可证安全的无证书代理环签名方案*

陈 虎, 魏仕民, 朱昌杰, 杨 忆
(淮北师范大学 计算机科学与技术学院, 安徽 淮北 235000)

摘 要: 代理环签名可使代理者以匿名的方式进行代理签名,具有很多优点。首先给出无证书代理环签名方案的最强安全模型,并利用双线性映射提出一个高效的无证书代理环签名方案。在所定义的最强的安全模型下,方案给出了严格的安全证明,它的安全性基于计算 Diffie-Hellman 问题的困难性。分析显示该方案满足诸如无条件匿名性、强不可伪造性等安全性质。鉴于该方案的安全、高效和无证书管理的优点,它可广泛应用于电子政务、移动代理系统等方面。

关键词: 无证书密码系统; 代理签名; 环签名; 代理环签名
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)03-0873-05
doi:10.3969/j.issn.1001-3695.2013.03.059

Provably secure certificateless proxy ring signature scheme

CHEN Hu, WEI Shi-min, ZHU Chang-jie, YANG Yi
(*School of Computer Science & Technology, Huaibei Normal University, Huaibei Anhui* 235000, *China*)

Abstract: Proxy ring signature, which enables a proxy signer to anonymously sign a message on behalf the original signer, has many advantages. This paper firstly proposed the strongest security model of certificateless proxy ring signature schemes and gave an efficient construction of certificateless proxy ring signature scheme using bilinear maps, with rigorous security proofs in the proposed strongest security model. The security of the scheme was based on the infeasibility of the computational Diffie-Hellman problem. The analysis shows that the new scheme satisfies the security requirements such as unconditional anonymity, strong unforgeability for a proxy ring signature scheme. Due to its security, efficiency and free of certificate management, it may have practical applications in electronic government affairs and mobile agent systems, etc.

Key words: certificateless cryptography; proxy signature; ring signature; proxy ring signature

0 引言

代理签名[1]因其能方便实现数字签名权利的委托,并且能保障具有代理关系双方所约定的合法权益而广泛地应用于日常生活之中。然而,生活的需求层出不穷,如某高校为打击论文剽窃、规范该校师生学术行为,由校学术委员会(原始签名人)授权校内外若干知名学者(代理签名人)对该校全体师生涉嫌剽窃的已发表论文进行网上监察,任一个代理签名人都可以代表原始签名人进行电子签名举报。但是,为了保护自己的权益,每个代理签名人更愿意以匿名方式进行代理签名,即代理签名人不希望包括原始签名人在内的任何人能追踪到他的身份。而环签名[2]恰能提供这种无条件的匿名性。

为解决上述问题,Zhang 等人[3]把代理签名和环签名结合起来,提出一个新概念——代理环签名,并给出具体的方案。随后,诸如基于证书的代理环签名方案[4,5]和基于身份的代理环签名方案[6,7]纷纷出现。然而,考虑到这两种公钥体制中,前者因伴有证书的管理而妨碍方案效率的提高,后者又因密钥托管问题使得方案存在一定的安全隐患。

为克服上述二个缺点并继承其优点,无证书公钥密码系统[8]应运出现,继而成为近期密码学领域的一个研究热点。许多的无证书加密和签名方案[9~14]如雨后春笋般涌现。其中,文献[13,14]分别提出了无证书代理环签名方案,但它们既没有给出相应的安全模型,也没能提供形式化的安全证明。据笔者所知,在目前可获得的公开文献中尚未发现可证安全的无证书代理环签名方案。

本文首先依据代理环签名复杂的应用场景,刻画出这种类型方案的安全模型,赋予攻击者最强的攻击能力;然后设计出一个具体的无证书代理环签名方案并给出形式化的安全证明。以标准的计算 Diffie-Hellman 问题作为其安全性的基础,其在代理环签名验证过程中需计算 7(预运算后只需 3)个双线性映射且不随环成员个数的增加而增加。该方案既满足代理签名又适合环签名的安全性要求。

1 无证书代理环签名的安全模型

本文中所说的攻击者均是指自适应选择消息和身份攻击下两类超级攻击者[10],分别表示为 A_{I} 和 A_{II}。其中:A_{I} 知道除

收稿日期: 2012-08-07; **修回日期**: 2012-09-18 **基金项目**: 国家自然科学基金资助项目(60673070);安徽省自然科学基金资助项目(1208085MF108);安徽省高校自然科学基金资助项目(KJ2012B157)

作者简介: 陈虎(1975-),男,江苏睢宁人,讲师,硕士,主要研究方向为信息安全与密码学(chenhuchh@163.com);魏仕民(1962-),男,安徽巢湖人,教授,博士,主要研究方向为密码学;朱昌杰(1963-),男,安徽怀宁人,教授,学士,主要研究方向为网络安全;杨忆(1980-),男,安徽凤阳人,讲师,硕士,主要研究方向为信息安全.

