一种可证明安全的有效无证书签密方案

孙 华[1] 郑雪峰[2]
(安阳师范学院计算机与信息工程学院 安阳 455000)[1]
(北京科技大学计算机与通信工程学院 北京 100083)[2]

摘 要 无证书密码体制消除了基于身份密码系统中固有的密钥托管问题,同时又克服了传统公钥密码系统中复杂的证书管理问题,它具有两者的优点。签密是一个通过数字签名和公钥加密而同时实现认证和保密的密码学原语,而它却比分别签名和加密具有更低的计算量。提出了一种可证安全的无证书签密方案,其只在解签密阶段需要两个双线性对计算,因而具有较高的效率。最后,在随机预言模型下利用困难问题假设证明了方案满足适应性选择密文攻击下的不可区分性以及适应性选择消息和身份攻击下的存在不可伪造性。

关键词 无证书密码体制,签密,可证明安全,随机预言模型
中图法分类号 TP309 **文献标识码** A

Provably Secure and Efficient Certificateless Signcryption Scheme

SUN Hua[1] ZHENG Xue-feng[2]
(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]
(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract Certificateless cryptography eliminates the key escrow problem inherent in identity-based cryptosystems and avoids the complex certificate managerment problem in traditional certificate-based public-key cryptosystems, so it achieves the best advantages of them. Signcryption is a cryptographic primitive that could achieve authentication and confidentiality simultaneously by combining digital signature and public key encryption, while it has lower computational cost than signing and encryption respectively. In this paper, a provably secure certificateless signcryption scheme was proposed, which requires only two bilinear pairing operation in the unsigncryption phase and is much more efficient than the existing ones. In the last, we proved it satisfies indistinguishability against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message and identity attack by using the complexity assumptions in the random oracle model.

Keywords Certificateless cryptography, Signcryption, Provable security, Random oracle model

为了解决传统的基于证书公钥密码系统中复杂的证书管理问题,1984年,Shamir[1]创造性地提出了基于身份的公钥密码学。在基于身份密码体制中,用户私钥由PKG一方产生,故其能够伪造用户的签名,因而基于身份的密码体制具有内在的密钥托管性质,并不能实现真正意义上的不可否认性。2003年,Al-Riyami等人[2]提出了无证书公钥密码学的概念。在该系统中,密钥生成中心KGC只产生用户的部分私钥,用户使用自己选取的秘密值和部分私钥生成自己的私钥,这样就消除了基于身份密码中的密钥托管问题。由于无需使用证书,同时也克服了公钥基础设施PKI中的证书管理问题,故它具有两者的优点。

保密和认证是密码学中两个重要的安全目标,在许多实际应用中需要同时实现这两个功能,而传统的先签名后加密的方法不仅计算量大,而且效率也较低。1997年,Zheng[3]首次提出了签密这一密码原语,同时提出了一个有效的签密方案,它结合了公钥加密和数字签名的功能,然而含有形式化安全证明的签密方案[4,5]直到若干年后才被提出来。

2008年,Barbosa等人[6]提出了无证书签密的概念,并给出了第一个无证书签密方案。然而该方案在实现过程中需要6个双线性对运算。不仅效率较低而且方案本身也是不安全的。随后,Aranha等人[7]也提出了一种无证书签密方案,可是该方案中没有给出形式化的安全性证明过程。同年,Wu等人[8]给出了一个有效的无证书签密方案,该方案在实现过程中需要4个双线性对运算。然而文献[9]指出Wu等人所提出的方案既不满足机密性,也不满足不可伪造性。2008年,Selvi等人[10]还提出了第一个多接收者签密方案。

2010年,Xie等人[11]利用基于身份的签密方案[12]和无证书的公钥加密方案[13],提出了一个无证书的签密方案,该方

到稿日期:2013-01-26 返修日期:2013-04-27 本文受国家自然科学基金资助项目(61170244,U1204402),河南省科技厅科技攻关计划项目(112102210370),河南省教育厅科学技术研究重点项目(12A520002)资助。

孙 华(1980—),男,博士,副教授,主要研究方向为密码学和信息安全,E-mail:sh1227@163.com;郑雪峰(1951—),男,教授,博士生导师,主要研究方向为计算机系统安全分析、现代计算机网络技术、信息安全。

案在实现过程中仅需要两个双线性对运算。然而文献[14]指出 Xie 等人所提出的签密方案不满足第一类攻击下的存在不可伪造性。同年,Liu 等人[15]在标准模型下提出了一种无证书的签密方案,该方案在实现过程中需要 5 个双线性对运算。然而文献[16]指出 Liu 等人所提出的签密方案是不安全的。Li 等人[17]也提出了一种可证明安全的无证书签密方案,该方案在实现过程中也只需要两个双线性对运算,可惜的是该方案经分析也是不安全的。

本文基于无证书短签名方案[18]和无证书加密方案[13],提出了一种有效的无证书签密方案(CLSC, certificateless signcrypiton),然后在随机预言模型下基于困难问题假设证明了方案的安全性,方案在整个实现过程中,仅在解签密阶段需要两个双线性对运算,故具有较高的效率。

1 预备知识

1.1 双线性对

设 G、G_T 是阶为素数 p 的循环加法群和循环乘法群,g 是群 G 的生成元,双线性对是满足如下性质的映射 $e:G\times G\to G_T$:

1. 双线性:对于所有的 $p,Q\in G$ 与 $a,b\in Z_p$,都有 $e(aP,bQ)=e(P,Q)^{ab}$;

2. 非退化性:$e(g,g)\neq 1$;

3. 可计算性:存在一个有效的算法计算 $e(P,Q)$,其中 $P,Q\in G$。

1.2 有关困难问题

1. CDH 问题:已知 P 是群 G 的生成元,$a,b\in Z_p^*$,给定 $P,aP,bP\in G$,计算 abP。

2. q-BDHI 问题:已知 $a\in Z_p^*$,$Q\in G$,给定一 $(q+1)$ 元数组 $(Q,aQ,\cdots,a^qQ)\in G^{q+1}$,计算 $e(Q,Q)^{1/a}$。

