无证书聚合签名方案

明 洋[1]，赵祥模[1]，王育民[2]

(1. 长安大学信息工程学院 西安 710064；2. 西安电子科技大学综合业务网理论与关键技术国家重点实验室 西安 710071)

【摘要】聚合签名通过聚合 n 个签名(n 个不同签名者对 n 个不同消息生成)为一个签名，节省带宽和提高签名验证效率。无证书公钥密码体制解决了传统公钥密码体制中的证书管理问题以及基于身份密码体制中的密钥托管问题。该文基于双线性对提出一个新的高效的无证书聚合签名方案。分析表明，在随机预言机模型中计算性Diffie-Hellman假设下，所提方案能够抵抗适应性选择消息攻击下的存在性伪造攻击，同时所提方案签名长度独立于签名者的数量仅为2个群元素，签名验证中仅需要4个对和n个标量乘运算，因此该方案更加适合资源受限网络环境中的应用。

关 键 词 双线性对； 无证书聚合签名； 无证书公钥密码学； 随机预言机模型

中图分类号 TN918.1 文献标志码 A doi:10.3969/j.issn.1001-0548.2014.02.005

Certificateless Aggregate Signature Scheme

MING Yang[1], ZHAO Xiang-mo[1], and WANG Yu-min[2]

(1. School of Information Engineering, Chang'an University Xi'an 710064;

2. State Key Laboratory of Integrated Network Theory and Key Technologies, Xidian University Xi'an 710071)

Abstract Aggregate signatures allow an efficient algorithm to aggregate n signatures of n distinct messages from n different signers into one single signature. Aggregate signature is useful to save bandwidth and improve the efficiency in verification phase. Certificateless public key cryptography overcomes the complicated certificate management in traditional public key cryptography and key escrow problem in identity based cryptography. In this paper, we present a new efficient certificateless aggregate signature scheme based on the bilinear pairing. The analysis shows that the proposed scheme is proven existentially unforgeable against adaptive chosen message attacks under the computational Diffie-Hellman assumption in the random oracle model. The signature length is only two group elements, which is independent of the number of signers, and the signature needs only four pairings and n scalar multiplications computations in verification phase. Thus, the proposed scheme is more suitable for the applications, in resource-constrained environment.

Key words bilinear pairing; certificateless aggragate signature; certificateless public key cryptography; random oracle model

1976年，文献[1]提出了公钥密码体制思想。数字签名能够提供认证性、数据完整性和不可否认性的特征是公钥密码体制的重要组成部分。在传统的数字签名中，用户的公钥私钥由用户自己选取，证书中心给每个用户颁发一个公钥证书(对用户公钥的签名)，因此，证书中心需要维护和管理庞大的公钥证书。为了简化公钥证书的管理，文献[2]首次提出基于身份密码学(ID-PKC)的思想，其中用户选取自己的身份信息(如IP地址、电子邮件等)作为公钥，用户私钥由私钥生成器(PKG)生成。基于身份签名方案虽然解决传统数字签名中的证书管理问题，然而存在内在的密钥托管问题，即PKG知道所有用户的私钥，可以伪造任何用户任意消息的签名。

基于此，文献[3]提出无证书公钥密码学(CL-PKC)的概念。在该系统中，密钥生成中心(KGC)生成用户的部分私钥，用户使用部分私钥和自己选取的秘密值独立生成自己的公钥和私钥，从而克服了传统公钥密码学中的证书管理问题，解决了基于身份密码学中的密钥托管问题。

现实中，n 层PKI证书链和安全边界网关协议(BGP)[4]均涉及 n 个签名者对 n 个不同消息的 n 个签名。如果使用传统数字签名方案，随着 n 增大，签

收稿日期：2011－09－21；修回日期：2013－12－12

基金项目：国家自然科学基金(61202438)；中国博士后科学基金(2011M501427)；陕西省自然科学基金(2010JQ8017)；中央高校基本科研业务费专项基金-长安大学基础研究支持计划专项基金(CHD2012JC047)

作者简介：明洋(1979－)，男，博士，副教授，主要从事数字签名理论、可证明安全理论方面的研究.