了系统主密钥之外的所有公开参数,并且可以替换系统中任何用户的公钥;A_{II}不仅可获知包括系统主密钥在内的所有参数,而且可以替换除了目标用户以外的任何用户的公钥。更详细的叙述,请参看文献[10]。

对无证书代理环签名的不可伪造性,可用一个游戏来刻画。游戏中涉及到两方:攻击者 $\Pi \in \{A_{\mathrm{I}}, A_{\mathrm{II}}\}$ 和挑战者 Σ。挑战者利用攻击者的能力去解决一个困难问题。

设置系统参数:设 l 为安全参数(下同)。Σ 输入 l 以初始化系统得到参数列表 public,并将 public 公开。Σ 需对 Π 保密系统主密钥,除非攻击者 Π 恰好是 A_{II}。

攻击:Π 可有限次地询问被 Σ 控制的各类预言器。在同 Π 交互过程中,Σ 要及时把产生的数据记录在初始为空的列表上。为叙述方便,符号 $\mathrm{ID}_0 \| P_0, \mathrm{ID}_i \| P_i$ 分别表示原始签名人和代理签名人的身份和公钥信息,$L_{\mathrm{ID}} \| P_{\mathrm{ID}}$表示 n 个代理签名人的身份和公钥信息,m_w 是委托证书。

部分私钥询问:(对 A_{II}无效)输入 public 和身份 ID,输出其部分私钥 D_{ID}。

公钥询问:输入 public 和身份 ID,输出其公钥 P_{ID}。

公钥替换询问:输入 public,身份 ID 和新公钥 P'_{ID},它把 ID 的公钥更新为 P'_{ID}。

秘密值询问:输入 public,身份 ID,输出其秘密值 x_{ID}。

部分代理钥询问:输入 public, $\mathrm{ID}_0 \| P_0, \mathrm{ID}_i \| P_i$ 以及 m_w,它输出部分代理钥 σ_0。

代理钥询问:输入 public, $\mathrm{ID}_0 \| P_0, \mathrm{ID}_i \| P_i$ 以及 m_w,输出代理钥 S_i。

代理环签名询问:输入 public, $\mathrm{ID}_0 \| P_0, L_{\mathrm{ID}} \| P_{\mathrm{ID}}$以及 m_w,它输出代理环签名 σ。

伪造:最后 Π 输出伪造元组$(m_w^*, P_0^*, \sigma_0^*, \mathrm{ID}_0^*)$或$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, \sigma^*, \mathrm{ID}_0^*)$。$\Pi$ 在游戏中获胜,只要下面情形至少有一个成立:

情形1 Π 输出元组$(m_w^*, P_0^*, \sigma_0^*, \mathrm{ID}_0^*)$满足:

a)$1 \leftarrow \mathrm{verify}(\mathrm{public}, m_w^*, \sigma_0^*, P_0^*, \mathrm{ID}_0^*)$。

b)当 Π 是 A_{I},则曾未作 ID_0^* 的部分私钥询问;否则,曾未作 ID_0^* 的秘密值和公钥替换询问。

c)对$(m_w^*, P_0^*, \mathrm{ID}_0^*)$曾未作部分代理钥询问。

情形2 Π 输出元组$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, \sigma^*, \mathrm{ID}_0^*)$满足:

a)$1 \leftarrow \mathrm{verify}(\mathrm{public}, m^*, m_w^*, L_{\mathrm{ID}}^*, L_{PK}^*, \sigma^*, P_0^*, \mathrm{ID}_0^*)$。

b)当 Π 是 A_{I},则曾未作 ID_0^* 的部分私钥询问;否则,曾未作 ID_0^* 的秘密值和公钥替换询问。

c)在 $m_w^*, \mathrm{ID}_0^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*$条件下,曾未对 L_{ID}^*中任何代理人作部分代理钥和代理钥询问。

d)对$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, \mathrm{ID}_0^*)$曾未作代理环签名询问。

情形3 Π 输出元组$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, \sigma^*, \mathrm{ID}_0^*)$满足:

a)$1 \leftarrow \mathrm{verify}(\mathrm{public}, m^*, m_w^*, L_{\mathrm{ID}}^*, L_{PK}^*, \sigma^*, P_0^*, \mathrm{ID}_0^*)$。

b)当 Π 是 A_{I},则曾未对 L_{ID}^*中任何代理人作部分私钥询问;否则,曾未对 L_{ID}^*中任何代理人作秘密值和公钥替换询问。

c)在 $m_w^*, \mathrm{ID}_0^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*$条件下,曾未对 L_{ID}^*中任何代理人作代理钥询问。

d)对$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, \mathrm{ID}_0^*)$曾未作代理环签名询问。

若任意多项式有界的攻击者,在上面的游戏中获胜的概率都是可忽视的,就称该无证书代理环签名是自适应选择消息和身份攻击存在不可伪造的。

2 无证书代理环签名方案

利用文献[9,12]中方案的一些思想设计本方案,其算法如下:

系统参数的生成:$(G_1, +)$和$(G_2, \cdot)$是素数 q 阶的循环群,其中 P 是 G_1 的一个生成元,$q \geqslant 2^l$。双线性映射 $e: G_1 \times G_1 \rightarrow G_2$。密钥生成中心(KGC)选择 $\lambda \in_R Z_q^*$ 作为系统主密钥,系统公钥 $P_{\mathrm{pub}} = \lambda P$,置 $g = e(P, P)$,H_1、H_2、$H_3: \{0,1\}^* \rightarrow G_1^*$,$H_4$、$H_5: \{0,1\}^* \rightarrow Z_q^*$ 是五个安全的密码哈希函数。消息空间 $M = \{0,1\}^*$。公开参数 public $= (G_1, G_2, e, H_1, H_2, H_3, H_4, H_5, q, P, P_{\mathrm{pub}}, g)$。

