一种可证安全的紧致无证书聚合签名方案

许 艳[1,2],黄刘生[1,3],田苗苗[1,3],仲 红[2],崔 杰[2]
(1. 中国科学技术大学计算机科学与技术学院,安徽合肥,230026;2. 安徽大学计算机科学与技术学院,安徽合肥,230601;
3. 中国科学技术大学苏州研究院,江苏苏州,215123)

摘 要: 聚合签名能够实现批验证,特别适用于资源受限的无线网络中批量身份认证. 无证书密码体制能够解决聚合签名的证书管理或私钥托管问题. 本文首先对一个无证书聚合签名方案进行分析,随后提出更加安全高效的无证书聚合签名方案,方案验证时需要更少的双线性对操作. 最后在随机预言模型下证明方案具有不可伪造性,其安全性等价于求解 CDH(Computation Diffie-Hellman)困难问题.

关键词: 无证书密码学; 聚合签名; 随机预言模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2016)08-1845-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.08.011

A Provably Secure and Compact Certificateless Aggregate Signature Scheme

XU Yan[1,2], HUANG Liu-sheng[1,3], TIAN Miao-miao[1,3], ZHONG Hong[2], CUI Jie[2]
(1. *School of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui* 230026, *China*;
2. *School of Computer Science and Technology, Anhui University, Hefei, Anhui* 230601, *China*;
3. *Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou, Jiangsu* 215123, *China*)

Abstract: Aggregate signature schemes are particularly useful for authentication in resource-constrained wireless networks for realizing batch verification. Certificateless cryptosystems can resolve the certificate management problem or key escrow problem in aggregate signature schemes. This paper firstly analyzed a certificatelss aggregate signature(CLAS) scheme. Then, a more efficient CLAS scheme that requires less bilinear paring operations was provided. The security analysis showed that this scheme can resist the forgery attack under the random oracle model, the security was equal to resolve CDH problem.

Key words: certificateless cryptography; aggregate signature; random oracle model

1 引言

聚合签名是 n 个签名者分别对 n 个不同的消息进行签名,这 n 个签名可以被聚合成一个签名,验证者只需验证聚合后的签名便可以确认这些消息是否来自对应的签名者. 聚合签名能够实现批验证,可用于解决资源受限的无线网络中批量身份认证问题[1,2]. 2003 年,Boneh 等[3]第一次提出聚合签名的概念,文献[4]基于陷门置换假设提出一个有序聚合签名方案,文献[5]提出基于身份的聚合签名方案. 然而基于传统公钥密码体制或基于身份密码体制的聚合签名方案存在着证书管理问题或私钥托管问题.

Al-Riyami 等[6]在 2003 年首次提出无证书公钥密码学的概念,能够解决传统公钥密码体制的证书管理问题和基于身份密码体制的私钥托管问题. 在无证书密码体制中,用户私钥包括用户随机选择的秘密值和密钥生成中心(KGC)产生的部分私钥,用户公钥由秘密值生成. 近年来已有不少学者对无证书签名进行研究,具有各种属性的无证书签名[7,8]相继被提出.

Gong 等[9]将聚合签名与无证书密码体制相结合,首次提出无证书聚合签名方案,但是没有给出方案的安全性证明. Zhang 等[10]提出一个在随机预言模型下可证安全的无证书聚合签名方案,但是聚合签名的长度随着签名人数的增加而增加. 文献[11,12]中,聚合签名的长度固定,但要求每个签名者维护一个共同的状态信息. 为解决上述不足,一些学者提出利用双线性对

收稿日期:2015-01-15;修回日期:2015-09-14;责任编辑:马兰英
基金项目:国家电网基础前瞻性项目(No. XXN51201304253);国家自然科学基金(No. 61572001, No. 61502443);中国博士后科学基金(No. 2015M570545);安徽省自然科学基金(No. 201508085QF132);安徽大学信息保障技术协同创新中心开放课题(No. ADXXBZ2014-9)

构造的无证书聚合签名方案[13~15],这些方案签名长度固定且验证高效.然而 Xiong 等[13]提出的无证书聚合签名方案,被 He 等[16]和 Cheng 等[17]分别指出难以抵抗恶意 KGC 的伪造攻击.杜红珍等[14]在随机预言模型下证明其无证书聚合签名方案的安全性可归约为 CDH 困难问题,然而本文研究发现杜红珍等人提出的方案(Du-Huang 方案[14])难以抵抗伪造攻击,本文将对 Du-Huang 方案的安全性进行详细分析.随后提出一个更加安全高效的无证书聚合签名方案,方案验证时只需要使用较少的双线对操作且在随机预言模型下具有不可伪造性.此外,由于方案最终生成的聚合签名长度与聚合者的个数无关,因此是紧致的聚合签名方案.最后,与文献[14,15]提出的无证书聚合签名方案进行效率对比,我们的方案更加高效.