名长度以及签名验证的工作量将急剧增大。聚合签名(aggregate signature, SA)正好能够解决该问题。在该签名中，n个签名者对n个消息$m_1,m_2,\cdots,m_n$分别签署得到n个签名$\sigma_1,\sigma_2,\cdots,\sigma_n$，而验证者只需要对聚合后的签名进行验证，即可确信$n$个消息是否被$n$个签名者分别进行了签名。聚合签名一方面能够聚合$n$个签名$\sigma_1,\sigma_2,\cdots,\sigma_n$为一个签名$\sigma$减少签名的长度；另一方面通过一个聚合签名$\sigma$验证减少了$n$个签名$\sigma_1,\sigma_2,\cdots,\sigma_n$验证的计算代价。

文献[5]首次提出聚合签名的概念，基于BLS短签名给出具体构建。文献[6]基于限门置换提出一个序列聚合签名方案，签名者依次将自己的签名聚合到由它前面的签名者产生的聚合签名中，产生自己的聚合签名。文献[7]对文献[6]的安全模型进行分析，提出新的安全模型并给出改进方案。将聚合签名扩展到基于身份环境中，大量基于身份聚合签名方案[8-13]被提出。文献[14]将聚合签名扩展到无证书环境中，首次提出无证书聚合签名方案。利用双线性对给出两个具体方案。文献[15]提出一个有效的无证书聚合签名方案，并在随机预言机模型证明安全性。文献[16]提出一个新的无证书聚合签名方案，所提方案中聚合签名长度为独立于签名数量。利用双线性对，文献[17]提出了无证书签名方案和无证书聚合签名方案。

本文基于双线性对提出一个高效随机预言机模型下可证安全的无证书聚合签名方案。基于计算性Diffie-Hellman假设，该方案在适应性选择消息攻击下是存在性不可伪造的。和现有无证书聚合签名方案相比，该方案效率更高，更加适合无线传感器网络等资源受限的网络环境中。

1　基础知识

1.1　双线性对和困难假设

设$(G_1,+)$是由P生成的加法群，其阶数为素数q，$(G_2,\cdot)$是乘法群，阶数也为q。设$e:G_1\times G_1\to G_2$是一个映射，满足下面的性质：

1) 双线性性：对所有的$R,Q\in G_1$，$a,b\in Z_q^*$，都有$e(aR,bQ)=e(R,Q)^{ab}$。

2) 非退化性：存在$R,Q\in G_1$，满足$e(R,Q)\neq 1$。

3) 可计算性：对所有的$R,Q\in G_1$，存在有效的算法计算$e(R,Q)$。

那么e称为双线性对。

群G_1中计算性Diffie-Hellman(CDH)问题：对于任意的$a,b\in Z_q^*$，给定群G_1中元素(P,aP,bP)，计算$abP\in G_1$。

群G_1中计算性Diffie-Hellman(CDH)假设：没有多项式时间的算法以不可忽略的概率解群G_1中的CDH问题。

1.2　无证书聚合签名形式化定义和安全模型

无证书聚合签名方案包含密钥生成中心(KGC)，n个签名者$\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n$和聚合签名生成者，由系统建立、部分私钥生成、密钥生成、签名生成、聚合签名生成、聚合签名验证6个算法组成[15-16]。

和无证书签名方案相同，无证书聚合签名方案面临两种类型攻击者：

类型I：攻击者A_I不拥有主密钥，但能够替换任何用户的公钥。

类型II：攻击者A_II拥有主密钥，但不能进行公钥替换。

无证书聚合签名方案的安全性需要同时满足类型I和类型II攻击下的存在性不可伪造[15-16]。

2　无证书聚合签名方案

系统建立算法：输入安全参数k，生成阶数为素数q的椭圆曲线上的循环群G_1和G_2，以及双线性对$e:G_1\times G_1\to G_2$，选择安全Hash函数：$H_1:\{0,1\}^*\to G_1$　$H_2:\{0,1\}^*\to G_1$，$H_3:\{0,1\}^*\to G_1$，$H_4:\{0,1\}^*\to Z_q^*$。KGC选择任意的生成元$P\in G_1$，选取主密钥$s\in Z_q^*$，计算$P_{\mathrm{pub}}=sP$，公开系统参数$(q,G_1,G_2,e,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4)$，保密主密钥$s$。

部分私钥生成算法：输入系统参数，用户身份$\mathrm{ID}_i\in\{0,1\}^*$和主密钥$s$，KGC计算$Q_i=H_1(\mathrm{ID}_i)$，通过安全信道输出部分私钥$D_i=sQ_i$。