部分私钥提取:KGC 对用户所提交的身份 $\mathrm{ID}_i \in \{0,1\}^*$ 认证后,为其计算部分私钥 $D_i = \lambda Q_i = \lambda H_1(\mathrm{ID}_i)$,并利用安全信道将 D_i 传给用户。

设置公/私钥:用户 ID_i 选 $x_i \in_R Z_q^*$,计算 $P_i = x_i P, T_i = H_2(P_i \| \mathrm{ID}_i), S_i = D_i + x_i T_i$,其中 P_i 为公钥,(D_i, x_i, S_i)为私钥,x_i 为其秘密值。

部分代理钥生成:原始签名人 ID_0 制定委托证书 m_w,规定了原始签名人和代理签名人的身份信息、代理签名的权限等内容。ID_0 用其私钥(D_0, x_0, S_0)和 m_w,按下列步骤给 m_w 中所列的每个代理人生成部分代理钥。该群代理人的身份集为 $L'_{\mathrm{ID}} = \{\mathrm{ID}_1, \cdots, \mathrm{ID}_m\}$ 且相应的公钥集 $L'_{Pk} = \{P_1, \cdots, P_m\}$。

a)任选 $r_0, r \in_R Z_q^*$,计算 $y_0 = g^{r0}$ 和 $y = g^r$。

b)计算 $h_0 = H_4(m_w \| y_0 \| P_0 \| \mathrm{ID}_0)$ 和 $h = H_4(m_w \| y \| P_0 \| \mathrm{ID}_0)$。

c)计算 $K_0 = r_0 P - h_0 S_0, W = rP - hS_0$,置 $\sigma_{01} = (y_0, K_0)$, $\sigma_{02} = (y, W), \sigma_0 = (\sigma_{01}, \sigma_{02})$ 。

d)输出(m_w, σ_0)给每个代理人,其中 $\sigma_{01} = (y_0, K_0)$ 为部分代理钥,$\sigma_{02} = (y, W)$是对 m_w 的公开签名。

部分代理钥验证:每个代理签名人 ID_i 收到(m_w, σ_0)后都进行验证,$i \in \{1, 2, \cdots, n\}$:

a)计算 $T_0 = H_2(P_0 \| \mathrm{ID}_0), h_0 = H_4(m_w \| y_0 \| P_0 \| \mathrm{ID}_0), h = H_4(m_w \| y \| P_0 \| \mathrm{ID}_0)$。

b)验证 $y_0 = e(K_0, P)[e(H_1(\mathrm{ID}_0), P_{\mathrm{pub}}) e(P_0, T_0)]^{h_0}$ 和 $y = e(W, P)[e(H_1(\mathrm{ID}_0), P_{\mathrm{pub}}) e(P_0, T_0)]^h$ 是否同时成立。若都成立,接收 σ_0;否则,拒绝 σ_0。

设置代理钥:若每个代理签名人 ID_i 均接受(m_w, σ_0),则各自置代理签名钥为(D_i, K_0, x_i)。

代理环签名:真实代理签名人 ID_s 在这群代理人中任选一个包含自己的子集组建环签名的匿名集。不妨设匿名集中用

户的身份集 $L_{ID}=\{ID_1,ID_2,\cdots,ID_n\}\subset L'_{ID}$,相应的公钥集 $L_{PK}=\{P_1,P_2,\cdots,P_n\}\subset L'_{PK}$;$s\in\{1,2,\cdots,n\}$。有 n 个代理成员参与的代理环签名称为 n-环签名。ID_s 用其代理私钥(D_s,K_0,x_s)按如下步骤对消息 $m\in\{0,1\}^*$ 签名,并输出$(P_0,ID_0,m_w,m,L_{ID},L_{PK},y,W,\sigma)$。

a)计算 $U=H_3(m\|m_w\|y_0\|L_{ID}\|L_{PK})$。

b)任选 $r_i\in_R Z_q^*$,计算 $y_i=g^{r_i}$,$h_i=H_5(m\|m_w\|y_0\|y_i\|P_i\|ID_i)$,$i\in\{1,2,\cdots,n\}\setminus\{s\}$。

c)任选 $r_s\in_R Z_q^*$,计算 $y_s=g^{r_s}e(P_{pub},\sum_{i=1,i\neq s}^{n}h_iQ_i)e(U,\sum_{i=1,i\neq s}^{n}h_iP_i)$。若 $y_s=1_{G2}$或 $y_s=y_j$ 且$j\neq s$,只需重新选择 r_s 避免冲突。

d)计算 $h_s=H_5(m\|m_w\|y_0\|y_s\|P_s\|ID_s)$,置 $V=K_0-h_s(D_s+x_sU)+P\sum_{i=1}^{n}r_i$。

e)设置代理环签名 $\sigma=(y_0,y_1,y_2,\cdots,y_n,V)$。

代理环签名验证:对$(P_0,ID_0,m_w,m,L_{ID},L_{PK},y,W,\sigma=(y_0,y_1,y_2,\cdots,y_n,V))$,验证人执行:

a)判断消息 m 和身份集 L_{ID}是否都在委托证书 m_w 的授权范围内。若不是,拒绝签名;否则,执行 b)。

b)计算 $Q_0=H_1(ID_0)$,$T_0=H_2(P_0\|ID_0)$,$h=H_4(m_w\|y\|P_i\|ID_i)$。

c)验证 $y=e(W,P)[e(Q_0,P_{pub})e(P_0,T_0)]^h$ 是否成立。若不成立,拒绝签名;否则,执行 d)。

d)计算 $h_0=H_4(m_w\|y_0\|P_0\|ID_0)$,$U=H_3(m\|m_w\|y_0\|L_{ID}\|L_{PK})$。

e)计算 $Q_i=H_1(ID_i)$,$h_i=H_5(m\|m_w\|y_0\|y_i\|P_i\|ID_i)$,$i\in\{1,2,\cdots,n\}$。

f)验证

$$\prod_{i=0}^{n}y_i=e(V,P)e(P_0,h_0T_0)e(P_{pub},\sum_{i=0}^{n}h_iQ_i)e(U,\sum_{i=0}^{n}h_iP_i)$$