3. k-CAA 问题:已知 $k,s,t_1,\cdots,t_k\in Z_p^*$,$P\in G$,给定一 $(2K+2)$ 元的数组 $(t_1,\cdots,t_k,P,Q=sP,(t_1+s)^{-1}P,\cdots,(t_k+s)^{-1}P)$,计算 $(c+s)^{-1}P$ 的值,其中 $c\in Z_P^*\backslash(t_1,\cdots,t_k)$。

4. mICDH 问题:已知 $a,b\in Z_p^*$,给定 $P,aP,b\in G$,计算 $(a+b)^{-1}P$。

1.3 无证书签密的形式化定义

定义 1 一个无证书签密方案由以下 7 个算法组成:

1)系统参数生成算法:输入安全参数 k,该算法产生系统公开参数 $params$、系统私钥 msk,其中 msk 保密。

2)部分私钥生成算法:输入系统公开参数 $params$、系统私钥 msk 及用户身份 ID,该算法产生用户的部分私钥 D_{ID}。

3)设置秘密值:输入安全参数 k 以及用户的身份 ID,该算法产生用户的秘密值 x_{ID}。

4)用户公钥生成算法:输入用户的身份 ID 及其秘密值 x_{ID},该算法产生用户的公钥 pk_{ID}。

5)用户私钥生成算法:输入用户的部分私钥 D_{ID}、秘密值 x_{ID} 以及用户的公钥 pk_{ID},该算法产生用户的私钥 sk_{ID}。

6)签密:输入签密发送者 ID_S 的私钥 sk_{ID_S}、签密接收者的身份 ID_R 和其公钥 pk_{ID_R}、待签密消息 m,该算法产生有效的无证书签密 σ。

7)解签密:输入签密发送者 ID_S 的身份 ID_S 和公钥 pk_{ID_S}、签密接收者 ID_R 的私钥 sk_{ID_R} 以及签密 σ,如果 σ 是一个有效的无证书签密,则该算法输出消息 m,否则,输出 $\perp$。

2 本文提出的无证书签密方案

1)系统参数生成算法:令 G、G_T 是阶为素数 p 的循环群,P 是群 G 的生成元,$e:G\times G\to G_T$ 是一个双线性映射。KGC 随机选取 $s\in Z_p^*$,计算 $P_{pub}=sP$,$g=e(P,P)$;选取哈希函数 $H_1:\{0,1\}^*\to Z_p^*$,$H_2:G\to Z_p^*$,$H_3:G_T\to\{0,1\}^n$,$H_4:\{0,1\}^n\times G_T\to Z_p^*$ 则系统公开参数为 $params=(G,G_T,e,P,P_{pub},g,H_1,H_2,H_3,H_4)$,系统私钥为 $msk=s$ 且保密。

2)部分私钥生成算法:给定用户身份 ID,KGC 先计算 $q_{ID}=H_1(ID)$,然后计算用户的部分私钥 $D_{ID}=(s+q_{ID})^{-1}P$,并通过安全信道将其发送给用户,用户在收到其部分私钥后,可以利用等式 $e(P_{pub}+H_1(ID)P,D_{ID})=e(P,P)=g$ 进行验证,如等式成立,则 D_{ID} 是一个有效的用户部分私钥。

3)设置秘密值:对于用户 ID,它随机选取 $x_{ID}\in Z_p^*$ 作为其秘密值。

4)用户公钥生成算法:对于用户 ID,它先计算 $Q_{ID}=P_{pub}+H_1(ID)P$,然后计算 $R_{ID}=x_{ID}Q_{ID}$ 并将其作为用户的公钥 pk_{ID}。

5)用户私钥生成算法:对于用户 ID,它先计算 $y_{ID}=H_2(R_{ID})$,然后利用其部分私钥计算 $S_{ID}=(x_{ID}+y_{ID})^{-1}D_{ID}$,则用户的私钥为 S_{ID}。

6)签密:设待签密消息为 $m\in\{0,1\}^n$,签密发送者的身份为 ID_S,签密接收者的身份为 ID_R,则通过执行下面的步骤来产生无证书的签密:

①签密发送者随机选取 $r\in Z_p^*$,计算 $U=g^r$,$c=m\oplus H_3(U)$;

②令 $h=H_4(m,U)$;

③签密发送者利用其私钥 S_{ID_S},计算 $S=(r+h)S_{ID_S}$;

④签密发送者首先计算 $Q_{ID_R}=P_{pub}+H_1(ID_R)P$,然后利用签密接收者 ID_R 的公钥 R_{ID_R} 计算 $y_{ID_R}=H_2(R_{ID_R})$,最后计算 $T=r(R_{ID_R}+y_{ID_R}Q_{ID_R})$。则生成的无证书签密为 $\sigma=(c,S,T)$。

7)解签密:设签密发送者的身份为 ID_S,签密接收者 ID_R 的私钥为 S_{ID_R},当收到无证书签密 $\sigma=(c,S,T)$ 后,其进行如下计算:

①计算 $U=e(T,S_{ID_R})$,$m=c\oplus H_3(U)$,$h=H_4(m,U)$;

②计算 $Q_{ID_S}=P_{pub}+H_1(ID_S)P$,然后利用签密发送者 ID_S 的公钥 R_{ID_S} 计算 $y_{ID_S}=H_2(R_{ID_S})$;

③当且仅当等式 $U=e(S,R_{ID_S}+y_{ID_S}Q_{ID_S})g^{-h}$ 成立时,σ 是一个有效的无证书签密,这时接受消息 m。

3 本文所提方案的安全性分析

3.1 正确性

方案的正确性很容易由下面的等式得到验证:

$$\begin{aligned}
&①e(T,S_{ID_R})=e(r(R_{ID_R}+y_{ID_R}Q_{ID_R}),S_{ID_R})\\
&\quad=e(r(x_{ID_R}+y_{ID_R})Q_{ID_R},(x_{ID_R}+y_{ID_R})^{-1}D_{ID_R})\\
&\quad=e(r(s+q_{ID_R})P,(s+q_{ID_R})^{-1}P)=e(P,P)^r=U\\
&②e(S,R_{ID_S}+y_{ID_S}Q_{ID_S})g^{-h}\\
&\quad=e((r+h)S_{ID_S},(x_{ID_S}+y_{ID_S})Q_{ID_S})g^{-h}
\end{aligned}$$