密钥生成算法：输入系统参数，用户ID_i随机选取$x_i\in Z_q^*$，计算$P_i=x_iP$。则x_i为用户的秘密值，P_i为用户的公钥。

签名生成算法：输入系统参数，消息m_i，签名者ID_i的签名密钥(x_i,D_i)以及公钥P_i，签名者ID_i随机选取一个状态信息θ，完成下面步骤：

1) 随机选取$r_i\in Z_q^*$，计算$R_i=r_iP$。

2) 计算$U=H_2(\theta)$，$T=H_3(\theta)$，$h_i=H_4(\theta\|m_i\|\mathrm{ID}_i\|P_i)$。

3) 计算$S_i=D_i+x_i(h_iP_{\mathrm{pub}}+U)+r_iT$。

4) 输出消息m_i的签名$\sigma_i=(R_i,S_i)$。

聚合签名生成算法：输入系统参数，n个签名者$\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n$的消息签名对$(m_1,\sigma_1),(m_2,\sigma_2),\cdots,$

(m_n,σ_n)，任何人计算 $R=\sum_{i=1}^{n}R_i$， $S=\sum_{i=1}^{n}S_i$。则聚合签名为 $\sigma=(R,S)$。

聚合签名验证算法：输入系统参数，n 个签名者 $\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$，以及相应公钥 $\{P_1,P_2,\cdots,P_n\}$，在相同状态信息 θ 下消息 $\{m_1,m_2,\cdots,m_n\}$ 的聚合签名 $\sigma=(R,S)$，验证者完成下面步骤：

1) 计算 $U=H_2(\theta)$， $T=H_3(\theta)$。

2) 对所有的 $1\leqslant i\leqslant n$，计算 $Q_i=H_1(\mathrm{ID}_i)$，$h_i=H_4(\theta\|m_i\|\mathrm{ID}_i\|P_i)$。

3) 验证

$$e(S,P)=e\left(\sum_{i=1}^{n}Q_i+\sum_{i=1}^{n}h_iP_i,P_{\mathrm{pub}}\right)\times e\left(\sum_{i=1}^{n}P_i,U\right)e(T,R)$$

如果等式成立，输出“接受”；否则输出“拒绝”。

3 本文方案分析

3.1 安全性证明

定理 1 在随机预言机模型中，若存在一个类型I攻击者 A_{I} 能够在时间 t 内最多进行 q_i 次 $H_i(i=1,2,3,4)$ 预言机询问、q_d 次部分私钥询问、q_k 次秘密值询问、q_p 次公钥询问、q_r 次公钥替换询问、q_s 次签名询问后，以不可忽略的概率 ε 在游戏1中获胜，那么存在一个算法能够以时间 $t'=t+(q_1+q_2+q_3+q_d+q_p+q_k+5q_s)t_{\mathrm{sm}}$，概率 $\varepsilon'=\frac{1}{q_d+n}(1-\frac{1}{q_d+n})^{q_d+n-1}\varepsilon$ 解CDH问题，这里 n 表示签名者的数量，t_{sm} 表示群 G_1 中计算一次标量乘运算的时间。

证明：假设 B 是一个解CDH问题的算法。给定CDH问题的一个随机实例 (P,aP,bP) 下，算法 B 使用 A_{I} 作为子程序计算出 abP。为了保持一致性，B维护 $L_1\sim L_4$ 共4个列表，分别跟踪 A_{I} 对 $H_i(i=1,2,3,4)$ 以及密钥的询问，所有列表初始化为空。

系统建立：算法 B 令 $P_{\mathrm{pub}}=aP$，返回参数 $(q,G_1,G_2,e,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4)$ 给 A_{I}。

询问：B 模拟游戏1中的挑战者 C 回答 A_{I} 的所有询问。

H_1 预言机询问：列表 L_1 格式为 $(\mathrm{ID}_i,\alpha_i,Q_i,c_i)$。当 B 收到 A_{I} 对 ID_i 进行 H_1 询问时，如果列表 L_1 中已经存在，则返回相应的值给 A_{I}；否则，B 随即选取 $c_i\in\{0,1\}$ 满足 $\Pr[c_i=0]=\delta$，如果 $c_i=0$，B 随即选取 $\alpha_i\in Z_q^*$，计算 $Q_i=\alpha_i bP$；如果 $c_i=1$，B 随即选取 $\alpha_i\in Z_q^*$，计算 $Q_i=\alpha_i P$。最后，B 返回 Q_i 并将 $(\mathrm{ID}_i,\alpha_i,Q_i,c_i)$ 加入列表 L_1 中。