是否成立。若等式成立,则接受签名 σ;否则,拒绝签名。

3　安全性和效率分析

限于篇幅,这里仅给出无条件匿名性[12]、强不可伪造性的证明。

3.1　无条件匿名性

设 Ψ 是该 n-代理环签名的外部攻击者。下面证明对一个给定有效的代理环签名,Ψ 即使知道 n 个代理成员的代理私钥,他也绝不能以高于$\frac{1}{n}$的概率猜中真实签名者。

设原始签名人的身份和公钥分别为 ID_0,P_0,环成员身份集 $L_{ID}=\{ID_1,\cdots,ID_n\}$和公钥集 $L_{PK}=\{P_1,\cdots,P_n\}$。消息 m 在委托证书 m_w 下的一个有效的代理环签名是 $\sigma=\{y_0,\cdots,y_n,V\}$。

按照所给代理环签名算法,设任一环成员 ID_s 可以概率 $P(ID_s,\sigma)$输出上述给定签名。

现来计算 $P(ID_s,\sigma)$。ID_s 能以概率

$$\frac{1}{q-1}\frac{1}{q-2}\cdots\frac{1}{q-n+1}$$

去正确算出 y_i,满足 $y_i\neq1_{G_2}$且两两相异,其中 $i\in\{1,2,\cdots,n\}\setminus\{s\}$。另外,他还能以概率$\frac{1}{q-n}$选择唯一的值 $r_s\in Z_q^*$,正好计算出 y_s 相异于上述 y_i 和 1_{G_2}。于是有

$$P(ID_s,\sigma)=\frac{1}{q-1}\frac{1}{q-2}\cdots\frac{1}{q-n+1}\frac{1}{q-n}$$

而该值是定值且与下标 s 无关,这意味着每个环成员可以等概率地产生给定代理环签名。换句话说,Ψ 不能以高于$\frac{1}{n}$的概率猜中真实签名者,所以方案具有无条件匿名性。

3.2　强不可伪造性

$A(m,n)$表示从 m 个不同物体中选 n 个的排列数,其中 $n\leqslant m$且 $n,m\in N$。攻击者询问所有随机预言器的次数是 R,攻击者对非随机预言器询问次数总计是 Q,不可忽略的概率为

$$\varepsilon\geqslant\max\{7\times A(q_5,n)\times2^{-l},10\times2^{-l}\times(Q+1)\times(R+Q)\}$$

其中 l 为安全参数。

定理 1　在随机预言模型下,如果 A_1 至多做 q_1 次生成用户询问,q_2 次 H_2 询问,q_3 次 H_3 询问,q_4 次 H_4 询问,q_5 次 H_5 询问,q_6 次部分私钥询问,q_7 次公钥替换询问,q_8 次秘密值询问,q_9 次部分代理钥询问,q_{10}次代理钥询问,q_{11}次代理环签名询问后,在时间 t 内,以不可忽略的概率 $\varepsilon>0$ 伪造出有效的签名,那么存在一个算法 Σ 以概率

$$\varepsilon'\geqslant\varepsilon^2(66A(q_5,n))^{-1}q_1^{-1}(1-q_1^{-1})^{q_6+q_{10}}$$

在时间

$$t'\leqslant2t+23tR\varepsilon^{-1}+q_1t_1+q_2t_2+q_3t_3+q_4t_4+q_5t_5+q_6t_6+q_7t_7+q_8t_8+q_9t_9+q_{10}t_{10}+q_{11}t_{11}$$

内解决 CDH 问题。其中 t_1($t_2,t_3,t_4,t_5,t_6,t_7,t_8,t_9,t_{10}$和 t_{11})表示生成一次用户(H_2,H_3,H_4,H_5 分别为部分私钥,公钥替换,秘密值,部分代理钥,代理钥和代理环签名)询问所用的时间。

证明　CDH 问题的解决者 Σ 被给定$(P\in G_1,P_1=aP,P_2=bP)$,要求出 abP。下面给出在 A_1 的帮助下,Σ 求出 abP 的过程。

系统参数的设置:Σ 设置主公钥为 $P_{pub}=P_1=aP$,把 public $=(G_1,G_2,e,H_1,H_2,H_3,H_4,H_5,q,P,P_{pub},g)$给 A_1。

攻击:A_1 可以作 H_2,H_3,H_4,H_5 哈希询问,生成用户、公钥替换、秘密值、部分私钥、部分代理钥、代理钥及代理环签名等询问。Σ 把哈希函数 $H_1\sim H_5$ 作为随机预言器并维护 $H_1,H_2,H_3,H_4,H_5,L_1,L_2$ 和 L_3 等列表,这些表初始为空表。

