软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(5):1173−1180 [doi: 10.13328/j.cnki.jos.004654]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

安全的无证书聚合签名方案*

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)

通讯作者: 陈虎, E-mail: chenhuchh@163.com

摘 要: 无证书密码系统既解决了密钥托管问题,又不涉及公钥证书;而聚合签名可以有效地减少计算代价和通信开销.结合二者的优点构造无证书聚合签名是很有意义的.尽管无证书聚合签名方案的构造已经取得了重要进展,但是现有的方案仍然不能同时达到既可抵抗两类超级攻击者又具有运算的高效性.使用双线性映射并引入状态信息来设计具有强安全性的无证书聚合签名方案.在随机预言模型中,该状态信息被用于嵌入给定困难问题的部分信息.结果显示,该方案的安全性基于计算 Diffie-Hellman 问题的困难性并可以抵抗超级攻击者的攻击.同时,由于充分利用公开信息和双线性映射的性质,它在个体签名和聚合签名验证过程只需 4 个双线性映射.另外,在该方案中,用户知道状态信息后可独立完成个体签名而无需交换信息,所以它允许用户动态地加入聚合签名.故它可应用于多对一的通信系统中.

关键词: 无证书密码系统;聚合签名;计算 Diffie-Hellman 问题;双线性映射;随机预言模型

中图法分类号: TP309

中文引用格式: 陈虎,魏仕民,朱昌杰,杨忆.安全的无证书聚合签名方案.软件学报,2015,26(5):1173−1180. http://www.jos.org.cn/1000-9825/4654.htm

英文引用格式: Chen H, Wei SM, Zhu CJ, Yang Y. Secure certificateless aggregate signature scheme. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1173−1180 (in Chinese). http://www.jos.org.cn/1000-9825/4654.htm

Secure Certificateless Aggregate Signature Scheme

CHEN Hu, WEI Shi-Min, ZHU Chang-Jie, YANG Yi

(School of Computer Science and Technology, Huaibei Normal University, Huaibei 235000, China)

Abstract: Certificateless public key cryptography can solve the key escrow problem without any digital certificates to bind users and their public keys. Meanwhile, aggregate signature can efficiently lower the cost of computations and communications. Hence it is of interest to construct a certificateless aggregate signature scheme by taking advantages of the two methods. Though great progress has been made in this area, certificateless aggregate signature schemes available today cannot simultaneously achieve the objectives of being secure against both types of super adversaries and being efficient in operation. This paper puts forward a construction of certificateless aggregate signature scheme with stronger security by using pairings and introducing state information. The state information is used to hold partial information on a given hard problem in the random oracle model. The results show that the presented scheme, based on the infeasibility of the computational Diffie-Hellman (CDH) problem, is secure against both super adversaries. At the same time, the new scheme needs only four pairings during the processes of individual signature and verification for an aggregate signature by making good use of public information and the properties of bilinear maps. Furthermore, after knowing the same state information, a user in the scheme can perform individual signature operations in a non-interactive manner, which allows any users in the system to join dynamically for generating an aggregate signature. As a result, it can have practical applications in many-to-one communications.

Key words: certificateless cryptography; aggregate signature; computational Diffie-Hellman problem; bilinear map; random oracle model

* 基金项目: 国家自然科学基金(61472309, 61173151, 60673070, 60773121); 安徽省自然科学基金(1208085MF108); 安徽省高校自然科学基金(KJ2012B157)

收稿时间: 2012-08-03; 定稿时间: 2014-05-21

2003 年,Al-Riyami 等人[1]首次提出无证书密码体制.该体制不但成功地解决了密钥托管问题,而且不涉及公钥证书.这使它成为近期一个研究热点,似雨后春笋般地涌出众多满足不同需求的无证书签名方案[2−6],如无证书代理签名方案[3]、无证书群签名方案[4]、无证书聚合签名方案[5−9].

聚合签名[10]是把来自 n 个不同签名者对 n 条不同消息的签名通过一种有效的算法压缩成单个签名.持有聚合签名的验证人可通过确定的验证算法检验其有效性,以此判定 n 个签名人对这 n 条消息的分别认可.故而,聚合签名可以有效地减少签名验证的计算代价和通信开销.

近年来,各具特色的无证书聚合签名方案[5−9]陆续被提出来,其中,文献[6,9]中方案的聚合签名验证计算量和聚合签名的长度均与聚合人数无关,但前者每次都要协商新的状态信息,后者完成个体签名时需要用户之间互相传递必须的数据,这些都会引起额外的通信开销致使方案低效.另外,上述除文献[8]以外的无证书聚合签名方案所给出的安全模型中的攻击者[1]能力相对较弱.虽然文献[8]中的攻击者能力得以加强,使之成为超级攻击者[2],但是签名验证计算量很大.本文提出一个在聚合签名验证阶段只需 4 个双线性运算的无证书聚合签名方案.它在保证较高效率的基础上,实现了在最强安全模型(即,赋予攻击者最强的攻击能力)下是可证安全的.受文献[6]的启发,我们的方案也选择使用一个共同的状态信息,以实现强安全性的聚合签名方案的设计.与文献[9]中方案的显著区别是,在我们的方案中,参与聚合的用户之间独立地完成个体签名,无需交换彼此的数据.因此,我们的聚合方案可方便地实现系统内的用户动态地加入完成聚合签名.