2 预备知识

2.1 数学困难问题

定义 1 计算 Diffie-Hellman 问题:给定$(P,aP,bP)\in G_1,a,b\in Z_q^*$,计算 $abP\in G_1$ 是困难的.

2.2 无证书聚合签名方案

定义 2 无证书聚合签名方案主要参与者有 KGC,签名者 $P_i(i=1,2,\cdots,n)$,聚合者和验证者.方案由系统参数生成算法,部分私钥提取算法,用户密钥生成算法,签名算法,聚合算法,验证算法等 6 个多项式时间算法构成,算法具体描述请参考文献[14].

2.3 无证书聚合签名方案安全模型

无证书聚合签名方案存在两种类型的攻击者:(1)攻击者 A_1:不知道系统主密钥,但可以替换任意签名者的公钥;(2)攻击者 A_2:知道系统主密钥,但不能替换签名者的公钥.

无证书聚合签名方案安全模型可以通过挑战者 C 和攻击者 A_1,A_2 之间的攻击游戏来定义:

Game 1

(1)系统参数设置 挑战者 C 运行系统参数生成算法,得到系统参数 *Params* 和系统主密钥 s. C 将 *Params* 发送给攻击者 A_1.

(2)询问:

(a)Hash 询问 A_1 可以访问方案中所有的 Hash 预言机.

(b)部分私钥提取询问 A_1 询问用户 P_i 的部分私钥,C 运行部分私钥提取算法生成部分私钥 d_{IDi} 返回给 A_1.

(c)秘密值询问 A_1 询问用户 P_i 的秘密值,C 运行用户密钥生成算法生成秘密值 x_i 返回给 A_1,如果 P_i 的公钥已被执行过公钥替换算法,则输出 $\perp$.

(d)公钥询问 A_1 询问用户 P_i 的公钥,C 运行用户密钥生成算法生成公钥 pk_{IDi} 返回给 A_1.

(e)替换公钥询问 A_1 能用自己选取的公钥 pk'_{IDi} 替换 P_i 的公钥 pk_{IDi}.

(f)无证书签名询问 A_1 询问 P_i 对消息 m_i 的签名,C 输入 P_i 的身份 ID_i,公钥 pk_{IDi} 生成签名 σ_i 返回给 A_1.

(3)伪造 A_1 输出签名者集合 $P_i(i=1,2,\cdots,n)$ 对消息 m_i^* 的聚合签名 σ^*,若满足以下条件,则攻击成功:

(a)至少一个 P_i 的身份 ID_i 没有同时提交给公钥替换询问和部分私钥提取询问.

(b)(m_i^*,P_i)没有经过无证书签名询问.

Game 2

(1)系统参数设置 与 Game1 类似,不同的是 C 将系统参数 Params 和系统主密钥 s 都发送给攻击者 A_2.

(2)询问 Hash 询问,秘密值询问,公钥询问,无证书签名询问与 Game1 中对应的询问相同.

(3)伪造 A_2 输出签名者集合 $P_i(i=1,2,\cdots,n)$ 对消息 m_i^* 的聚合签名 σ^*,若满足以下条件,则攻击成功:

(a)至少一个 P_i 的身份 ID_i 没有经过秘密值询问.

(b)(m_i^*,P_i)没有经过无证书签名询问.

定义 3 如果攻击者 A_1,A_2 在游戏 Game1,Game2 中获胜的概率可以忽略,那么无证书聚合签名方案在随机预言模型下,对适应性选择消息攻击是不可伪造的.

3 Du-Huang 无证书聚合签名方案及安全性分析

3.1 Du-Huang 无证书聚合签名方案[14]

签名者 $P_i(i=1,2,\cdots,n)$ 的身份信息为 ID_i,对 n 个消息 m_i 进行聚合签名,方案构造如下:

(1)系统参数生成算法 给定安全参数 k,KGC 选择 q 阶循环群 G_1,G_2,q 是素数满足 $q>2^k$,P 是 G_1 的生成元,$e:G_1\times G_1\rightarrow G_2$ 表示双线性映射.H_1,H_2,H_3,H_4 是安全 hash 函数 $H_1\sim H_3:\{0,1\}^*\rightarrow G_1$,$H_4:\{0,1\}^*\rightarrow Z_q^*$.KGC 随机选择 $s\in Z_q^*$,计算 $P_{pub}=sP$.公开系统参数 $params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2,H_3,H_4\}$,保密系统主密钥 s.

(2)部分私钥提取算法 输入 $P_i(i=1,2,\cdots,n)$ 的身份 ID_i,KGC 验证 ID_i 后,计算 $d_{IDi}=sQ_i$,其中 $Q_i=H_1(ID_i)$.