生成用户询问:Σ 选择随机 $k\in\{1,2,\cdots,q_1\}$。当 A_1 询问 generate(ID_i)时,Σ 选 $x_i,\alpha_i\in_R Z_q^*$ 满足$(*,*,\alpha_i,*,*,*)$以前未出现在 H_1 列表,执行:当 $i=k$ 时,置 $P_k=x_kP$,$Q_k=\alpha_kP+P_2$,$D_k=\perp$(符号 $\perp$ 表示该值未知,下同);否则,置 $P_i=x_iP$,$Q_i=\alpha_iP$,$D_i=\alpha_iP_1$。Σ 把$(Q_i,D_i,\alpha_i,x_i,P_i,ID_i)$ 添加到 H_1 列表,并把 Q_i,P_i 给 A_1。

部分私钥询问:当 A_1 询问 pkey(ID_i)时,Σ 执行:当 $i=k$ 时,终止协议;否则,据 ID_i 在 H_1 列表中搜寻$(Q_i,D_i,\alpha_i,x_i,P_i,ID_i)$,并把 D_i 给 A_1。

公钥替换询问:当 A_1 询问 replace(P'_i,ID_i)时,Σ 据 ID_i 查找 H_1 列表,把元组$(Q_i,D_i,\alpha_i,x_i,P_i,ID_i)$替换为$(Q_i,D_i,\alpha_i,\perp,P'_i,ID_i)$。

秘密值询问:当 A_I 询问 secretValue(ID_i)时,Σ 据 ID_i 搜索 H_1 列表。若 $x_i \neq \perp$,则把 x_i 传递给 A_1;否则,输出 $\perp$。

H_2 哈希询问:A_1 询问 $H_2(P_i \| ID_i)$,Σ 选择 $\beta_i \in_R Z_q^*$,当把 $(*,\beta_i,*,*)$加到列表 H_2 时不会出现相同的记录,把 $T_i = \beta_i P$ 给 A_1。

H_3 哈希询问:当 A_1 询问 $H_3(m_i \| m_w^i \| y_0^i \| L_{ID}^i \| L_{PK}^i)$时,$\Sigma$ 选择 $\gamma_i \in_R Z_q^*$ 满足$(*,*,*,*,*,\gamma_i,*)$未出现在 H_3 列表。置 $U_i = \gamma_i P$。Σ 把 U_i给 A_1 并添$(m_i, m_w^i, y_0^i, L_{ID}^i, L_{PK}^i, \gamma_i, U_i)$到 H_3 列表。

H_4 哈希询问:当 A_1 询问 $H_4(m_w^i \| y_0^i \| P_0^i \| ID_0^i)$[或 $H_4(m_w^i \| y^i \| P_0^i \| ID_0^i)$]时,$\Sigma$ 选择 $h_0^i \in_R Z_q^*$[或 $h^i \in_R Z_q^*$]满足$(*,*,*,h_0^i,*)$[或$(*,*,*,h^i,*)$]未出现在 H_4 列表。Σ 把 h_0^i[或 h^i]给 A_1 并添$(m_w^i, y_0^i, P_0^i, h_0^i, ID_0^i)$[或$(m_w^i, y^i, P_0^i, h^i, ID_0^i)$]到 H_4 列表。

H_5 哈希询问:当 A_1 询问 $H_5(m_i \| m_w^i \| y_0^i \| y_i \| P_i \| ID_i)$时,$\Sigma$ 选择 $h_i \in_R Z_q^*$ 满足$(*,*,*,*,*,h_i,*)$未出现在 H_5 列表。Σ 返回 h_i给 A_1 并添$(m_i, m_w^i, y_0^i, y_i, P_i, h_i, ID_i)$到 H_5 列表。

部分代理钥询问:当 A_1 询问 PProxyK$(m_w^i, P_0{}^i, ID_0^i)$时,Σ 据(P_0^i, ID_0^i)检查 H_1 获得$(Q_0^i, D_0^i, \alpha_i, x_i, P_i, ID_0^i)$。若 $P_0{}^i \neq P_i$,则更新其公钥为 $P_0{}^i$ 且置 $x_i = \perp$,从 H_2 列表获得 T_0^i。Σ 按如下步骤执行:

a)任选 $K_0^i \in_R G_1^*$,$h_0^i \in_R Z_q^*$ 满足$(*,*,*,h_0^i,*)$未出现在 H_4 列表上。

b)计算 $y_0^i = e(K_0^i, P)[e(h_0^i Q_0^i, P_{pub}) e(h_0^i P_0^i, T_0^i)]$,置 $H_4(m_w^i \| y_0^i \| P_0^i \| ID_0^i) = h_0^i$。