本文第 1 节给出无证书聚合签名的概念和安全模型.第 2 节提出一个无证书聚合签名方案.第 3 节分析方案的安全性和效率.最后总结全文.

1 有关的概念和安全模型

无证书聚合签名方案包含了 n 个用户、一个密钥生成中心(KGC)和一个聚合者,它由系统参数生成、部分私钥提取、设置公/私钥、个体签名、聚合和聚合签名验证等 6 个算法组成.各算法的定义参见文献[5].

无证书聚合签名中存在两类攻击者,即第一类攻击者 A_{I} 和第二类攻击者 A_{II}.文献[1]最初赋予攻击者的能力为"A_{I} 不能获知系统主密钥,但可在公钥空间随意取值以替代任何用户的公钥;A_{II} 可获知系统主密钥,但不能替换任何用户的公钥."后来,文献[2]不仅对 A_{II} 能力作了增强——"可获知系统主私钥,可替换除了目标用户之外的任何用户的公钥",而且对安全模型中所定义的签名预言器按能力强弱分为正常、强和超级这 3 种签名预言器.进而,每种类型的攻击者依据被允许访问签名预言器的类型进一步分为正常、强和超级攻击者.具体细节见表 1 和表 2.

Table 1 Types of attackers

表 1 攻击者类型

类型	第一类			第二类		
	正常攻击者	强攻击者	超级攻击者	正常攻击者	强攻击者	超级攻击者
能力	不能获知系统主密钥,但可以替换系统中任何用户的公钥			可以获知系统主密钥,可以替换系统中除了目标身份以外的任何用户的公钥		
配置的签名预言器	$\mathcal{O}_1$	$\mathcal{O}_2$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_2$	$\mathcal{O}_3$

Table 2 Types of oracles

表 2 签名预言器类型

正常签名预言器$\mathcal{O}_1$	输入:身份 ID,消息 m;$\mathcal{O}_1$ 输出有效签名 σ.这里的签名要使用身份 ID 在"用户生成算法中产生的秘密值和部分私钥"来生成;验证签名 σ 有效性要使用"用户生成算法中产生的公钥"完成.
强签名预言器$\mathcal{O}_2$	输入:身份 ID,消息 m,秘密值 x;$\mathcal{O}_2$ 输出有效签名 σ.若攻击者没有提供秘密值 x,则 $\mathcal{O}_2$ 的签名使用身份 ID 在"用户生成算法中产生的秘密值和部分私钥"来生成;验证签名 σ 有效性使用"用户生成算法中产生的公钥"完成.若攻击者提供了秘密值 x,则 $\mathcal{O}_2$ 的签名使用身份 ID 在"用户生成算法中产生的部分私钥和攻击者所提供的秘密值 x"来生成;验证签名 σ 有效性使用"该秘密值所对应的公钥"完成.
超级签名预言器$\mathcal{O}_3$	输入:身份 ID,消息 m;$\mathcal{O}_3$ 输出有效签名 σ.验证签名 σ 有效性使用"该用户当前的公钥"完成.这里,"当前的公钥"是指用户公钥列表上的最新记录.换句话说,若该用户的公钥截止当前已被替换了 $k\geqslant 0$ 次,则使用第 k 次替换的公钥去验证签名.特殊地,k=0 表示公钥没有被替换.

为了方便下面方案之间安全性的比较,本文把具有文献[1]所赋予的攻击能力并且只允许访问正常签名预言器的攻击者称为弱正常攻击者.

无证书聚合签名的不可伪造性是通过一个解决困难问题的挑战者 Q 和一个攻击者 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$之间的游戏来定义.本文考虑的攻击者为超级攻击者,对其他类型攻击者,只需相应地修改签名询问过程.

- 设置系统参数:Q 初始化系统,以安全参数 ℓ 作为输入,输出参数列表 List.若 A 是 A_{I},则 Q 把 List 给 A;否则,Q 把 List∪{系统主密钥}给 A.
- 攻击:A 被允许受限次地访问受控于 Q 的预言器(和可能存在的 hash 函数预言器).另外,Q 要维护和 A 交互过程中涉及到的数据所形成的一些列表,这些列表初始均为空表:
  - 生成用户询问:输入 List,一个身份 ID,它输出该用户的公钥 P_{ID} 和身份 ID 的哈希值 Q_{ID}.
  - 部分私钥询问(仅对 A_{I} 有效):输入 List 和一个用户的身份 ID,它输出其部分私钥 D_{ID}.
  - 公钥替换询问:输入 List,一个用户的身份 ID 和新公钥 P'_{ID},它把身份 ID 的公钥置为 P'_{ID}.
  - 秘密值询问:输入 List,一个用户的身份 ID,它输出其秘密值 x_{ID}.
  - 个体签名询问:输入 List、消息 m、状态信息 Δ、签名者的身份 ID 和公钥 P_{ID},它输出有效的个体签名 δ.若公钥已被替换,攻击者不必提供相应的秘密值.
- 伪造:攻击者 A 输出在相同状态信息 Δ^* 下,公钥集是 $L^*_{PK}=\{P_1^*,P_2^*,...,P_n^*\}$、身份集是 $L^*_{\mathrm{ID}}=\{ID_1^*,ID_2^*,...,ID_n^*\}$ 的 n 个用户对消息 $m_1^*,m_2^*,...,m_n^*$ 的聚合签名 $\sigma^*=(R_1^*,R_2^*,...,R_n^*,K^*)$ 作为伪造.A 在游戏中获胜,当且仅当同时满足如下两个条件:

  (1) $1\leftarrow verify(List,\Delta^*,m_1^*,...,m_n^*,L^*_{PK},L^*_{\mathrm{ID}},\sigma^*)$.

