_i H(c) S_{ID_i} + h_i S_{ID_i}$,$e(S, P) = e(U'_i + H_0(m \| c, U'_i) Q_{ID}, P_{pub}))$,则签名 $\sigma = (U'_i, S_i, M, c)$,B 返回 σ 给敌手。

最后使用分叉技术。假设敌手成功伪造一个签名 $\sigma = (U', S, M, c)$,那么 B 可以重放敌手的攻击能力,获得另外一个伪造签名 $\sigma' = (U'_i, S_i, M, c)$。B 输入 $(X = aP, Z = bP)$,则满足 $e(S^*, P) = e(U'^* + H_0(m \| c, U'^*) Q_{ID}, P_{pub}))$。其中 $P_{Pub} = sP$,$U'^* = tP$,$S^* = S_{ID}X$。故有 $e(S_{ID}X, P) = e(tP + H_0(m \| c, tP) Q_{ID}, sP))$,即 $e(S_{ID}X, P) = e(tP + H_0(m \| c, tP) Q_{ID}, sP)) e(S_{ID}aP, P) = e(tP + H_0(m \| c, tP) Q_{ID}, sP))$,$a = (tP + H_0(m \| c, tP) Q_{ID}, sP)) / (P, PS_{ID})$。这样敌手就解决了 DLP 难题,从而出现矛盾。

定理 2 在假设 hash 函数 H_1 和 H_2 是随机预言且在 Z_p^* 中 DLP 是难解的情况下,该方案的 Type II 攻击是安全的。

令 B 是问题 DLP 的解决者,假设敌手能伪造签名成功,则证明 B 可利用敌手的能力解决 DLP 问题。

B 选取随机数 $a, b \in Z_q^*$,其目标是计算 $\frac{a}{b} P$。将系统参数交给敌手,然后执行预言机模拟。假设密钥提取询问和签名询问由 H_1 处理,为避免对询问的回答冲突并保持回答的一致性,B 保持一个表 $L =$ ID, Y_{ID}, s_{ID}, T ,进行下列询问应答:

a)对随机预言机 H_1 的询问。B 保持一个列表 $L_1 = \{ID, Q\}$,初始为空,设 ID_i 是敌手对 H_1 的第 i 次访问。若 ID_i 在 L_1 列表中,返回 Q_i 值;如果 ID_i 不在 L_1 列表中,执行以下步骤:如果 $ID_i = ID^*$,B 选择 $Q^* \in Z_q^*$,且 $Q^* \notin (Q_1, Q_2, \cdots, Q_{q_h})$,将 Q^* 返回,并将 (ID_i, Q^*) 添加到表 L_1 中;否则将从 $(Q_1, Q_2, \cdots, Q_{q_h})$ 中返回一个值,返回敌手并将 (ID_i, Q^*) 添加到表 L_1 中。

b)部分私钥的询问。当敌手询问身份 ID_i 公钥时,B 判断 $ID_i = ID^*$ 是否成立,若 $ID_i = ID^*$,B 终止并返回“失败”。若 $ID_i \neq ID^*$,B 将返回给敌手,并将其添加到列表 $(ID_i, Y_{ID}, s_{ID}, T)$ 中,处理终止。

c)公钥询问。当敌手想要查询的 ID 已在 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 表中,B 直接给予应答;当敌手想要查询的 ID 不在 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 表中,B 随机选取 $T \in \{0,1\}$ 和 $w \in Z_q^*$。如果 $T = 1$,则令 $Y_{ID} = wY \in G_1$,并令 $S_{ID} = w$,把值 $Y_{ID} = wP$ 返回给敌手,将 (ID, Y_{ID}, s_{ID}, T) 添加到 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 中,以跟踪敌手对公钥的询问。

d)私钥询问。当收到敌手对 ID_i 的私钥询问,B 从表 $L = \{(ID, Y_{ID}, s_{ID}, T)\}$ 中,找到 ID_i 的部分私钥 D_i,返回敌手的私钥 $S_{ID_i} = x_i D_{ID_i}$。

e)公钥替换询问。当收到敌手关于身份 ID_i 的公钥替换询问,敌手选取 Y'_{ID},那么 B 更新 L 列表中 Y_{ID} 为 Y'_{ID}。

f)签名询问。如果敌手进行 (ID, Y_{ID}, s_{ID}, T) 的签名询问,其中 M_i 表示消息,Y_i 表示由敌手选择的公钥,ID_i 表示身份,B 按照如下步骤新建签名:假设 $ID_i \neq ID^*$。随机选取 $x_i \in_R Z_p^*$,计算 $S_i = r_i H(c) S_{ID_i} + h_i S_{ID_i}$,$e(S_i, P) = e(U'_i + H_0(m \| c, U'_i) Q_{ID}, P_{pub}))$,则签名 $\sigma = (U'_i, S_i, M, c)$,B 返回 σ 给敌手。

最后使用分叉技术。假设敌手成功伪造一个签名 $\sigma = (U', S, M, c)$,那么 B 可以重放敌手的攻击能力,获得另外一个伪造签名 $\sigma' = (U'_i, S_i, M, c)$。B 输入 $(X = aP, Z = bP)$,则满足 $e(S^*, P) = e(U'^* + H_0(m \| c, U'^*) Q_{ID}, P_{pub}))$。其中:

$$U'^* = tP, S^* = S_{ID}X, Q_{ID*} = t'Z$$

$$e(S^*, P) = e(U'^* + H_0(m \| c, U'^*) Q_{ID}, P_{pub}))$$

$$e(S_{ID}X, P) = (tP + H_0(m \| c, tP) t'Z, P_{pub})$$

$$\frac{a}{b} P = (t + H_0(m \| c, tP)) t'$$

这样 B 也就解决了 CDH 问题,从而出现矛盾。

3.4 强壮性

强壮性是指即使恶意攻击者贿赂了某些成员(最多 $t-1$ 个)使其在签名协议中不按照规定执行,最后仍然可以计算出正确的签名。本方案在私钥分发和部分随机数产生的每一步中都有广播用来验证部分私钥以及部分随机数的公开信息,这样保证了私钥分发和随机数产生具有强壮性;在签名过程中,通过验证 $e(s'_i, P) = e((w_i U + w_i h H_1(c)) Q_{ID}, P_{pub})$ 可以验证成员 P_i 是诚实的。因此,此无证书门限部分盲签名方案的强壮性得到保证。

4 性能分析

本方案由于避免了密钥托管,故比在基于身份的公钥密码体制下的部分盲签名安全性高。在效率方面,本方案所用的运算主要包括 G_1 中的点的加法、点数乘、Z_q 中的乘法和除法、哈希函数的运算、双线性对的运算等。与现有的各种基于 RSA 和离散对数的门限签名和盲签名相比,本文所用的双线性对方案计算的效率更高,更具有实际应用价值。 (下转第 636 页)

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

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

另一方面，有

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

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

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

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

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.