(3)用户密钥生成算法 签名者 $P_i(i=1,2,\cdots,n)$ 随机选择 $x_i\in Z_q^*$ 作为秘密值,计算 $pk_{IDi}=x_iP$ 作为公钥.

(4)签名算法 输入参数 $params,P_i(i=1,2,\cdots,n)$

的身份 ID_i,私钥 d_{IDi}, x_i,公钥 pk_{IDi} 和消息 m_i,不失一般性假设 P_i 对消息 m_i 进行如下签名:

(a)选择随机数 $r_i \in Z_q^*$,计算 $U_i = r_i P$, $T = H_2(P_{pub})$, $W = H_3(P, P_{pub})$ 和 $h_i = H_4(m_i, ID_i, pk_{IDi})$.

(b)计算 $V_i = r_i T + h_i(d_{IDi} + x_i W)$,则 $\sigma_i = (U_i, V_i)$ 是 P_i 对不同消息 m_i 的签名.

(5)聚合　聚合人对 $P_i(i = 1, \cdots, n)$ 发来的签名 $(m_i, \sigma_i = (U_i, V_i))$ 进行验证然后聚合.

(a)验证　计算 $T = H_2(P_{pub})$, $W = H_3(P, P_{pub})$, $h_i = H_4(m_i, ID_i, pk_{IDi})$,验证等式 $e(P, V_i) = e(U_i, T) e(P_{pub}, h_i Q_i) e(h_i pk_{IDi}, W)$ 是否成立,若成立则接受 σ_i 否则终止算法.

(b)聚合　计算 $U = \sum_{i=1}^{n} U_i, V = \sum_{i=1}^{n} V_i$,则 $\sigma = (U, V)$ 是 n 个签名者 $P_i(i = 1, 2, \cdots, n)$ 对消息 m_i 的聚合签名.

(6)验证算法　输入 $(m_i, ID_i, pk_{IDi})(i = 1, \cdots, n)$, $\sigma = (U, V)$,验证者计算 $T = H_2(P_{pub})$, $W = H_3(P, P_{pub})$, $h_i = H_4(m_i, ID_i, pk_{IDi})$,接受 σ 为 P_i 对消息 m_i 的签名当且仅当等式成立 $e(P, V) = e(U, T) e(P_{pub}, \sum_{i=1}^{n} h_i Q_i) e(\sum_{i=1}^{n} h_i pk_{IDi}, W)$.

3.2　安全性分析

本节给出具体的攻击方法,展示 Du-Huang 无证书聚合签名方案是不安全的. 攻击者 $A \in \{A_1, A_2\}$,(1)如果 $A = A_1$, A 满足 2.3 节 Game1 中(3)的两个条件:(a)至少有一个签名者 P_k 没有被 A 控制,同时 ID_k 没有经过公钥替换询问、部分私钥提取询问;(b)(m_k^*, P_k) 没有经过无证书签名询问;(2)如果 $A = A_2$,则 A 满足 2.3 节 Game2 中(3)的两个条件. 攻击过程如下:

(1)系统参数设置　挑战算法 C 运行系统参数生成算法,得到系统参数 $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$ 和系统主密钥 s. 将 $params$ 发送给攻击者 A.

(2)询问　攻击者进行签名询问,得到 P_k 对消息 m_k 的聚合签名 $\sigma_k = (U_k, V_k)$.

(3)伪造　为了伪造 $P_i(i = 1, 2, \cdots, n)$ 对消息 m_i^* 的签名,A 做如下操作:

(a)A 控制签名者 $P_i(i \in [1, n], i \neq k)$,故 A 能计算出 P_i 对 m_i^* 的合法签名 $\sigma_i^* = (U_i^*, V_i^*)$.

(b)A 伪造 P_k 对消息 m_k^* 的签名 σ_k^*:A 计算 $h_k = H_4(m_k, ID_k, pk_{IDk})$, $h_k^* = H_4(m_k^*, ID_k, pk_{IDk})$,随后计算 $V_k^* = V_k \cdot \frac{h_k^*}{h_k}$, $U_k^* = U_k \cdot \frac{h_k^*}{h_k}$,则 $\sigma_k^* = (U_k^*, V_k^*)$ 是 P_k 对消息 m_k^* 的签名.

(c)A 聚合签名:计算 $U^* = \sum_{i=1}^{n} U_i^*, V^* = \sum_{i=1}^{n} V_i^*$, $\sigma^* = (U^*, V^*)$ 是 $P_i(i = 1, 2, \cdots, n)$ 对消息 m_i^* 的聚合签名.