  (2) 至少存在一个身份 $ID_j^*\in L^*_{\mathrm{ID}}$ 未对 $(\Delta^*,m_j^*,ID_j^*,P_j^*)$ 做个体签名询问.同时,当 A 是 A_{I} 时,则未曾做 ID_j^* 的部分私钥询问;否则,未曾做 ID_j^* 的秘密值询问,也未曾做 ID_j^* 公钥替换询问.

在游戏中,若任何多项式有界的攻击者 $A\in\{A_{\mathrm{I}},A_{\mathrm{II}}\}$获胜的概率是可忽视的,则称此无证书聚合签名方案是自适应选择消息和身份攻击存在不可伪造的.

另外,因攻击者获得个体签名后可以自己生成聚合签名,故我们的安全模型无需进行聚合签名询问.

2 无证书聚合签名方案

受文献[6]的启发,我们在构造聚合签名方案时也引入了状态信息,为了增强方案的安全性以抵抗超级攻击者的攻击.聚合者在个体签名前随机选取并广播状态信息,这里状态信息可选择随机长度的比特串.

- 系统参数的生成:设安全参数为 ℓ,素数 $q\geqslant 2^{\ell}$,$(G_1,+)$和$(G_2,\cdot)$是循环群,其阶均为 q.双线性映射 $e:G_1\times G_1\rightarrow G_2$. $H_1,H_2,H_3:\{0,1\}^*\rightarrow G_1^*$;$H_4,H_5:\{0,1\}^*\rightarrow\mathbb{Z}_q^*$ 是 5 个抗碰撞的哈希函数.P 是 G_1 的一个生成元,KGC 设置系统主密钥 $s\in_R\mathbb{Z}_q^*$,系统公钥为 $P_0=sP$,消息空间 $\mathcal{M}=\{0,1\}^*$,公开参数:

  $$\mathrm{List}=\{G_1,G_2,e,q,P,P_0,H_1,H_2,H_3,H_4,H_5\}.$$

- 部分私钥提取:KGC 对用户所提交的身份 $ID_i\in\{0,1\}^*$ 认证后,为其计算部分私钥 $D_i=sQ_i=sH_1(ID_i)$,并安全地传 D_i 给该用户.
- 设置公/私钥:用户 ID_i 选 $x_i\in_R\mathbb{Z}_q^*$,计算 $P_i=x_iP$.这里,P_i 为公钥,(x_i,D_i)为私钥,x_i 作为其秘密值.
- 个体签名:聚合者随机选择一个状态信息 Δ 并广播.公钥和身份分别为 P_i 与 ID_i 的用户,用其私钥 (x_i,D_i),按如下步骤对消息 m_i 签名,其中,$i=1,2,\ldots,n$:

  ① 任选 $r_i\in_R\mathbb{Z}_q^*$,计算 $R_i=r_iP,h_i=H_4(m_i\|\Delta\|R_i\|ID_i)$和 $g_i=H_5(m_i\|\Delta\|R_i\|P_i)$;

  ② 计算 $W_i=g_iD_i+x_ih_iU+r_iV$,其中,$U=H_2(\Delta\|P),V=H_3(\Delta\|P_0)$;

  ③ 输出 $\sigma_i=(R_i,W_i)$为个体签名.
- 聚合:设 $L_{\mathrm{ID}}=\{ID_1,ID_2,\ldots,ID_n\}$是参与聚合的 n 个用户的身份集,公钥集是 $L_{PK}=\{P_1,P_2,\ldots,P_n\}$.当收齐这

n 个用户在相同状态信息Δ下的消息-签名对$(m_1,\sigma_1),(m_2,\sigma_2),\ldots,(m_n,\sigma_n)$后,聚合者计算 $W=W_1+W_2+\ldots+W_n$ 并输出聚合签名$\sigma=(R_1,R_2,\ldots,R_n,W)$.

- 聚合签名验证:在状态信息Δ下,欲验证身份集是 $L_{ID}=\{ID_1,ID_2,\ldots,ID_n\}$,公钥集是 $L_{PK}=\{P_1,P_2,\ldots,P_n\}$的 n 个用户对消息 $m_1,m_2,\ldots,m_n$ 的聚合签名$\sigma=(R_1,R_2,\ldots,R_n,W)$,验证者按如下步骤进行检验:

  ① 计算 $U=H_2(\Delta\|P),V=H_3(\Delta\|P_0),h_i=H_4(m_i\|\Delta\|R_i\|ID_i),g_i=H_5(m_i\|\Delta\|R_i\|P_i),Q_i=H_1(ID_i),i=1,2,\ldots,n$;

  ② 验证 $e(W,P)=e\left(\sum_{i=1}^{n}g_iQ_i,P_0\right)e\left(\sum_{i=1}^{n}h_iP_i,U\right)e\left(\sum_{i=1}^{n}R_i,V\right)$ 是否为真:若真,则接受σ,否则,拒绝σ.