H_2 预言机询问：列表 L_2 格式为 (θ_i,l_i,U_i)。当 B 收到 A_{I} 对 θ_i 进行 H_2 询问时，如果列表 L_2 中已经存在，则返回相应的值给 A_{I}；否则，B 随即选取 $l_i\in Z_q^*$，计算 $U_i=l_iP$。最后，B 返回 U_i 并将 (θ_i,l_i,U_i) 加入列表 L_2 中。

H_3 预言机询问：列表 L_3 格式为 (θ_i,β_i,T_i)。当 B 收到 A_{I} 对 θ_i 进行 H_3 询问时，如果列表 L_3 中已经存在，则返回相应的值给 A_{I}；否则，B 随即选取 $\beta_i\in Z_q^*$，计算 $T_i=\beta_iP$。最后，B 返回 T_i 并将 (θ_i,β_i,T_i) 加入列表 L_3 中。

H_4 预言机询问：列表 L_4 格式为 $(\theta_i,m_i,\mathrm{ID}_i,P_i,h_i)$。当 B 收到 A_{I} 对 $(\theta_i,m_i,\mathrm{ID}_i,P_i)$ 进行 H_4 询问时，如果列表 L_4 中已经存在，则返回相应的值给 A_{I}；否则，B 随即选取 $h_i\in Z_q^*$。最后，B 返回 h_i 并将 $(\theta_i,m_i,\mathrm{ID}_i,P_i,h_i)$ 加入列表 L_4 中。

部分私钥询问：列表 L 格式为 $(\mathrm{ID}_i,D_i,x_i,P_i)$。当 B 收到 A_{I} 对 ID_i 进行部分私钥询问时，如果列表 L 中已经存在，则返回相应的值给 A_{I}；否则，B 查询列表 L_1 是否存在 $(\mathrm{ID}_i,\alpha_i,Q_i,c_i)$，如果不存在，$B$ 首先对 ID_i 进行 H_1 询问得到相应的 $(\mathrm{ID}_i,\alpha_i,Q_i,c_i)$，

1) 如果 $c_i=0$ 时，B放弃。

2) 如果 $c_i=1$ 时，B 返回 $D_i=\alpha_iP_{\mathrm{pub}}$ 并将 $(\mathrm{ID}_i,D_i,\perp,\perp)$ 加入列表 L 中。

公钥询问：当 B 收到 A_{I} 对 ID_i 进行公钥询问时，如果列表 L 中已经存在，则返回相应的值给 A_{I}；否则，B 随机选取 x_i，计算 $P_i=x_iP$。最后，B 返回 P_i 并将 $(\mathrm{ID}_i,\perp,x_i,P_i)$ 加入列表 L 中。

秘密值询问：当 B 收到 A_{I} 对 ID_i 进行秘密值询问时，如果列表 L 中已经存在，则返回相应值给 A_{I}；否则，B 对 ID_i 进行公钥询问并返回 x_i。

公钥替换询问：当 B 收到 A_{I} 对 (ID_i,P_i') 进行公钥替换询问时，如果列表 L 中包含 $(\mathrm{ID}_i,D_i,x_i,P_i)$；否则，$B$ 对 ID_i 进行公钥询问得到 $(\mathrm{ID}_i,D_i,x_i,P_i)$。最后，$B$ 返回 P_i' 并更新列表 L 为 $(\mathrm{ID}_i,D_i,x_i,P_i')$。

签名询问：当 B 收到 A_{I} 对 $(\theta_i,m_i,\mathrm{ID}_i,P_i)$ 进行签名询问时，B 从列表 L_1 中得到 $(\mathrm{ID}_i,\alpha_i,Q_i,c_i)$，列表 L_2 中得到 (θ_i,l_i,U_i)，列表 L_3 中得到 (θ_i,β_i,T_i) 以及列表 L_4 中得到 $(\theta_i,m_i,\mathrm{ID}_i,P_i,h_i)$。

1) 如果 $c=1$ 时，B 随机选取 $R_i\in G_1$，计算 $S_i=\alpha_iP_{\mathrm{pub}}+h_ix_iP_{\mathrm{pub}}+l_iP_i+\beta_iR_i$。