$=e((r+h)(x_{ID_S}+y_{ID_S})^{-1}D_{ID_S},(x_{ID_S}+y_{ID_S})Q_{ID_S})g^{-h}$

$=e(P,P)^{r+h}g^{-h}=U$

故方案是正确的。

3.2 机密性

由文献[6]可知,在无证书签密中存在两类攻击者,$\mathcal{A}_{\mathrm{I}}$(恶意用户)和 $\mathcal{A}_{\mathrm{II}}$(恶意的 KGC)。对于 $\mathcal{A}_{\mathrm{I}}$ 类攻击者而言,它不知道系统私钥,但可以替换任意用户的公钥;对于 $\mathcal{A}_{\mathrm{II}}$ 类攻击者而言,它知道系统私钥 msk,但不可以替换用户的公钥。下面通过挑战者 $\mathcal{C}$ 与攻击者 $\mathcal{A}\in(\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}})$ 之间的游戏,证明方案满足机密性。

定理 1 在 q-BDHI 困难问题假设下,本文方案在第一类攻击者 $\mathcal{A}_{\mathrm{I}}$ 攻击下是 IND-CLSC-CCA2-I 的。

证明:假设攻击者 $\mathcal{A}_{\mathrm{I}}$ 能以不可忽略的优势攻击本方案,则能够构造算法 B,B 可以利用 $\mathcal{A}_{\mathrm{I}}$ 解决 q-BDHI 问题。

给定 B 一个 q-BDHI 问题的实例$(Q,aQ,\cdots,a^qQ)$,其目标是计算 $e(Q,Q)^{1/a}$,其中 $a\in Z_p^*$。为此 B 模仿 $\mathcal{A}_{\mathrm{I}}$ 的挑战者,具体过程如下:

系统初始化:算法 B 随机选取 $w_0,w_1,\cdots,w_{q-1}\in Z_p^*$,进行如下计算:

①利用 $w_i(i\in 1,\cdots,q-1)$ 构造多项式 $f(x)=\prod_{i=1}^{q-1}(x+w_i)=\sum_{i=1}^{q-1}c_ix^i$,从而得到多项式的系数 $c_0,\cdots,c_{q-1}$;

②计算 G 的生成元为 $P=f(q)Q=\sum_{i=0}^{q-1}c_i(a^iQ)$,并设 $P_{pub}=-\sum_{i=1}^{q}c_{i-1}(a^iQ)-w_0\sum_{i=0}^{q-1}c_i(a^iQ)$,那么有 $P_{pub}=-(a+w_0)P$,即 $msk=s=-a-w_0$;

③计算 $f_i(x)=f(x)/(x+w_i)=\sum_{i=0}^{q-2}d_ix^i,1\leqslant i\leqslant q-1$,则有 $\sum_{i=0}^{q-2}d_i(a^iQ)=f_i(a)Q=\frac{1}{a+w_i}P$,从而可得 $q-1$ 个元素对 $(w_i,\frac{1}{a+w_i}P)$,令 $I_i=w_0-w_i$,则可得到 $q-1$ 个元素对$(I_i,\frac{1}{s+I_i}P)$。

算法 B 然后将系统公开 *params* 参数发送给 $\mathcal{A}_{\mathrm{I}}$,其中 $g=e(P,P)$,$P_{pub}=(a+w_0)P$,系统私钥 $msk=s$ 对 B 未知。B 随机选取 $ID^*\in\{0,1\}^*$ 并把 ID^* 发送给 $\mathcal{A}_{\mathrm{I}}$。

第 1 阶段 攻击者 $\mathcal{A}_{\mathrm{I}}$ 可以适应性地向挑战者 $\mathcal{C}$ 发起如下一定数量的询问,这里假定 $\mathcal{A}_{\mathrm{I}}$ 在对部分私钥询问、用户公钥询问、用户私钥询问和签密询问之前已进行 H_1 询问,在对用户私钥询问和签密询问之前已进行用户公钥询问。算法 B 维护 5 个列表 L_1、L_2、L_3、L_4 和 $L_K=(ID,R_{ID},x_{ID},c\in(0,1))$,它们在初始状态下都是空表。

①H_1 询问:询问 $H_1(ID_i)$时,如果 $ID_i=ID^*$,则 B 返回 $q_{ID_i}=w_0$;否则,B 返回 $q_{ID_i}=I_i,i\in(1,\cdots,q-1)$。然后 B 计算 $Q_{ID_i}=P_{pub}+q_{ID_i}P$,并将$(ID_i,Q_{ID_i},q_{ID_i})$添加到列表 L_1 中。

②H_2 询问:询问 $H_2(R_{ID_i})$时,如果列表 L_2 中存在(R_{ID_i},y_{ID_i}),则返回 y_{ID_i};否则,B 随机选取 $y_{ID_i}\in Z_p^*$ 返回,并把(R_{ID_i},y_{ID_i})添加到列表 L_2 中。

③H_3 询问:询问 $H_3(U)$时,如果列表 L_3 中存在(U,h_3),则返回 h_3;否则,B 随机选取 $h_3\in\{0,1\}^n$ 返回,并把(U,h_3)添加到列表 L_3 中。

④H_4 询问:在询问 $H_4(m,U)$时,如果列表 L_4 中存在(m,U,h_4,c,γ),则返回 h_4;否则,B 随机选取 $h_4\in Z_p^*$ 返回,然后从列表 L_3 中选取 $h_3=H_3(U)$,计算 $c=m\oplus h_3$,$\gamma=U\cdot g^{h_4}$,并把(m,U,h_4,c,γ)添加到列表 L_4 中。

⑤部分私钥询问:当询问 ID_i 的部分私钥 D_{ID_i} 时,如果 $ID_i=ID^*$,那么算法 B 失败并退出;否则,B 返回 $D_{ID_i}=(s+I_i)^{-1}P$。