Σ 将$(m_w^i, P_0^i, y_0^i, K_0^i, h_0^i, ID_0^i)$添加到 L_1 列表并把 K_0^i、y_0^i 给 A_1。

代理钥询问:当 A_1 询问 proKey(m_w^i, ID_0^i, ID_i)时,Σ 据 ID_i 检查 H_1 列表获得$(Q_i, D_i, \alpha_i, x_i, P_i, ID_i)$。当 $x_i = \perp$(说明 ID_i 的公钥已被替换),Σ 返回 $\perp$;否则,Σ 检查 L_1 列表。

a)若元组$(m_w^i, P_0^i, y_0^i, K_0^i, h_0^i, ID_0^i)$在 L_1 列表上,Σ 检查 ID_i。当 $ID_i = ID_k$,Σ 终止协议;否则,Σ 返回(D_i, K_0^i, x_i)作答,并添$(m_w^i, P_0^i, ID_i, P_i, x_i, D_i, K_0^i, ID_0^i)$到 L_2 列表。

b)否则,Σ 据 ID_0^i 检查 H_1 列表以获得 P_0^i,接着做 PProxyK(m_w^i, P_0^i, ID_0^i),再按 a)执行。

代理环签名询问:当 A_1 询问 proSign$(m_i, m_w^i, P_0^i, L_{ID}^i, L_{PK}^i, ID_0^i)$时,$\Sigma$ 据(m_w^i, P_0^i, ID_0^i)查询 L_1 列表以获得(y_0^i, K_0^i, h_0^i),再做一次 PProxyK (m_w^i, P_0^i, ID_0^i)询问得到 $\sigma_{02}^i = (y^i, W^i)$。据$(m_i, m_w^i, y_0^i, L_{ID}^i, L_{PK}^i)$查询 H_3 列表以获得 U_i,再据(P_0^i, ID_0^i)查询 H_2 列表以获得 T_0^i。Σ 执行:

a)任选 $s \in \{1,2,\cdots,n\}$。

b)对每个 $j \in \{1,2,\cdots,n\} \setminus \{s\}$,选 $r_j \in_R Z_q^*$,计算 $y_j^i = g^{r_j}$和 $h_j^i = H_5(m_i \| m_w^i \| y_0^i \| y_j^i \| P_j^i \| ID_j^i)$。

c)任选 $V^i \in_R G_1^*$ 和 $h_s^i \in_R Z_q^*$ 满足$(*,*,*,*,*,h_s^i,*)$未出现在 H_5 列表。

d)计算

$$y_s^i = e(h_0^i T_0^i, P_0^i) e(h_0^i Q_0^i, P_{pub}) e(\sum_{j=0}^n h_j^i Q_j^i, P_{pub}) e(\sum_{j=0}^n h_j^i P_j^i, U_i) \times e(V^i - P\sum_{j\neq s} r_i, P)$$

若 $y_s^i = 1_{G2}$或 $y_s^i = y_j^i$ 且 $j \neq s$,只需重新选择 V^i 避免出现上述冲突。

e)置 $H_5(m_i \| m_w^i \| y_0^i \| y_s^i \| P_s^i \| ID_s^i) = h_s^i$ 和 $\sigma_i = (y_0^i, y_1^i, y_2^i, \cdots, y_n^i, V^i)$。

Σ 将$(m_i, m_w^i, P_0^i, L_{ID}^i, L_{PK}^i, s, h_s^i, y^i, W^i, \sigma_i, ID_0^i)$添加到 L_3 列表并返回(y^i, W^i, σ_i)作答。

伪造:A_1 输出元组$(m_w^*, P_0^*, \sigma_{01}^*, ID_0^*)$或$(m_w^*, P_0^*, \sigma_{02}^*, ID_0^*)$或$(m^*, m_w^*, P_0^*, L_{ID}^*, L_{PK}^*, y^*, W^*, \sigma^*, ID_0^*)$。

a)若 A_1 输出$(m_w^*, P_0^*, \sigma_{01}^* = (y_0^*, K_0^*), ID_0^*)$且满足第 1 章中的情形 1。

若 $ID_0^* \neq ID_k$,Σ 终止协议。若 $ID_0^* = ID_k$,若 A_1 在上述攻击交互时间间隔 t 内能以至少 $\varepsilon \geqslant 10(Q+1)(R+Q)2^{-l}$的概率输出有效部分代理钥,则 Σ 选择不同的哈希函数 H_4' 并再次利用 A_1 的能力,据 Forking lemma[15],在不超过 $23tR\varepsilon^{-1}$时间内以至少 1/9 的概率,可得到另一个有效的伪造元组$(m_w^*, P_0^*, \sigma_{01}^{*\prime} = (y_0^*, K_0^{*\prime}), ID_0^*)$,其中 $H_4(m_w^* \| y_0^* \| P_0^* \| ID_0^*) = h_0^* \neq h_0^{*\prime} = H_4'(m_w^* \| y_0^* \| P_0^* \| ID_0^*)$。查询 H_2 列表获得 $T_0^* = \beta^* P$。

于是,Σ 得到方程组:

$$y_0^* = e(K_0^*, P)[e(Q_0^*, P_{pub}) e(P_0^*, T_0^*)]^{h_0^*}$$

$$y_0^* = e(K_0^{*\prime}, P)[e(Q_0^*, P_{pub}) e(P_0^*, T_0^*)]^{h_0^{*\prime}}$$

得出 $e(K_0^* - K_0^{*\prime}, P) = [e(Q_0^*, P_{pub}) e(P_0^*, T_0^*)]^{h_0^* - h_0^{*\prime}}$

解出

$$abP = (h_0^{*\prime} - h_0^*)^{-1}(K_0^* - K_0^{*\prime}) - \alpha_k P_1 - \beta^* P_0^*$$

b)若 A_1 输出$(m_w^*, P_0^*, \sigma_{02}^* = (y^*, W^*), ID_0^*)$且满足第 1 章中的情形 1。

过程完全同 a)。

c)若 A_1 输出$(m^*, m_w^*, P_0^*, L_{ID}^*, L_{PK}^*, y^*, W^*, \sigma^* = (y_0^*, y_1^*, y_2^*, \cdots, y_n^*, V^*), ID_0^*)$且满足第 1 章中的情形 2。