2) 如果 $c=0$ 时，B 随机选取 $r_i,\beta_i\in Z_q^*$，令 $T_i=\beta_i P_{\text{pub}}$，计算 $R_i=r_iP-\beta_i^{-1}Q_i$，$S_i=r_i\beta_iP_{\text{pub}}+h_ix_iP_{\text{pub}}+l_iP_i$。

最后，B 返回 $\sigma_i=(R_i,S_i)$ 给 A_{I}。

伪造：A_{I} 输出 n 个用户 $\{\text{ID}_1^*,\text{ID}_2^*,\cdots,\text{ID}_n^*\}$ 以及相应的公钥 $\{P_1^*,P_2^*,\cdots,P_n^*\}$，$n$ 个消息集合 $\{m_1^*,m_2^*,\cdots,m_n^*\}$，状态信息 θ^* 和伪造聚合签名 $\sigma^*=(R^*,S^*)$。这里要求至少存在一个 $k\in\{1,2,\cdots,n\}$ 满足 A_{I} 不能对 ID_k^* 进行部分私钥询问，不能对 $(\theta^*,m_k^*,\text{ID}_k^*,P_k^*)$ 进行签名询问，不失一般性，选定 $k=1$。

对于所有的 $1\leqslant i\leqslant n$，B 从列表 L_1 和 L_4 中分别得到 $(\text{ID}_i^*,\alpha_i^*,Q_i^*,c_i^*)$ 和 $(\theta^*,m_i^*,\text{ID}_i^*,P_i^*,h_i^*)$，从列表 L_2 和 L_3 中得到 (θ^*,l^*,U^*) 和 (θ^*,β^*,T^*)。

如果 $c_1^*\neq 0$，$c_i^*\neq 1(2\leqslant i\leqslant n)$，$B$ 放弃；否则 $c_1^*=0$，$c_i^*=1$，B 计算 $abP=\alpha_1^{-1}\left[S^*-\beta^*R^*-\sum_{i=1}^{n}l^*P_i^*-h_1^*x_1^*aP-\sum_{i=2}^{n}(\alpha_i^*+h_i^*x_i^*)aP\right]$。

为了分析算法 B 成功解CDH问题的概率，定义以下事件：

E_1：在部分私钥询问中 B 不放弃。

E_2：A_{I} 能够生成一个有效的聚合签名。

E_3：E_2 发生时，且 $c_1^*=0$，$c_i^*=1(2\leqslant i\leqslant n)$。

B 成功的概率为：

$$\Pr[E_1\wedge E_2\wedge E_3]=\Pr[E_1]\Pr[E_2\mid E_1]\Pr[E_3\mid E_2\wedge E_1]$$

在部分私钥询问中，B 不放弃的概率为 $1-\delta$，且最多进行 q_d 次部分私钥询问，则 $\Pr[E_1]\geqslant(1-\delta)^{q_d}$。如果 B 在部分私钥询问中不放弃，此时模拟环境和真实环境对攻击者来说是不可区分的，即 $\Pr[E_2\mid E_1]\geqslant\varepsilon$。当 E_1 和 E_2 发生时，攻击者 A_{I} 能够输出一个有效伪造签名。当 $c_1^*=0$，$c_i^*=1(2\leqslant i\leqslant n)$ 时，B 不放弃，则 $\Pr[E_3\mid E_2\wedge E_1]\geqslant\delta(1-\delta)^{n-1}$。因此有：

$$\varepsilon'=\Pr[E_1\wedge E_2\wedge E_3]=(1-\delta)^{q_d}\varepsilon\delta(1-\delta)^{n-1}=\delta(1-\delta)^{q_d+n-1}\varepsilon$$

当 $\delta=\dfrac{1}{q_d+n}$ 时，ε' 取最大值，$\varepsilon'=\dfrac{1}{q_d+n}\left(1-\dfrac{1}{q_d+n}\right)^{q_d+n-1}\varepsilon$。

算法 B 运行的时间等于攻击者 A_{I} 的伪造时间加上回答 q_1 次 H_1 询问的时间、q_2 次 H_2 询问的时间、q_3 次 H_3 询问的时间、q_d 次部分私钥询问的时间、q_p 次公钥询问的时间、q_k 次秘密值询问的时间和 q_s 次签名询问的时间。每次 H_1 询问、H_2 询问、H_3 询问，部分私钥询问、公钥询问和秘密值询问均需要1个标量乘运算，每次签名询问需要5个标量乘运算，则 $t'=t+(q_1+q_2+q_3+q_d+q_p+q_k+5q_s)t_{\text{sm}}$。