⑥用户公钥询问:当询问ID_i的公钥R_{ID_i}时,如果列表 L_K 中存在$(ID_i,R_{ID_i},x_{ID_i},c)$,则返回 R_{ID_i};否则,B 先在列表 L_1 中查询ID_i所对应的 Q_{ID_i},然后随机选取 $x_{ID_i}\in Z_p^*$ 并计算 $R_{ID_i}=x_{ID_i}Q_{ID_i}$,最后把$(ID_i,R_{ID_i},x_{ID_i},1)$添加到列表 L_K 中。

⑦用户私钥询问:当询问ID_i的私钥时,如果$ID_i=ID^*$,那么算法 B 失败并退出。如果$ID_i\neq ID^*$,B 先在列表 L_K 中查询$(ID_i,R_{ID_i},x_{ID_i},c)$,若 $c=1$ 并且列表 L_2 中含有(R_{ID_i},y_{ID_i}),则 B 返回 $S_{ID_i}=(x_{ID_i}+y_{ID_i})^{-1}(s+I_i)^{-1}P$;若 $c=1$ 并且列表 L_3 中不含有(R_{ID_i},y_{ID_i}),则 B 随机选取 $y_{ID_i}\in Z^{*p}$,并返回 $S_{ID_i}=(x_{ID_i}+y_{ID_i})^{-1}(t_i+s)^{-1}P$;若 $c=0$,则 B 先从 $\mathcal{A}_{\mathrm{I}}$ 处得到 x'_{ID_i},然后按照上面相同的方法计算并返回 S_{ID_i}。

⑧替换公钥询问:当将 ID_i 的公钥替换为 R'_{ID_i} 时,B 先在列表 L_K 中查询$(ID_i,R_{ID_i},x_{ID_i},c)$,若含有则将其公钥替换为 $R_{ID_i}=R'_{ID_i}$ 且 $c=0$;否则,B 先对 ID_i 进行用户公钥询问,然后令 $R_{ID_i}=R'_{ID_i}$ 且 $c=0$,并在列表 L_K 中作出相应的修改。

⑨签密询问:当询问(m,ID_S,ID_R)的签密时,若 $ID_S\neq ID^*$,则算法 B 能够构造 ID_S 的私钥,然后执行签密算法并返回相应的签密 σ;若 $ID_S=ID^*$,则可知 $ID_R\neq ID^*$,这时算法 B 能够构造 ID_R 的私钥 S_{ID_R},为使等式 $e(S,R_{ID_S}+y_{ID_S}Q_{ID_S})=e(T,S_{ID_R})g^h$ 成立,此时它进行如下计算:

1)算法 B 随机选取 $r_1,r_2\in Z_p^*$ 以及 $h_3\in\{0,1\}^n$;

2)令 $S=r_1S_{ID_R}$,$h=r_2$,$T=r_1(R_{ID_S}+y_{ID_S}Q_{ID_s})-r_2(R_{ID_R}+y_{ID_R}Q_{ID_R})$以及 $c=m\oplus h_3$,其中$(R_{ID_S},y_{ID_S},Q_{ID_S},R_{ID_R},y_{ID_R},Q_{ID_R})$可由前面的询问得到。

3)算法 B 计算 $U=e(T,S_{ID_R})$,$h_3=H_3(U)$,$c=m\oplus h_3$,$h_4=r_2$,$\gamma=U\cdot g^{h_4}$,并把(U,h_3)添加到列表 L_3 中,同时把(m,U,h_4,c,γ)添加到列表 L_4 中。

如果 h_3、h_4 已存在相应的列表 L_3、L_4 中,那么算法 B 失败退出。否则,B 返回相应的无证书签密 $\sigma=(c,S,T)$。

⑩解签密询问:当询问$(ID_S,ID_R,\sigma=(c,S,T))$的解签密时,若 $ID_R\neq ID^*$,则算法 B 能够构造 ID_R 的私钥,然后执行解签密算法并返回相应的明文 m;若 $ID_R=ID^*$,则可知 $ID_S\neq ID^*$,这时算法 B 能够构造 ID_S 的私钥 S_{ID_S}。如果 σ 是一个有效的无证书签密,则有等式 $e*(T,S_{ID_S})=e(S-hS_{ID_S},R_{ID_R}+y_{ID_R}Q_{ID_R})$成立,$h$ 来自列表(m,U,h_4,c,γ)中,其中 $h=h_4$。最后,算法 B 验证等式 $e(S,R_{ID_S}+y_{ID_S}Q_{ID_S})=Ug^h=\gamma$ 是否成立,若等式成立,则返回相应的消息签名对(m,S)。

挑战阶段:攻击者 $\mathcal{A}_{\mathrm{I}}$ 取两个相同长度的消息 m_0、m_1,签密发送者 ID_S、签密接收者 ID_R,如果 $ID_R\neq ID^*$,那么算法 B 失败并退出;否则,B 随机选取 $\xi\in Z_p^*$,$c\in\{0,1\}^n$,$S\in G$,$T=-\xi P$,并返回挑战密文 $\sigma^*=(c,S,T)$。

第 2 阶段 攻击者 $\mathcal{A}_{\mathrm{I}}$ 可以如同第一阶段那样,发出一定数量询问,但是 $\mathcal{A}_{\mathrm{I}}$ 不能询问 ID_R 的私钥以及对 σ^* 进行解签

密询问。

猜测阶段：最后 $\mathcal{A}_{\mathrm{I}}$ 输出对消息 $m_b, b\in(0,1)$ 的猜测。如果猜测正确，则算法 B 从列表 L_3、L_4 中查询 (U,h_3)、(m,U,h_4,c,γ)，它们当中应包含正确的元素 $U=e(T,S_{ID_R})=e(-\xi P,\frac{1}{s+w_0}P)=e(P,P)^{\xi/a}$，若令 $\tau=e(Q,Q)^{1/a}$，由 $P=f(a)Q=\sum_{i=0}^{q-1}c_i(a^iQ)$，可得 $e(P,P)^{1/a}=\tau^{c_0^2}e(\sum_{i=0}^{q-2}c_{i+1}(a^iQ),c_0Q)e(P,\sum_{i=0}^{q-2}c_{i+1}(a^iQ))$，从而可计算出 $e(\theta,\theta)^{1/a}$。