3 安全性和效率

3.1 正确性

下面证明方案是正确的.

$$\begin{aligned}e(W,P)&=e\left(\sum_{i=1}^{n}W_i,P\right)\\&=e\left(\sum_{i=1}^{n}(g_iD_i+x_ih_iU+r_iV),P\right)\\&=e\left(\sum_{i=1}^{n}g_iD_i,P\right)e\left(\sum_{i=1}^{n}x_ih_iU,P\right)e\left(\sum_{i=1}^{n}r_iV,P\right)\\&=e\left(\sum_{i=1}^{n}g_iQ_i,P_0\right)e\left(\sum_{i=1}^{n}h_iP_i,U\right)e\left(\sum_{i=1}^{n}R_i,V\right).\end{aligned}$$

3.2 不可伪造性

符号 $Query_A^t(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9)$ 表示在时间 t 内,攻击者 A 被允许至多做 x_1 次生成用户询问、x_2 次 H_2 询问、x_3 次 H_3 询问、x_4 次 H_4 询问、x_5 次 H_5 询问、x_6 次部分私钥询问、x_7 次公钥替换询问、x_8 次秘密值询问、x_9 次个体签名询问.上述 9 种询问中,每种询问一次的耗时依次记为 $t_1,t_2,t_3,t_4,t_5,t_6,t_7,t_8$ 和 t_9.符号 $A(n,m)$表示从 m 个不同事物中选出 n 个物体的排列数,其中 $n\leqslant m$ 且 $n,m\in\mathbb{N}$.用(t,ε)-CDH 表示给定的 CDH 问题可在 t 时间内以概率ε解决.

定理 1. 在随机预言模型下,如果A_1是第一类超级攻击者,做自适应选择消息和身份攻击询问 $Query_{A_1}^t(q_1,q_2,q_3,q_4,q_5,q_6,q_7,q_8,q_9)$后,以不可忽略的概率 $\varepsilon\geqslant 7A(n,q_5)\cdot 2^{-\ell}$ 攻破所提出的方案,那么存在一个(t',ε')-CDH 算法 Q,其中,$t'\leqslant 2t+2\sum_{i=1}^{9}q_it_i,\varepsilon'\geqslant[66\cdot A(n,q_5)]^{-1}\cdot q_1^{-2}(1-q_1^{-1})^{q_6}\cdot\varepsilon^2$.

证明:若有$(G_1,+)$上的 CDH 问题的一个随机实例$(P,P_1=aP,P_2=bP)$,该困难问题的解决者是 Q,则其目标是算出 abP.下证凭借 A_1 的能力,Q 是一个(t',ε')-CDH 的挑战者.

- 设置系统参数:Q 置 $P_0=P_1=aP$ 并把 List=$\{G_1,G_2,e,q,P,P_0,H_1,H_2,H_3,H_4,H_5\}$给 A_1.
- 攻击:抗碰撞的哈希函数 H_1~H_5 受控于 Q,它们被作为随机预言器.为简单,假设 A_1 的询问都是不同的.Q 维护 H_1~H_5 和 L 等列表,它们初始都为空.这些列表中每项的格式依次为$(ID_i,Q_i,P_i,D_i,\alpha_i,x_i),(\Delta_i,U_i,\beta_i),(\Delta_i,V_i,\lambda_i),(m_i,\Delta_i,R_i,ID_i,h_i),(m_i,\Delta_i,R_i,P_i,g_i),(m_i,\Delta_i,ID_i,P_i,R_i,r_i,h_i,g_i,W_i)$.
- 生成用户询问:Q 随机选择 $k\in\{1,2,\ldots,q_1\}$.当 A_1 询问 Create(ID_i)时,Q 选择 $x_i,\alpha_i\in_R\mathbb{Z}_q^*$ 满足(*,*,*,*,α_i,*)以前未出现在 H_1 列表.当 $i=k$ 时,置 $Q_k=\alpha_kP+P_2,D_k=\perp$(符号$\perp$表示该值未知,下同),$P_k=x_kP$;当 $i\neq k$ 时,置 $Q_i=\alpha_iP,P_i=x_iP,D_i=\alpha_iP_1$.$Q$ 将$(ID_i,Q_i,P_i,D_i,\alpha_i,x_i)$添加到 H_1 列表,并把 P_i,Q_i 返给 A_1.

不失一般性,下面 A_1 询问所涉及的 ID_i 均已生成.