若 $ID_0^* \neq ID_k$,Σ 终止协议。若 $ID_0^* = ID_k$,据 Forking lemma[15],过程同 a),可得到另一个有效的伪造元组$(m^*, m_w^*, P_0^*, L_{ID}^*, L_{PK}^*, y^*, W^*, \sigma^{*\prime} = (y_0^*, y_1^*, y_2^*, \cdots, y_n^*, V^{*\prime}), ID_0^*)$,$H_4(m_w^* \| y_0^* \| P_0^* \| ID_0^*) = h_0^* \neq h_0^{*\prime} = H_4'(m_w^* \| y_0^* \| P_0^* \| ID_0^*)$。查询 H_2 列表获得 $T_0^* = \beta^* P$。

Σ 解出 $abP = (h_0^{*\prime} - h_0^*)^{-1}(V^* - V^{*\prime}) - \alpha_k P_1 - \beta^* P_0^*$。

d)若 A_1 输出$(m^*, m_w^*, P_0^*, L_{ID}^*, L_{PK}^*, y^*, W^*, \sigma^* = (y_0^*, y_1^*, y_2^*, \cdots, y_n^*, V^*), ID_0^*)$且满足第 1 章中的情形 3。

若 $ID_k \in L_{ID}^*$,Σ 终止协议。若 $ID_k \in L_{ID}^*$,不妨设 ID_k 在环签名中的下标为 $s \in \{1,2,\cdots,n\}$。据 Ring Forking lemma[16],若 A_1 在上述攻击交互时间 t 内能以至少 $\varepsilon \geqslant 7 \times A(q_5, n) \times 2^{-l}$的概率输出有效代理环签名,则 Σ 选择不同的哈希函数 H_5' 并再次利用 A_1 的能力,在不超过 $2t$ 的时间内以至少 $\varepsilon^2[66A(q_5, n)]^{-1}$的概率,可得到另一个有效的伪造元组$(m^*, m_w^*, P_0^*, L_{ID}^*, L_{PK}^*, y^*, W^*, \sigma^{*\prime} = (y_0^*, y_1^*, y_2^*, \cdots, y_n^*, V^{*\prime}), ID_0^*)$,有 $H_5(m^* \| m_w^* \| y_0^* \| y_s^* \| P_s^* \| ID_s^*) = h_s^* \neq h_s^{*\prime} = H_5'(m^* \| m_w^* \| y_0^* \| y_s^* \| P_s^* \| ID_s^*)$,对任意的 $i \in \{1,2,\cdots,n\} \setminus \{s\}$,总有 $h_i^* =$

$h_i^{*'}$。查询 H_3 列表获得 $U=\gamma^* P$。

Σ 解出 $abP=(h_s^{*'}-h_s^*)^{-1}(V^*-V^{*'})-\alpha_k P_1-\gamma^* P_s^*$。

成功概率分析:Σ 能解决给定的 CDH 问题,需要下面事件同时满足。

C_1:协议没有在部分私钥和代理钥询问时终止。

C_2:A_1 对部分代理钥或代理环签名伪造是成功的。

C_3:下列事件有其一发生。

a)A_1 输出有效元组$(m_w^*, P_0^*, \sigma_{01}^*=(y_0^*, K_0^*), \mathrm{ID}_0^*)$且 $\mathrm{ID}_0^*=\mathrm{ID}_k$。

b)A_1 输出有效元组$(m_w^*, P_0^*, \sigma_{02}^*=(y^*, W^*), \mathrm{ID}_0^*)$且 $\mathrm{ID}_0^*=\mathrm{ID}_k$。

c)A_1 输出有效元组$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, y^*, W^*, \sigma^*=(y_0^*, y_1^*, y_2^*, \cdots, y_n^*, V^*), \mathrm{ID}_0^*)$且 $\mathrm{ID}_0^*=\mathrm{ID}_k$。

d)A_1 输出有效元组$(m^*, m_w^*, P_0^*, L_{\mathrm{ID}}^*, L_{PK}^*, y^*, W^*, \sigma^*=(y_0^*, y_1^*, y_2^*, \cdots, y_n^*, V^*), \mathrm{ID}_0^*)$且 $\mathrm{ID}_k \in L_{\mathrm{ID}}^*$。

C_4:Forking lemma 实施成功。

Σ 成功的概率是 $P(C_1\cap C_2\cap C_3\cap C_4)=P(C_1)Pr(C_2\mid C_1)P(C_3\mid C_2\cap C_1)P(C_4\mid C_3\cap C_2\cap C_1)$。$P(C_1)\geqslant(1-q_1^{-1})^{q_6+q_{10}}$,$P(C_2\mid C_1)\geqslant\varepsilon$,$P(C_3\mid C_2\cap C_1)\geqslant q_1^{-1}$,$P(C_4\mid C_3\cap C_2\cap C_1)\geqslant\varepsilon^2[66A(q_5,n)]^{-1}$。

$$Pr(C_1\cap C_2\cap C_3\cap C_4)=\varepsilon'\geqslant \varepsilon^2(66A(q_5,n))^{-1}q_1^{-1}(1-q_1^{-1})^{q_6+q_{10}}$$