因此，如果存在一个攻击者 $\mathcal{A}_{\mathrm{I}}$ 能以不可忽略的概率进行 CCA2 攻击，那么就存在一个有效的算法能以不可忽略的概率解决 q-BDHI 问题，而这与 q-BDHI 问题是一个困难问题相矛盾，故方案是 IND-CLSC-CCA2-I 安全的。

定理 2 在 CDH 困难问题假设下，本文方案在第二类攻击者 $\mathcal{A}_{\mathrm{II}}$ 攻击下是 IND-CLSC-CCA2-II 的。

证明：假设攻击者 $\mathcal{A}_{\mathrm{II}}$ 能以不可忽略的优势攻击本方案，则能够构造算法 B，B 可以利用 $\mathcal{A}_{\mathrm{II}}$ 解决 CDH 问题。

给定 B 一个 CDH 问题的实例 (P,aP,bP)，其目标是计算 abP。为此 B 模仿 $\mathcal{A}_{\mathrm{II}}$ 的挑战者，具体过程如下：

系统初始化：算法 B 构造系统公开参数 $params$，其中 $g=e(P,P)$，$P_{pub}=sP$，系统私钥 $msk=s$ 由 B 选定，然后 B 随机选取 $ID^*\in\{0,1\}^*$，并将 $params$、msk 和 ID^* 发送给 $\mathcal{A}_{\mathrm{II}}$。

第 1 阶段　攻击者 $\mathcal{A}_{\mathrm{II}}$ 可以适应性地向挑战者 $\mathcal{C}$ 发起如下一定数量的询问，这里假定 $\mathcal{A}_{\mathrm{II}}$ 在对用户公钥询问、用户私钥询问和签密询问之前已进行 H_1 询问，在对用户私钥询问和签密询问之前已进行用户公钥询问。算法 B 维护 5 个列表 L_1、L_2、L_3、L_4 和 $L_K=(ID,R_{ID},x_{ID},c=x_{ID}+y_{ID})$，它们在初始状态下都是空表。

① H_1 询问：询问 $H_1(ID_i)$ 时，B 随机选取 $q_{ID_i}\in Z_p^*$ 并返回，然后 B 计算 $Q_{ID_i}=P_{pub}+q_{ID_i}P$，并将 (ID_i,Q_{ID_i},q_{ID_i}) 添加到列表 L_1 中。

② H_2 询问：询问 $H_2(R_{ID_i})$ 时，B 如同定理 1 证明中那样进行响应。

③ H_3 询问：询问 $H_3(U)$ 时，B 如同定理 1 证明中那样进行响应。

④询问：在询问 $H_4(m,U)$ 时，B 如同定理 1 证明中那样进行响应。

⑤用户公钥询问：当询问 ID_i 的公钥 R_{ID_i} 时，如果 $ID_i=ID^*$，则 B 返回 $R_{ID_i}=saP+q_{ID_i}aP$，并把 $(ID_i,R_{ID_i},\perp,\perp)$ 添加到列表 L_K 中；如果 $ID_i\neq ID^*$，则 B 先在列表 L_1 中查询 (ID_i,Q_{ID_i},q_{ID_i})，然后随机选取 $x_{ID_i}\in Z_p^*$ 计算 $R_{ID_i}=x_{ID_i}Q_{ID_i}$，$y_{ID_i}=H_2(R_{ID_i})$，$c=x_{ID_i}+y_{ID_i}$，并返回 R_{ID_i}，最后把 $(ID_i,R_{ID_i},x_{ID_i},c)$ 添加到列表 L_K 中。

⑥用户私钥询问：当询问 ID_i 的私钥时，如果 $ID_i=ID^*$，那么算法 B 失败并退出。如果 $ID_i\neq ID^*$，则 B 先在列表 $L_1=(ID_i,Q_{ID_i},q_{ID_i})$ 和 $L_K=(ID_i,R_{ID_i},x_{ID_i},c)$ 中进行查询，若列表 L_2 中含有 (R_{ID_i},y_{ID_i})，那么 B 返回 $S_{ID_i}=(x_{ID_i}+y_{ID_i})^{-1}(s+q_{ID_i})^{-1}P$；否则，B 先进行 $H_2(R_{ID_i})$ 询问，然后返回 $S_{ID_i}=(x_{ID_i}+y_{ID_i})^{-1}(s+q_{ID_i})^{-1}P$。

⑦签密询问：B 如同定理 1 证明中那样进行响应。

⑧解签密询问：B 如同定理 1 证明中那样进行响应。

挑战阶段：攻击者 $\mathcal{A}_{\mathrm{I}}$ 取两个相同长度的消息 m_0、m_1，签密发送者 ID_S、签密接收者 ID_R，如果 $ID_R\neq ID^*$，那么算法 B 失败并退出；否则，B 随机选取 $\mu\in Z_p^*$，$c\in\{0,1\}^n$，$S\in G$，$T=\mu(s+H_1(ID_R))bP$，并返回挑战密文 $\sigma^*=(c,S,T)$。

第 2 阶段　攻击者 $\mathcal{A}_{\mathrm{I}}$ 可以如同第一阶段那样，发出一定数量的询问，但是 $\mathcal{A}_{\mathrm{I}}$ 不能询问 ID_R 的私钥以及对 σ^* 进行解签密询问。

猜测阶段：最后 $\mathcal{A}_{\mathrm{II}}$ 输出对消息 $m_b, b\in(0,1)$ 的猜测。由本方案可知，有如下等式成立：

$$e(T,R_{ID_R})=e((x_{ID_R}+y_{ID_R})Q_{ID_R},rx_{ID_R}Q_{ID_R})$$

因此，如果 $\mathcal{A}_{\mathrm{II}}$ 猜测正确，则算法 B 从列表 L_2，L_K 中查询 (R_{ID_i},y_{ID_i})，$(ID_i,R_{ID_i},x_{ID_i},c_i=x_{ID_i}+y_{ID_i})$，它们当中应包含正确的元素 y_{ID_R}，$c_R=\mu$，满足 $e(T,R_{ID_R})=e(c_RQ_{ID_R},T-ry_{ID_R}Q_{ID_R})$，又由 $R_{ID_R}=saP+q_{ID_R}aP$，$T=\mu(s+H_1(ID_R))bP$，$ry_{ID_R}Q_{ID_R}=y_{ID_R}(s+H(ID_R))bP$，可知：

$$\begin{aligned}rx_{ID_R}Q_{ID_R}&=T-ry_{ID_R}Q_{ID_R}=(s+H(ID_R))abP\\&=T-y_{ID_R}(s+H(ID_R))bP\end{aligned}$$