- 部分私钥询问:当 A_1 询问 PPKey(ID_i)时,Q 执行:当 $i=k$ 时,终止协议;否则,检查 H_1 列表寻找元组$(ID_i,Q_i,P_i,D_i,\alpha_i,x_i)$,将 D_i 返给 A_1.
- 公钥替换询问:当 A_1 询问 Replace(ID_i,P_i') 时,Q 据 ID_i 检查 H_1 列表,把元组$(ID_i,Q_i,P_i,D_i,\alpha_i,x_i)$替换为$(ID_i,Q_i,P_i',D_i,\alpha_i,\perp)$.
- 秘密值询问:当 A_1 询问 Value(ID_i)时,Q 据 ID_i 检查 H_1 列表:若 $x_i\neq\perp$,则返回 x_i 给 A_1;否则,输出$\perp$.

- H_2 哈希询问:当 A_I 询问 $H_2(\Delta\|P)$时,Q 选择 $x_i,\alpha_i \in_R \mathbb{Z}_q^*$ 满足$(*,*,\beta_i)$未出现在 H_2 列表,将 $U_i=\beta_i P$ 返给 A_I 并把(Δ_i,U_i,β_i)添入 H_2 列表.
- H_3 哈希询问:当 A_I 询问 $H_3(\Delta_i\|P_0)$时,Q 选择 $\lambda_i \in_R \mathbb{Z}_q^*$ 满足$(*,*,\lambda_i)$未出现在 H_3 列表,将 $V_i=\lambda_i P-P_1$ 返给 A_I 并添(Δ_i,V_i,λ_i)到 H_3 列表.
- H_4 哈希询问:当 A_I 询问 $H_4(m_i\|\Delta\|R_i\|ID_i)$时,$Q$ 选择 $h_i \in_R \mathbb{Z}_q^*$ 满足$(*,*,*,*,h_i)$未出现在 H_4 列表,将 h_i 返给 A_I 并添$(m_i,\Delta_i,R_i,ID_i,h_i)$到 H_4 列表.
- H_5 哈希询问:当 A_I 询问 $H_5(m_i\|\Delta\|R_i\|P_i)$时,$Q$ 选择 $g_i \in_R \mathbb{Z}_q^*$ 满足$(*,*,*,*,g_i)$未出现在 H_5 列表,将 g_i 返给 A_I,并把$(m_i,\Delta_i,R_i,P_i,g_i)$添入 H_5 列表.
- 个体签名询问:当 A_I 询问 Sign(m_i,Δ_i,ID_i,P_i)时,Q 查询 H_2,H_3 列表以分别获得 $U_i=\beta_i P$ 和 $V_i=\lambda_i P-P_1$.
  Q 执行如下步骤:
  (1) 任选 $r_i,h_i,g_i \in_R \mathbb{Z}_q^*$ 满足$(*,*,*,*,h_i)$和$(*,*,*,*,g_i)$分别未出现在 H_4 和 H_5 列表.
  (2) 计算 $R_i=r_i P+g_i Q_i$,并置 $H_4(m_i\|\Delta\|R_i\|ID_i)=h_i$ 和 $H_5(m_i\|\Delta\|R_i\|P_i)=g_i$.
  (3) 计算 $W_i=h_i\beta_i P_i+\lambda_i g_i Q_i+\lambda_i r_i P-r_i P_1$.
  Q 把$(m_i,\Delta_i,ID_i,P_i,R_i,r_i,h_i,g_i,W_i)$添入 L 列表并以 R_i,W_i 作答.由设定 $P_0=P_1$ 和个体签名验证算法可知,该返回值(R_i,W_i)是关于(m_i,Δ_i,ID_i,P_i)的一个有效签名,因为

$$\begin{aligned} e(g_iQ_i,P_0)e(h_iP_i,U)e(R_i,V) &= e(g_iQ_i,P_1)e(h_iP_i,\beta_iP)e(r_iP+g_iQ_i,\lambda_iP-P_1)\\ &= e(h_i\beta_iP_i+\lambda_ig_iQ_i+r_i\lambda_iP-r_iP_1,P)\\ &= e(W_i,P). \end{aligned}$$

- 伪造:A_I 输出公钥集是 $L_{PK}^*=\{P_1^*,P_2^*,...,P_n^*\}$、身份集是 $L_{ID}^*=\{ID_1^*,ID_2^*,...,ID_n^*\}$ 的 n 个用户在相同状态信息Δ^*下对消息 $m_1^*,m_2^*,...,m_n^*$ 的聚合签名 $\sigma^*=(R_1^*,R_2^*,...,R_n^*,W^*)$,且同时满足如下条件:
  (1) $e(W^*,P)=e\left(\sum_{i=1}^n g_i^*Q_i^*,P_0\right)e\left(\sum_{i=1}^n h_i^*P_i^*,U^*\right)e\left(\sum_{i=1}^n R_i^*,V^*\right)$.
  (2) 至少存在一个身份 $ID_j^*\in L_{ID}^*$,既未对它做部分私钥询问,也未对 $(\Delta^*,m_j^*,ID_j^*,P_j^*)$ 做个体签名询问.
  Q 只把哈希函数 H_5 替换为 H_5',其余保持不变.重复上述交互过程.由 Forking lemma[11]可知:在不大于 $2t$ 时间内,借助 A_I 的能力以不低于 $\varepsilon^2\cdot[66\cdot A(n,q_5)]^{-1}$ 的概率,获得一个新的有效的伪造元组 $\sigma^{*\prime}=(R_1^*,R_2^*,...,R_n^*,W^{*\prime})$,其中存在 $s\in\{1,2,\ldots,n\}$,当 $i\in\{1,2,\ldots,n\}\backslash\{s\}$时,总有 $g_i^*=g_i^{*\prime}$;但当 $i=s$ 时,有:

$$H_5(m_s^*\|\Delta^*\|R_s^*\|P_s^*)=g_s^*\neq g_s^{*\prime}=H_5'(m_s^*\|\Delta^*\|R_s^*\|P_s^*).$$