定理 2　在随机预言机模型中，若存在一个类型II攻击者 A_{II} 能够在时间 t 内最多进行 q_i 次 $H_i(i=2,3,4)$ 预言机询问、q_k 次秘密值询问、q_p 次公钥询问、q_s 次签名询问后，以不可忽略的概率 ε 在游戏2中获胜，那么存在一个算法能够以时间 $t'=t+(q_2+q_3+q_p+q_k+6q_s)t_{\text{sm}}$，概率 $\varepsilon'=\dfrac{1}{q_k+n}\left(1-\dfrac{1}{q_k+n}\right)^{q_k+n-1}\varepsilon$ 解CDH问题，这里 n 表示签名者的数量，t_{sm} 表示群 G_1 中一次标量乘运算的时间。

证明：假设 B 是CDH问题的解决者，给定CDH问题的一个随机实例 (P,aP,bP) 下，算法 B 使用 A_{II} 作为子程序计算出 abP。为了保持一致性，B 维护 L_2,L_3,L_4,L 共4个列表，分别跟踪 A_{II} 对 $H_i(i=2,3,4)$ 和密钥询问，所有列表初始化为空。

系统建立：B 随机选取 $s\in Z_q^*$，计算 $P_{\text{pub}}=sP$，返回系统参数 $(q,G_1,G_2,e,P,P_{\text{pub}},H_1,H_2,H_3,H_4)$ 和主密钥 s 给 A_{II}。此时 B 知道主密钥，因此能够计算出任何用户的部分私钥 $D_i=sH_1(\text{ID}_i)$，不需要进行 H_1 和部分私钥询问。

询问：B 模拟游戏2中的挑战者 C 回答 A_{II} 的所有询问。

H_2 预言机询问：列表 L_2 格式为 (θ_i,l_i,U_i)。当 B 收到 A_{II} 对 θ_i 进行 H_2 询问时，如果列表 L_2 中已经存在，则返回相应的值给 A_{II}；否则，B 随即选取 $l_i\in Z_q^*$，计算 $U_i=l_ibP$。最后，B 返回 U_i 并将 (θ_i,l_i,U_i) 加入列表 L_2 中。

H_3 预言机询问：列表 L_3 格式为 (θ_i,β_i,T_i)。当 B 收到 A_{II} 对 θ_i 进行 H_3 询问时，如果列表 L_3 中已经存在，则返回相应的值给 A_{II}；否则，B 随即选取 $\beta_i\in Z_q^*$，计算 $T_i=\beta_iP$。最后，B 返回 T_i 并将 (θ_i,β_i,T_i) 加入列表 L_3 中。

H_4 预言机询问：列表 L_4 格式为 $(\theta_i,m_i,\text{ID}_i,P_i,h_i)$。当 B 收到 A_{II} 对 $(\theta_i,m_i,\text{ID}_i,P_i)$ 进行 H_4 询问时，如果列表 L_4 中已经存在，则返回相应的值给 A_{II}；否则，B 随即选取 $h_i\in Z_q^*$。最后，B 返回 h_i 并将 $(\theta_i,m_i,\text{ID}_i,P_i,h_i)$ 加入列表 L_4 中。

公钥询问：列表 L 格式为 $(\text{ID}_i,x_i,P_i,c_i)$。当 B 收

到 A_{II} 对 ID_i 进行公钥询问时，如果列表L中已经存在，则返回相应的值给 A_{II}；否则，B 随即选取 $c_i \in \{0,1\}$ 满足 $\Pr[c_i=0]=\delta$，如果 $c_i=0$，B 随机选取 $x_i \in Z_q^*$，计算 $P_i=x_i aP$；如果 $c_i=1$，B 随即选取 $x_i \in Z_q^*$，计算 $P_i=x_i P$。最后，B 返回 P_i 并将 $(\mathrm{ID}_i,x_i,P_i,c_i)$ 加入列表 L 中。

秘密值询问：当 B 收到 A_{II} 对 ID_i 进行秘密值询问时，B 首先对 ID_i 进行公钥询问得到相应的 $(\mathrm{ID}_i,x_i,P_i,c_i)$。如果 $c_i=0$ 时，B 放弃；否则 $c_i=1$ 时，B返回 x_i。