从而可计算出 $abP=\dfrac{T-y_{ID_R}(s+H_1(ID_R))bP}{s+H(ID_R)}$。

因此，如果存在一个攻击者 $\mathcal{A}_{\mathrm{II}}$ 能以不可忽略的概率进行 CCA2 攻击，那么就存在一个有效的算法能以不可忽略的概率解决 CDH 问题，而这与 CDH 问题是一个困难问题相矛盾，故方案是 IND-CLSC-CCA2-II 安全的。

3.3　不可伪造性

下面通过挑战者 $\mathcal{C}$ 与攻击者 $\mathcal{A}\in(\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}})$ 之间的游戏，证明方案满足存在不可伪造性。

定理 3 在 k-CAA 困难问题假设下，本文方案在第一类攻击者 $\mathcal{A}_{\mathrm{I}}$ 攻击下是 EUF-CLSC-CMA-I 的。

证明：假设攻击者 $\mathcal{A}_{\mathrm{I}}$ 能以不可忽略的优势攻击本方案，则能够构造算法 B，B 可以利用 $\mathcal{A}_{\mathrm{I}}$ 解决 k-CAA 问题。

给定 B 一个 k-CAA 问题的实例 $(t_1,\cdots,t_k,P,Q=sP,(t_1+s)^{-1}P,\cdots,(t_k+s)^{-1}P)$，其目标是计算 $(t_0+s)^{-1}P$，其中 $t_0\in Z_p^*\backslash(t_1,\cdots,t_k)$。为此 B 模仿 $\mathcal{A}_{\mathrm{I}}$ 的挑战者，具体过程如下：

系统初始化：算法 B 构造系统公开参数 $params$，其中 $g=e(P,P)$，$P_{pub}=Q=sP$，系统私钥 $msk=s$ 对 B 未知，然后 B 随机选取 $ID^*\in\{0,1\}^*$，并将 $params$ 和 ID^* 发送给 $\mathcal{A}_{\mathrm{I}}$。

询问阶段：假定 $\mathcal{A}_{\mathrm{I}}$ 在对部分私钥询问、用户公钥询问、用户私钥询问和签密询问之前已进行 H_1 询问，在对用户私钥询问和签密询问之前已进行用户公钥询问。算法 B 维护 5 个列表 L_1、L_2、L_3、L_4 和 $L_K=(ID,R_{ID},x_{ID},c\in(0,1))$，它们在初始状态下都是空表。当攻击者 $\mathcal{A}_{\mathrm{I}}$ 发起一定数量的询问时，算法 B 进行如下响应：

① H_1 询问：询问 $H_1(ID_i)$，$1\leqslant i\leqslant q_{H_1}$ 时，q_{H_1} 为进行 H_1 询问的最大次数，如果 $ID_i=ID^*$，则 B 返回 $q_{ID_i}=t_0$；否则，B 返回 $q_{ID_i}=t_i, t_i\in(t_1,\cdots,t_k)$。然后 B 计算 $Q_{ID_i}=P_{pub}+q_{ID_i}P$，并将 (ID_i,Q_{ID_i},q_{ID_i}) 添加到列表 L_1 中。

② H_2 询问：询问 $H_2(R_{ID_i})$ 时，B 如同定理 1 证明中那样进行响应。

③ H_3 询问：询问 $H_3(U)$ 时，B 如同定理 1 证明中那样进行响应。

④ H_4 询问：在询问 $H_4(m,U)$ 时，B 如同定理 1 证明中那

样进行响应。

⑤部分私钥询问：当询问 ID_i 的部分私钥 D_{ID_i} 时，如果 $ID_i=ID^*$，那么算法 B 失败并退出；如果 $ID_i\neq ID^*$，那么 B 返回 $D_{ID_i}=(t_i+s)^{-1}P$。

⑥用户公钥询问：当询问 ID_i 的公钥 R_{ID_i} 时，B 如同定理 1 证明中那样进行响应。

⑦用户私钥询问：当询问 ID_i 的私钥时，B 如同定理 1 证明中那样进行响应。

⑧替换公钥询问：当将 ID_i 的公钥替换为 R'_{ID_i} 时，B 如同定理 1 证明中那样进行响应。

⑨签密询问：B 如同定理 1 证明中那样进行响应。

⑩解签密询问：B 如同定理 1 证明中那样进行响应。

伪造阶段：攻击者 $\mathcal{A}_I$ 输出消息 m^*、签密发送者 ID_S^*、签密接收者 ID_R^* 下的伪造无证书签密 $\sigma_1^*=(c,S_1,T)$，如果 $ID_S^*\neq ID^*$，那么算法 B 失败退出；否则，B 在列表 L_4 中查找 (m,U,h_4,c,γ)。根据分叉引理[19]，通过重放 $\mathcal{A}_I$，B 可以获得另一个不同的伪造 $\sigma_1^*=(c,S_2,T)$，这里 $h_4\neq h_4'$。由以下等式：

$$e(S_1,R_{ID_S}+y_{ID_S}Q_{ID_S})=Ug^{h_4} \tag{1}$$

$$e(S_2,R_{ID_S}+y_{ID_S}Q_{ID_S})=Ug^{h_4'} \tag{2}$$

可得 $g^{h_4'-h_4}=e(S_2-S_1,R_{ID_S}+y_{ID_S}Q_{ID_S})$，又由 $Q_{ID_S}=sP+t_0P$，有 $e(\frac{1}{s+t_0}P,P)=e(\frac{x_{ID_S}+y_{ID_S}}{h_4'-h_4}(S_2-S_1),P)$，故 k-CAA 问题的解为 $\frac{1}{s+t_0}P=\frac{x_{ID_S}+y_{ID_S}}{h_4'-h_4}(S_2-S_1)$。