于是,Q 得到方程组:

$$\begin{cases} e\left(\sum_{i=1}^n g_i^*Q_i^*,P_0\right)e\left(\sum_{i=1}^n h_i^*P_i^*,U^*\right)e\left(\sum_{i=1}^n R_i^*,V^*\right)=e(W^*,P)\\ e\left(\sum_{i=1}^n g_i^{*\prime}Q_i^*,P_0\right)e\left(\sum_{i=1}^n h_i^*P_i^*,U^*\right)e\left(\sum_{i=1}^n R_i^*,V^*\right)=e(W^{*\prime},P) \end{cases}.$$

两式相除,得到:

$$e((g_s^*-g_s^{*\prime})Q_s^*,P_0)=e(W^*-W^{*\prime},P).$$

- ✓ 若 $ID_j^*=ID_k=ID_s^*$,则 $Q_s^*=Q_k=\alpha_kP+P_2$,解出 $abP=(g_s^*-g_s^{*\prime})^{-1}(W^*-W^{*\prime})-\alpha_kP_1$;
- ✓ 否则,Q 终止协议.

- 成功概率:Q 成功解决给定的 CDH 问题可转化为以下 3 个事件的发生:
  - ➢ S_1:协议未终止于部分私钥询问.
  - ➢ S_2:聚合签名被 A_I 成功地伪造且 Forking Lemma 应用成功.
  - ➢ S_3:满足 $ID_j^*=ID_k=ID_s^*$.

Q 解决 CDH 问题的概率是 $P(S_1\cap S_2\cap S_3)=P(S_1)P(S_2|S_1)P(S_3|S_1\cap S_2)$,其中,$P(S_1)\geqslant(1-1/q_1)^{q_0}$,$P(S_2|S_1)\geqslant$

$\varepsilon^2\cdot[66\cdot A(n,q_5)]^{-1}$ 且 $\mathrm{P}(S_3\mid S_1\cap S_2)\geqslant q_1^{-2}$, 即, $\varepsilon'\geqslant[66\cdot A(n,q_5)]^{-1}\cdot q_1^{-2}(1-q_1^{-1})^{q_6}\cdot\varepsilon^2$. □

定理 2. 在随机预言模型下,如果 A_{II} 是第二类超级攻击者,做自适应选择消息和身份攻击询问 $Query^t_{A_{\mathrm{II}}}(q_1, q_2,q_3,q_4,q_5,q_6,q_7,q_8,q_9)$后,以不可忽略的概率 $\varepsilon\geqslant 7A(n,q_5)\cdot 2^{-\ell}$ 攻破提出的方案,那么存在一种(t',ε')-CDH 算法 Q, 其中, $t'\leqslant 2\left(t+\sum_{i=1}^{5}q_it_i+\sum_{i=7}^{9}q_it_i\right),\varepsilon'\geqslant[66\cdot A(n,q_4)]^{-1}q_1^{-2}(1-q_1^{-1})^{q_7+q_8}\varepsilon^2$.

证明:Q 选择系统主密钥 $s\in_R\mathbb{Z}_q^*$, 计算 $P_0=sP$,把$\{G_1,G_2,e,q,P,P_0,H_1,H_2,H_3,H_4,H_5\}\cup\{s\}$给 A_{II}.Q 仍然将 H_1~H_5 作为随机预言器,维护 H_1~H_5 和 L 等列表,Q 的目标是由$(P,P_1=aP,P_2=bP)$计算出 abP.

- 生成用户询问:Q 随机选择 $k\in\{1,2,\ldots,q_1\}$.当 A_{II} 询问 Create(ID_i)时,Q 选择 $x_i,\alpha_i\in_R\mathbb{Z}_q^*$ 满足(*,*,*,α_i,*)以前未出现在 H_1 列表.当 $i\neq k$ 时,置 $Q_i=\alpha_iP,P_i=x_iP$;当 $i=k$ 时,置 $Q_k=\alpha_kP,P_k=x_kP+P_2$.$Q$ 把$(ID_i,Q_i,P_i,\alpha_i,x_i)$添入到 H_1 列表,并把 P_i 和 Q_i 返给 A_{II}.
- 公钥替换询问:当 A_{II} 询问 Replace(ID_i,P_i') 时,Q 执行:当 $i=k$ 时,终止协议;当 $i\neq k$ 时,Q 检查 H_1 列表,把元组$(ID_i,Q_i,P_i,\alpha_i,x_i)$更新为 $(ID_i,Q_i,P_i',\alpha_i,\perp)$.
- 秘密值询问:当 A_{II} 询问 Value(ID_i)时,Q 遍历 H_1 列表.当 $i=k$ 时,终止协议.当 $i\neq k$ 且 $x_i\neq\perp$时,则为 A_{II}输出 x_i;否则,返回⊥.
- H_2 哈希询问:当 A_{II} 询问 $H_2(\Delta\|P)$时,Q 选择 $\beta_i\in_R\mathbb{Z}_q^*$ 满足(*,*,β_i)未出现在 H_2 列表,把 $U_i=\beta_iP+P_1$ 返给 A_{II} 并添(Δ_i,U_i,β_i)到 H_2 列表.