签名询问：当 B 收到 A_{II} 对 $(\theta_i,m_i,\mathrm{ID}_i,P_i)$ 进行签名询问时，B 从列表 L_2 中得到 (θ_i,l_i,U_i)，列表 L_3 中得到 (θ_i,β_i,T_i)，列表 L_4 中得到 $(\theta_i,m_i,\mathrm{ID}_i,P_i,h_i)$ 以及列表 L 中得到 $(\mathrm{ID}_i,x_i,P_i,c_i)$，

1) 如果 $c_i=1$ 时，B 已知 ID_i 的部分私钥和秘密值，使用“签名生成算法”得到 $\sigma_i=(R_i,S_i)$。

2) 如果 $c_i=0$ 时，B 随机选取 $r_i \in Z_q^*$，令 $T_i=\beta_i P_i$，计算 $R_i=r_i P-\beta^{-1}l_i bP$，$S_i=r_i\beta_i P_i+sh_i P_i+sH_1(\mathrm{ID}_i)$。

最后，B 返回签名 $\sigma_i=(R_i,S_i)$。

伪造：A_{II} 输出 n 个身份集合 $\{\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_n^*\}$ 以及相应的公钥 $\{P_1^*,P_2^*,\cdots,P_n^*\}$，$n$ 个消息集合 $\{m_1^*,m_2^*,\cdots,m_n^*\}$，状态信息 θ^* 和伪造聚合签名 $\sigma^*=(R^*,S^*)$。这里要求至少存在一个 $k\in\{1,2,\cdots,n\}$ 满足 A_{II} 不能对 ID_k^* 进行秘密值询问，不能对 $(\theta^*,m_k^*,\mathrm{ID}_k^*,P_k^*)$ 进行签名询问，不失一般性，选定 $k=1$。

对所有的 $1\leqslant i\leqslant n$，B 从列表 L_4 和 L 中分别得到 $(\theta^*,m_i^*,\mathrm{ID}_i^*,P_i^*,h_i^*)$ 和 $(\mathrm{ID}_i,x_i,P_i,c_i)$，从列表 L_2 中得到 (θ^*,l^*,U^*)，从列表 L_3 中得到 (θ^*,β^*,T^*)。

如果 $c_1^*\neq 0$，$c_i^*\neq 1(2\leqslant i\leqslant n)$，$B$ 放弃；否则 $c_1^*=0$，$c_i^*=1$，B 计算 $abP=(x_1^*l^*)^{-1}\times\left(S^*-\sum_{i=1}^{n}s(Q_i^*+h_i^*P_i^*)-\beta_i^*R^*-\sum_{i=2}^{n}x_i^*l^*bP\right)$。

使用与定理1相同的分析方法可得，B 成功的概率为 $\varepsilon'=\frac{1}{q_k+n}\left(1-\frac{1}{q_k+n}\right)^{q_k+n-1}\varepsilon$，运行时间为 $t'=t+(q_2+q_3+q_p+q_k+6q_s)t_{\mathrm{sm}}$。

3.2 效率

表1比较了本文方案和文献[14-17]中已知无证书聚合签名方案。定义 P 为双线性对的运算，sm 为 G_1 中的标量乘运算，$|G_1|$ 为群 G_1 中元素长度，n为签名者的数量，不考虑其它运算和所有的Hash函数运算。

表1 无证书聚合签名比较

方案	签名生成算法	聚合验证算法	部分私钥长度	聚合签名长度
文献[14]方案1	2 sm	$(4n+1)P$	$\|G_1\|$	$(n+1)\|G_1\|$
文献[14]方案2	3 sm	$(3n+2)P$+1n sm	$\|G_1\|$	$2\|G_1\|$
文献[15]	3 sm	$(n+3)P$	$\|G_1\|$	$(n+1)\|G_1\|$
文献[16]	5 sm	$5P+2n$ sm	$2\|G_1\|$	$2\|G_1\|$
文献[17]	3 sm	$4P+2n$ sm	$\|G_1\|$	$(n+1)\|G_1\|$
本文方案	4 sm	$4P+1n$ sm	$\|G_1\|$	$2\|G_1\|$