因此，如果存在一个攻击者 $\mathcal{A}_I$ 能以不可忽略的概率伪造一个有效的无证书签密，那么就存在一个有效的算法能以不可忽略的概率解决 k-CAA 问题，而这与 k-CAA 问题是一个困难问题相矛盾，故方案是 EUF-CLSC-CMA-I 安全的。

定理 4 在 mICDH 困难问题假设下，本文方案在第二类 $\mathcal{A}_{II}$ 攻击下是 EUF-CLSC-CMA-II 的。

证明：假设攻击者 $\mathcal{A}_{II}$ 能以不可忽略的优势攻击本方案，则能够构造算法 B，B 可以利用 $\mathcal{A}_{II}$ 解决 mICDH 问题。

给定 B 一个 mICDH 问题的实例 (P,aP,b)，其目标是计算 $(a+b)^{-1}P$，其中 $a,b\in Z_p^*$。为此 B 模仿 $\mathcal{A}_{II}$ 的挑战者，具体过程如下：

系统初始化：算法 B 构造系统公开参数 $params$，其中 $g=e(P,P)$，$P_{sub}=sP$，系统私钥 $msk=s$ 由 B 选定，然后 B 随机选取 $ID^*\in\{0,1\}^*$，并将 $params$、msk 和 ID^* 发送给 $\mathcal{A}_{II}$。

询问阶段：假定 $\mathcal{A}_{II}$ 在对用户公钥询问、用户私钥询问和签密询问之前已进行 H_1 询问，在对用户私钥询问和签密询问之前已进行用户公钥询问。算法 B 维护 5 个列表 L_1、L_2、L_3、L_4 和 $L_K=(ID,R_{ID},x_{ID})$，它们在初始状态下都是空表。当攻击者 $\mathcal{A}_{II}$ 发起一定数量的询问时，算法 B 进行如下响应：

① H_1 询问：询问 $H_1(ID_i)$ 时，B 如同定理 2 证明中那样进行响应。

② H_2 询问：询问 $H_2(ID_i)$ 时，如果 $R_{ID_i}=saP+q_{ID_i}aP$，则返回 $y_{ID_i}=b$；否则，B 随机选取 $y_{ID_i}\in Z_p^*$ 返回，并把 (R_{ID_i},y_{ID_i}) 添加到列表 L_2 中。

③ H_3 询问：询问 $H_3(U)$ 时，B 如同定理 1 证明中那样进行响应。

④ H_4 询问：在询问 $H_4(m,U)$ 时，B 如同定理 1 证明中那样进行响应。

⑤用户公钥询问：当询问 ID_i 的公钥 R_{ID_i} 时，如果 $ID_i=ID^*$，则 B 返回 $R_{ID_i}=saP+q_{ID_i}aP$，并把 $(ID_i,R_{ID_i},\perp)$ 添加到列表 L_K 中；如果 $ID_i\neq ID^*$，则 B 先在列表 L_1 中查询 (ID_i,Q_{ID_i},q_{ID_i})，然后随机选取 $x_{ID_i}\in Z_p^*$ 计算 $R_{ID_i}=x_{ID_i}Q_{ID_i}$ 并返回，最后把 (ID_i,R_{ID_i},x_{ID_i}) 添加到列表 L_K 中。

⑥用户私钥询问：当询问 ID_i 的私钥时，B 如同定理 2 证明中那样进行响应。

⑦签密询问：B 如同定理 3 证明中那样进行响应。

⑧解签密询问：B 如同定理 3 证明中那样进行响应。

伪造阶段：攻击者 $\mathcal{A}_{II}$ 输出消息 m^*、签密发送者 ID_S^*、签密接收者 ID_R^* 下的伪造无证书签密 $\sigma_1^*=(c,S_1,T)$，如果 $ID_S\neq ID^*$，那么算法 B 失败退出；否则，B 在列表中 L_4 查找 (m,U,h_4,c,γ)。根据分叉引理，通过重放 $\mathcal{A}_{II}$，B 可以获得另一个不同的伪造 $\sigma_1^*=(c,S_2,T)$，这里 $h_4\neq h_4'$。由以下等式：

$$e(S_1,R_{ID_S}+y_{ID_S}Q_{ID_S})=Ug^{h_4} \tag{3}$$

$$e(S_2,R_{ID_S}+y_{ID_S}Q_{ID_S})=Ug^{h_4'} \tag{4}$$

可得 $g^{h_4'-h_4}=e(S_2-S_1,R_{ID_S}+y_{ID_S}Q_{ID_S})$，又由 $R_{ID_S}=saP+q_{ID_S}aP$，$y_{ID_S}=b$，有 $e(\frac{1}{a+b}P,P)=e(\frac{s+q_{ID_S}}{h_4'-h_4}(S_2-S_1),P)$，故 mICDH 问题的解为 $\frac{1}{a+b}P=\frac{s+q_{ID_S}}{h_4'-h_4}(S_2-S_1)$。

因此，如果存在一个攻击者 $\mathcal{A}_{II}$ 能以不可忽略的概率伪造一个有效的无证书签密，那么就存在一个有效的算法能以不可忽略的概率解决 mICDH 问题，而这与 mICDH 问题是一个困难问题相矛盾，故方案是 EUF-CLSC-CMA-II 安全的。

结束语 无证书公钥密码体制既避免了传统 PKI 中复杂的证书管理，又克服了基于身份密码体制中的密钥托管问题，因此引起了广大学者的浓厚兴趣。本文在无证书公钥密码体制下基于随机预言模型提出了一个有效可证安全的无证书签密方案，并通过对方案的安全性进行分析，证明其是安全可靠的。笔者下一步将继续研究基于标准模型的无证书公钥密码体制下的有关方案，并结合具体的应用环境进行分析、探讨，从而提出有效的方案。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 1984, LNCS 196. Berlin: Springer-Verlag, 1985: 47-53

[2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C] // Proceedings of ASIACRYPT 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452-473

[3] Zheng Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption) [C] // Proceedings of CRYPTO 1997, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179

[4] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption [C] // Proceedings of EUROCRYPT 2002, LNCS 2332. Berlin: Springer-Verlag, 2002: 83-107