H_3,H_4 和 H_5 哈希询问与定理 1 的证明过程相同.

- 个体签名询问:当A_{II} 询问 Sign(m_i,Δ_i,ID_i,P_i)时,Q 查询 H_2,H_3 列表以分别获得 $U_i=\beta_iP+P_1$ 和 $V_i=\lambda_iP-P_1$.Q 执行如下步骤:

  (1) 任选 $r_i,h_i,g_i\in_R\mathbb{Z}_q^*$ 满足(*,*,*,*,h_i)和(*,*,*,*,g_i)分别未出现在 H_4 和 H_5 列表;

  (2) 计算 $R_i=r_iP+h_iP_i$ 并置 $H_4(m_i\|\Delta\|R_i\|ID_i)=h_i$ 和 $H_5(m_i\|\Delta\|R_i\|P_i)=g_i$;

  (3) 计算 $W_i=h_i(\beta_i+\lambda_i)P_i+sg_iQ_i+\lambda_ir_iP-r_iP_1$.

  Q 把$(m_i,\Delta_i,ID_i,P_i,R_i,r_i,h_i,g_i,W_i)$添入 L 列表并以 R_i,W_i 作答.根据 $P_0=sP$ 和个体签名验证算法知:该返回值(R_i,W_i)是关于(m_i,Δ_i,ID_i,P_i)的一个有效签名,因为

$$\begin{aligned}e(g_iQ_i,P_0)e(h_iP_i,U)e(R_i,V)&=e(g_iQ_i,sP)e(h_iP_i,\beta_iP+P_1)e(r_iP+h_iP_i,\lambda_iP-P_1)\\&=e(sg_iQ_i,P)e(h_i\beta_iP_i,P)e(h_iP_i,P_1)e(\lambda_ir_iP+\lambda_ih_iP_i,P)e(-r_iP_1,P)e(h_iP_i,-P_1)\\&=e(h_i\beta_iP_i+\lambda_ih_iP_i+sg_iQ_i+\lambda_ir_iP-r_iP_1,P)\\&=e(W_i,P).\end{aligned}$$

- 伪造:类似与定理 1 相应过程,只是 Q 选择不同的哈希函数 H_4' 并应用 Forking lemma[11],进而构造出一个方程组:

$$\begin{cases}e\left(\sum_{i=1}^{n}g_i^*Q_i^*,P_0\right)e\left(\sum_{i=1}^{n}h_i^*P_i^*,U^*\right)e\left(\sum_{i=1}^{n}R_i^*,V^*\right)=e(W^*,P)\\e\left(\sum_{i=1}^{n}g_i^*Q_i^*,P_0\right)e\left(\sum_{i=1}^{n}h_i^{*\prime}P_i^*,U^*\right)e\left(\sum_{i=1}^{n}R_i^*,V^*\right)=e(W^{*\prime},P)\end{cases}.$$

两式相除,得出:

$$e((h_s^*-h_s^{*\prime})P_s^*,U^*)=e(W^*-W^{*\prime},P).$$

✓ 若 $ID_j^*=ID_k=ID_s^*$,则 $U^*=\beta_kP+P_1$, $P_s^*=P_k=x_kP+P_2$.Q 可以解出:

$$abP=(h_s^*-h_s^{*\prime})^{-1}(W^*-W^{*\prime})-\beta_kP_2-x_kP_1-x_k\beta_kP;$$

✓ 否则,Q 终止协议.

- 成功概率:类似于定理 1 中相应的部分. □

表 3 列举了几个在随机预言模型下可证安全的无证书聚合签名方案.数据显示,只有文献[8]和本文的方案给出了能够抵抗两类超级攻击者形式化的证明,而文献[5−7,9]中的方案给出了只能抵抗弱正常攻击者 A_{II} 的

证明.