从表1中可以看出，在签名生成阶段所提方案需要4个标量乘运算，然而比文献[16]方案需要5个标量乘运算。尽管许多的文章讨论对的复杂性以及如何加速对的运算[18]，但是对的计算量仍然高于标量乘运算量。在聚合签名验证阶段，本文方案仅仅需要4个对运算和n个标量乘运算，比文献[16]方案节省1个对运算和n个标量乘运算；比文献[17]节省n个标量乘运算，比文献[14]方案2节省 $(3n-2)$ 个对运算。此外，本文方案的部分私钥长度和文献[14,15,17]方案相同仅为1个群 G_1 中的元素，而文献[16]中需要2个群 G_1 中的元素，同时签名长度独立于签名者的数量仅为2个群 G_1 中的元素。因此，和已知聚合签名方案相比，本文方案效率更高，更加适合实际中应用。

4 结 束 语

本文基于双线性对提出一个新的无证书聚合签名方案，在随机预言机模型中证明其安全性。与已知方案相比，本文方案签名长度独立于签名者的数量，且签名验证所需运算量小，仅需要4个对和n个标量乘运算。因此，新方案更加适应于计算资源和带宽都受限的网络环境中。

参 考 文 献

[1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, IT-22(6): 644-654.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag, 1984, 47-53.

[3] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology-ASIACRYPT'03. Berlin: Springer-Verlag, 2003, 452-473.

[4] KENT S, LYNN C, SEO K. Secure border gateway protocol (Secure-BGP)[J]. IEEE Journal on Selected Areas in Communications, 2000, 28(4): 582-592.

[5] BONEN D, GENTRY C, LYNN B, et al. Aggregate and

verifiably encrypted signatures from bilinear maps[C]// Advances in Cryptology-EUROCRYPT'03. Berlin: Springer-Verlag, 2003, 416-432.

[6] LYSYANSKAYA A, MICALI S, REYZIN L, et al. Sequential aggregate signatures from trapdoor permutations[C]//Advances in Cryptology- EUROCRYPT' 04. Berlin: Springer-Verlag, 2004, 74-90.

[7] SHAO Zu-hua. Enhanced aggregate signatures from pairings[C]//The SKLOIS Conference on Iformation Security and Cryptology. Berlin: Springer-Verlage, 2005, 140-149.

[8] CHEON J H, KIM Y, YOON H. A new ID-based signature with batch verification[EB/OL]. [2011-10-11]. http://eprint. iacr.org/2004/131.

[9] CHENG Xing-guo, LIU Jing-mei, WANG Xin-mei. Identity-based aggregate and verifiably encrypted signatures from bilinear pairing[C]//International Conference on Computational Science and Its Applications. Berlin: Springer-Verlage, 2005, 1046-1054.

[10] XU Jing, ZHANG Zhen-feng, FENG Deng-guo. ID-based aggregate signatures from bilinear pairings[C]//Cryptology and Network Security. Berlin: Springer-Verlage, 2005, 110-119.

[11] GENTRY C, RAMZAN Z. Identity-based aggregate signatures[C]//Public Key Cryptography. Berlin: Springer-Verlage, 2006, 257-273.

[12] HERRANZ J. Deterministic identity based signatures for partial aggregate[J]. The Computer Journal, 2006, 49(3): 322-330.

[13] KYUNG-AH S. An ID-based aggregate signature scheme with constant pairing computations[J]. The Journal of Systems and Software, 2010, 83(10): 1873-1880.

[14] GONG Zheng, LONG Yu, HONG Xuan, et al. Two certificateless aggregate signatures from bilinear maps[C]//Proceedings of the IEEE SNPD'07. [S.l.]: IEEE, 2007: 188-193.

[15] ZHANG Lei, ZHANG Fu-tai. A new certificateless aggregate signature scheme[J]. Computer Communications, 2009, 32(6): 1079-1085.

[16] ZHANG Lei, QIN Bo, WU Qian-hong, et al. Efficient many-to-one authentication with certificateless aggregate signatures[J]. Computer Networks, 2010, 54(14): 2482-2491.

[17] XIONG Hu, GUAN Zhi, CHEN Zhong, et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2013, 219(10): 225- 235.

[18] BARRETO P S L M, GALBRAITH S, EIGEARTAIGH C O, et al. Efficient implementation of pairing-based cryptosystems[J]. Journal of Cryptography, 2004, 17(4): 321-334.

编 辑 张 俊