[5] Baek J, Steinfeld R, Zheng Yu-liang. Formal proofs for the security of signcryption [J]. Journal of Cryptology, 2007, 20(2): 203-235

(下转第 125 页)

题 1)。

在假名追踪协议中,将 TA 私钥分配给 k 个权威,至少 m 个权威协同才可恢复用户身份(命题 2),显然,多个权威协同追踪比单个权威追踪更加公平可靠。而且,假名 $ID_{PU_i}=r_i\cdot(i\parallel ID_U\parallel \exp)\parallel r_i^{e_{TA}}$ 加入了随机成分 r_i,即使是 TAs 得到一个假名,也需对 r_i 进行穷搜索才可以获得 U 的其他假名,只要 r_i 足够长,即使多个权威协同也无法由用户 U 的一个假名 ID_{PU_i} 推出另一个假名 ID_{PU_j}。

因此,在匿名、不可伪造、可追踪方面,模型都体现了公平性。

结束语 本文提出新的部分盲签名方法,用以解决 CA 对假名盲签时,能够嵌入 ID,又不对外泄露 ID 的问题。通过该方法,能够防止用户欺骗,限制 CA 的权限,实现假名发行与追踪的分离,保证假名证书发行协议的公平性。身份和秘密关联的追踪机制导致管理员存储和搜索开销随着用户数量的增加而增加,本文提出将身份嵌入在假名中,由追踪组直接打开,提高了假名追踪的有效性。追踪时引入秘密共享方案,增强了系统的健壮性。同时,由于假名证书与传统数字证书的结构基本一致,本模型能够与基于 PKI 的应用较好地衔接。

参 考 文 献

[1] 朱建明,马建峰. 一种高效的具有用户匿名性的无线认证协议[J]. 通信学报,2004,25(6):12-18

[2] 彭华熹,冯登国. 匿名无线认证协议的匿名性缺陷和改进[J]. 通信学报,2006,27(9):78-85

[3] 于爱民,初晓博,冯登国. 基于可信芯片的终端平台匿名身份建立方法研究[J]. 计算机学报,2010,33(9):1703-1712

[4] 吴振强,周彦伟,乔子芮. 一种可控可信的匿名通信方案[J]. 计算机学报,2010,33(9):1686-1702

[5] Boneh D, Boyen X, Shacham H. Short group signatures[C]// Proceedings of Crypto'04. Springer Berlin Heidelberg, 2004: 41-55

[6] Sun Xiao-ting, Ho Pin-han, Shen Xue-min. GSIS: Secure vehicular communications with privacy preserving [J]. IEEE Transactions on vehicular technology, 2007, 56(6): 3442-3456

[7] 田子健,王继林,伍云霞. 一个动态的可追踪匿名认证方案[J]. 电子与信息学报,2005,27(11):1737-1740

[8] 李梦东,杨义先. 无可信第三方的离线电子现金匿名性控制[J]. 电子学报,2005,33(3):456-458

[9] Cao Tian-jie, Lin Dong-dai, Xue Rui. A randomized RSA-based partially blind signature scheme for electronic cash[J]. Computers & Security, 2005, 24(1): 44-49

[10] 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

[11] 冯涛,彭伟,马建峰. 安全的无可信 PKG 的部分盲签名方案[J]. 通信学报,2010,31(1):12-18

[12] Housley R, Ford W, Polk W, et al. Internet X. 509 Public Key Infrastructure Certificate and CRL Profile[EB/OL]. http://www.ietf.org/rfc/rfc2459.txt, 2012-03

[13] Shamir A. How to share a secret [J]. Communications of the ACM, 1989, 22(11): 612-613

(上接第 116 页)

[6] Barbosa M, Farshim P. Certificateless signcryption[C]// Proceedings of ASIACCS 2008. ACM, New York, 2008: 369-372

[7] Aranha D, Castro R, Lopez J, et al. Efficient certificateless signcryption[EB/OL]. http://labcom.inf.ufrgs.br/labcom/ceseg/anais/2008/data/pdf/st03_01_resumo.pdf

[8] Wu Chen-huang, Cheng Zhi-xiong. A new efficient certificateless signcryption scheme[C]// Proceedings of ISISE 2008. IEEE Computer Society, 2008: 661-664

[9] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[EB/OL]. Cryptology ePrint Archive, 2009. http://eprint.iacr.org/2009/298

[10] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certificateless multi-receiver signcryption[C]// Proceedings of ProvSec 2008, LNCS 5324. Berlin: Springer-Verlag, 2008: 52-67

[11] Xie Wen-jian, Zhang Zhang. Efficient and provably secure certificateless signcryption from bilinear maps[C]// Proceedings of WCNIS 2010. IEEE Press, 2010: 558-562

[12] Barreto P S L M, Libert B, Mccullagh N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]// Proceedings of ASIACRYPT 2005, LNCS 3788. Berlin: Springer-Verlag, 2005: 515-532

[13] Chen Yan, Zhang Fu-tai. A new certificateless public key encryption scheme[J]. Wuhan University Journal of Natural Sciences, 2008, 13(6): 721-726

[14] Selvi S S D, Vivek S S, Rangan C P. Security weaknesses in two certificateless signcryption schemes[EB/OL]. Cryptology ePrint Archive, 2010. http://eprint.iacr.org/2010/092

[15] Liu Zhen-hua, Hu Yu-pu, Zhang Xiang-song, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3): 452-464

[16] Weng Jian, Yao Guo-xiang, Deng R H, et al. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3): 661-667

[17] Li Peng-cheng, He Ming-xing, Li Xiao, et al. Efficient and provably secure certificateless signcryption from bilinear pairings[J]. Journal of Computational Information Systems, 2010, 6(11): 3643-3650

[18] Du Hong-zhen, Wen Qiao-yan. Efficient and provably-secure certificateless short signature scheme from bilinear pairings[J]. Computer Standards and Interfaces, 2009, 31(2): 390-394

[19] Javier H, German S. Forking lemmas for ring signature schemes [C]// Proceedings of INDOCRYPT 2003, LNCS 2904. Berlin: Springer-Verlag, 2003: 266-279