Table 3 Comparison of certificateless aggregate signature schemes

表 3 无证书聚合签名方案比较

方案	个体签名	聚合验证	聚合签名长度	安全性
文献[5]	3SM+2H	(n+3)BP+(2n+1)H	(n+1)L	抗超级A_{I}和弱正常A_{II}
文献[6]	5SM+3H	5BP+2nSM+(2n+3)H	2L	抗超级A_{I}和弱正常A_{II}
文献[7]-1	2SM+1H	(2n+1)BP+2nH	(n+1)L	抗强A_{I}和弱正常A_{II}
文献[7]-2	3SM+1H	(n+2)BP+nSM+2nH	2L	抗强A_{I}和弱正常A_{II}
文献[9]	4SM+1H	4BP+nSM+(n+1)H	2L	抗正常A_{I}和弱正常A_{II}
文献[8]	3SM	(n+1)BP+2nSM+nH	(n+1)L	抗超级A_{I}和超级A_{II}
本文	4SM+2H	4BP+2nSM+(n+2)H	(n+1)L	抗超级A_{I}和超级A_{II}

3.3 效 率

方案的效率从两个方面考察:计算和通信代价.为了方便,用 L 表示群 G_1 中元素的比特长度,pairing 运算用 BP 表示, $\{0,1\}^* \to G_1^*$ 上的 hash 运算记为 H,群 G_1 中标量乘运算为 SM.这 3 种运算代价较大,尤其是 BP.故比较时只考虑它们.文献[7]包含两个聚合签名方案,我们用[7]-1 和[7]-2 加以区别.表 3 数据显示:本文方案的聚合验证运算量明显小于文献[5−8],稍大于文献[9].虽然我们的聚合签名长度比文献[9]大,但是文献[9]中每个个体签名时必须所有参与成员互相传递数据后才能完成,最后再聚合产生聚合签名.因需要成员间交互信息而加大了通信代价,这必将极大地降低方案的效率,故在通信代价上,文献[9]并不比我们的方案占优势.另外,由于文献[9]涉及交换数据,所以在个体签名之前需要确定参与的成员.而我们的方案却没有这种限制,故它可以方便地实现系统中成员动态地加入每次的聚合签名.

4 结 论

本文利用双线性映射提出一个无证书聚合签名方案.该方案具有效率高、安全性强等优点.另外,方案中用户个体签名只使用公共信息和用户自己的信息,阻断了用户间的耦合性,可以方便实现系统中用户动态加入聚合签名,这使得方案具有应用的灵活性.鉴于该方案安全、高效和无证书管理的优点,它可应用于多对一的通信系统中对消息的认证.

致谢 我们向给予支持和提出宝贵建议的同行深表感谢.

References:

[1] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[2] Huang XY, Mu Y, Susilo W, Wong DS, Wu W. Certificateless signature revisited. In: Pieprzyk J, Ghodosi H, Dawson E, eds. Proc. of the ACISP 2007. LNCS 4586, Heidelberg: Springer-Verlag, 2007. 308−322. [doi: 10.1007/978-3-540-73458-1_23]

[3] Chen H, Zhang FT, Song RS. Certificateless proxy signature scheme with provable security. Ruan Jian Xue Bao/Journal of Software, 2009,20(3):692−701 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/574.htm [doi: 10.3724/SP.J.1001.2009.00574]

[4] Chen H, Zhu CJ, Song RS. Efficient certificateless signature and group signature schemes. Journal of Computer Research and Development, 2010,47(2):231−237 (in Chinese with English abstract).

[5] Zhang L, Zhang FT. A new certificateless aggregate signature scheme. Computer Communications, 2009,32(6):1079−1085. [doi: 10.1016/j.comcom.2008.12.042]

[6] Zhang L, Qin B, Wu QH, Zhang FT. Efficient many-to-one authentication with certificateless aggregate signatures. Computer Networks, 2010,54(14):2482−2491. [doi: 10.1016/j.comnet.2010.04.008]

[7] Gong Z, Long Y, Hong X, Chen KF. Practical certificateless aggregate signatures from bilinear maps. Journal of Information Science and Engineering. 2010,26:2093−2106.

[8] Chen H, Song WG, Zhao B. Certificateless aggregate signature scheme. In: Xie S, *et al*., eds. Proc. of the 2010 Int'l Conf. on E-Business and E-Government (ICEE). IEEE Computer Society, 2010. 3790−3793. [doi: 10.1109/ICEE.2010.950]

[9] Lu HJ, Yu XY, Xie Q. Provably secure certificateless aggregate signature with constant length. Journal of Shanghai Jiaotong University, 2012,46(2):259−263 (in Chinese with English abstract).

[10] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Proc. of the EUROCRPYT 2003. LNCS2656, Heidelberg: Springer-Verlag, 2003. 416−432. [doi: 10.1007/3-540-39200-9_26]

[11] Herranz J, Saez G. New identity-based ring signature schemes. In: Lopez J, Qing S, Okamoto E, eds. Proc. of the ICICS 2004. LNCS 3269, Heidelberg: Springer-Verlag, 2004. 27−39. [doi: 10.1007/978-3-540-30191-2_3]

附中文参考文献:

[3] 陈虎,张福泰,宋如顺.可证安全的无证书代理签名方案.软件学报,2009,20(3):692−701. http://www.jos.org.cn/1000-9825/574.htm [doi: 10.3724/SP.J.1001.2009.00574]

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

[9] 陆海军,于秀源,谢琪.可证安全的常数长度无证书聚合签名方案.上海交通大学学报,2012,46(2):259−263.

陈虎(1975－),男,江苏睢宁人,博士生,副教授,主要研究领域为密码学.

朱昌杰(1963－),男,教授,CCF 会员,主要研究领域为软件与理论.

魏仕民(1962－),男,博士,教授,主要研究领域为密码学.

杨忆(1980－),男,博士生,讲师,主要研究领域为信息安全.