Σ 需要的时间 $t'\leqslant 2t+23tR\varepsilon^{-1}+q_1t_1+q_2t_2+q_3t_3+q_4t_4+q_5t_5+q_6t_6+q_7t_7+q_8t_8+q_9t_9+q_{10}t_{10}+q_{11}t_{11}$。

定理 2　在随机预言模型下,如果 A_{II} 至多进行 q_1 次生成用户询问,q_2 次 H_2 询问,q_3 次 H_3 询问,q_4 次 H_4 询问,q_5 次 H_5 询问,q_6 次公钥替换询问,q_7 次秘密值询问,q_8 次部分代理钥询问,q_9 次代理钥询问,q_{10}次代理环签名询问后,在时间 t 内以不可忽略的概率 $\varepsilon>0$ 攻破提出的方案,那么存在一个算法 Σ 以概率 $\varepsilon'\geqslant\varepsilon^2(66A(q_5,n))^{-1}q_1^{-1}(1-q_1^{-1})^{q_6+q_7+q_9}$,在时间 $t'\leqslant 2t+23tR\varepsilon^{-1}+q_1t_1+q_2t_2+q_3t_3+q_4t_4+q_5t_5+q_6t_6+q_7t_7+q_8t_8+q_9t_9+q_{10}t_{10}$内解决 CDH 问题。其中 $t_1\sim t_{10}$含义类似于定理 1。

定理 2 的证明过程类似于定理 1,不再赘述。

3.3　效率

记 Bp 表示双线性映射运算,Sm 表示 G_1 上的标量乘运算,H 表示 $\{0,1\}^*\rightarrow G_1^*$ 上的 hash 函数运算。代理环签名方案的效率应主要考虑代理环签名生成与验证的计算量,注意到诸如 $H_1(\mathrm{ID}_0)$,$H_2(P_0\|\mathrm{ID}_0)$,$e(Q_0,P_{\mathrm{pub}})$,$e(W,P)$,$e(P_0,T_0)$可以预运算。如表 1 所示,本方案实现了所需 Bp 个数与代理环的规模无关,具有计算上的优势。另外,它可以抵抗超级攻击者的攻击,具有安全性强的优势。

表 1　效率

计算方式	代理环签名	代理环签名验证
不除去预运算	$2Bp+(2n+1)Sm+nH$	$7Bp+(2n+1)Sm+(n+3)H$
除去预运算	$2Bp+(2n+1)Sm+nH$	$3Bp+2nSm+(n+1)H$

4　结束语

为满足以匿名方式实现代理签名的实际需求,本文研究了新兴无证书密码系统下的代理环签名和相应的安全模型问题。由于该类型方案涉及到的成员众多,刻画适当是安全模型尤为关键的问题,本文在这方面进行了尝试。分析表明该方案不仅具有计算效率上的优势,而且具有安全性强的优点,它可广泛应用于电子拍卖、电子政务等场合。然而,如何构造签名长度固定且较小的代理环签名方案仍然是一个公开问题。

参考文献:

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans on Fundamentals, 1996, E79-A(9): 1338-1353.

[2] RIVEST R, SHAMIRE A, TAUMAN Y. How to leak a secret[C]// Proc of ASIACRYPT. Berlin: Springer, 2001: 552-565.

[3] ZHANG Fang-guo, SAFAVI-NAINI R, LIN Chin-yin. Some new proxy signature schemes from pairings[M]//Progress on Cryptography: 25 Years of Cryptography in China. Shanghai: Shanghai Jiaotong University Press, 2004: 59-66.

[4] LI Jin, CHEN Xiao-feng, TSZ H Y, *et al*. Proxy ring signature: formal definitions, efficient construction and new variant[C]//Proc of International Conferenceon Computational Inteuigence and Security. 2007: 545-555.

[5] 禹勇,杨波,李发根,等. 一个有效的代理环签名方案[J]. 北京邮电大学学报,2007,30(3):23-26.

[6] AMIT K, SUNDER L. ID-based ring signature and proxy ring signature schemes from bilinear pairings[J]. Internal Journal of Network Security, 2007, 4(2): 187-192.

[7] 张建中,薛荣红,彭丽慧. 一种基于身份的代理环签名方案[J]. 计算机工程,2011,37(17):126-127.

[8] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[C]//Proc of ASIACRYPT. Berlin: Springer-Verlag, 2003: 452-473.

[9] 陈虎,朱昌杰,宋如顺. 高效的无证书签名和群签名方案[J]. 计算机研究与发展,2010,47(2):231-237.

[10] HUANG Xin-yi, MU Yi, SUSILO W, *et al*. Certificateless signature revisited[C]//Lecture Notes in Computer Science, vol 4586. 2007: 308-322.

[11] 陈虎,张福泰,宋如顺. 可证安全的无证书代理签名方案[J]. 软件学报,2009,20(3):692-701.

[12] ZHANG Lei, ZHANG Fu-tai, WU Wei. A provably secure ring signature scheme in certificateless cryptography[C]//Lecture Notes in Computer Science, vol 4784. 2007: 103-121.

[13] 张俊茸,任平安,李文莉. 一种新的无证书的代理环签名方案[J]. 计算机工程与应用,2012,48(2):63-65.

[14] 王会歌,沈峰,赵靖,等. 不使用双线性对的无证书代理环签名方案[J]. 安徽科技学院学报,2011,25(4):45-48.

[15] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[16] HERRANZ J, SAEZ G. New identity-based ring signature schemes[C]//Lecture Notes in Computer Science, vol 3269. 2004: 27-39.