容易验证 $\sigma^* = (U^*, V^*)$ 是有效的无证书聚合签名,分析如下,验证者首先计算 $T = H_2(P_{pub})$, $W = H_3(P, P_{pub})$, $h_i^* = H_4(m_i^*, ID_i, pk_{IDi})$, $1 \leqslant i \leqslant n$. 然后验证:

$$
\begin{aligned}
e(P, V^*) &= e(P, \sum_{i=1}^{n} V_i^*) \\
&= e(P, \sum_{i=1, i\neq k}^{n} V_i^*) e(P, V_k^*) \\
&= (\prod_{i=1, i\neq k}^{n} e(P, V_i^*)) e(P, V_k \cdot \frac{h_k^*}{h_k}) \\
&= (\prod_{i=1, i\neq k}^{n} e(U_i^*, T) e(P_{pub}, h_i^* Q_i) \\
&\quad \cdot e(h_i^* pk_{IDi}, W)) e(P, (r_k T + h_k(d_{IDk} + x_k W) \frac{h_k^*}{h_k}) \\
&= (\prod_{i=1, i\neq k}^{n} e(U_i^*, T) e(P_{pub}, h_i^* Q_i) e(h_i^* pk_{IDi}, W)) \\
&\quad \cdot e(P, r_k T \frac{h_k^*}{h_k} + h_k^*(d_{IDk} + x_k W)) \\
&= (\prod_{i=1, i\neq k}^{n} e(U_i^*, T) e(P_{pub}, h_i^* Q_i) e(h_i^* pk_{IDi}, W)) \\
&\quad \cdot e(U_k^*, T) e(P_{pub}, h_k^* Q_k) e(h_k^* pk_{IDk}, W) \\
&= \prod_{i=1}^{n} e(U_i^*, T) e(P_{pub}, h_i^* Q_i) e(h_i^* pk_{IDi}, W) \\
&= e(\sum_{i=1}^{n} U_i^*, T) e(P_{pub}, \sum_{i=1}^{n} h_i^* Q_i) \\
&\quad \cdot e(\sum_{i=1}^{n} h_i^* pk_{IDi}, W) \\
&= e(U^*, T) e(P_{pub}, \sum_{i=1}^{n} h_i^* Q_i) e(\sum_{i=1}^{n} h_i^* pk_{IDi}, W)
\end{aligned}
$$

等式成立. 在攻击过程中,A 既没收到系统主密钥也没有执行替换公钥询问,故方案对任何类型的攻击者 A_1 或 A_2 都不具有不可伪造性.

文献[14]的安全性证明过程存在缺陷才导致上述攻击成立,本文具体分析文献[14]引理 1 的证明过程,引理 2 的分析与引理 1 类似,不再详述. 伪造阶段,A 输出 n 个消息-身份-公钥 (m_i^*, ID_i, pk_{IDi}) 的聚合签名 (U^*, V^*),易知 $V^* = U^* l^* + \sum_{i=1}^{n} h_i^* t_i^* P_{pub} + \sum_{i=1}^{n} j^* h_i^* pk_{IDi}^*$. 然而 A 伪造 (U^*, V^*) 时需要满足 Game1 中的两个条件,即至少一个签名者(假设为 $P_k(k \in [1, n])$)的身份 ID_k 没有同时提交给公钥替换询问和部分私钥提取询问,且 (m_k^*, P_k) 没有经过无证书签名询问,故 A 并不知道 V_k^* 也不知道 $t_k^* P_{pub}$,所以在伪造阶段,攻击者 A 并不能成功伪造出签名 V^*,更无法通过已知 V_k^* 求解

CDH 困难问题. Du-Huang 方案的安全性可归约为 CDH 问题的推导并不成立.

此外需要注意的是,本节对 Du-Huang 方案[14]的攻击方法不适用于 Zhou-Zhang 方案[15]. Du-Huang 方案将明文消息映射到有限域,而 Zhou-Zhang 在构造签名时,将明文消息映射到加法群,而加法群中不一定存在乘法逆元,因此无法使用本节所述的攻击方法去伪造 Zhou-Zhang 的无证书聚合签名.

4 一个高效的无证书聚合签名方案

本节将提出一个更加安全高效的无证书聚合签名方案,方案将任意选择的随机数 r_i 固定于部分私钥中,签名消息的随机性不依赖于 r_i,攻击者无法按照 3.2 节介绍的方法伪造签名消息. 此外,部分私钥和用户私钥都是有限域 Z_q^* 中的随机数,这一特点使得方案在验证时仅使用两次双线对运算. 最后我们将证明方案在随机预言模型下不可伪造.

4.1 具体方案

(1)系统参数生成算法 给定安全参数 k,KGC 选择 q 阶循环群 G_1,G_2,q 是素数满足 $q>2^k$,P 是 G_1 的生成元,$e:G_1\times G_1\rightarrow G_2$ 表示双线性映射. H_1,H_2,H_3 是安全 hash 函数 $H_1,H_2:\{0,1\}^*\rightarrow Z_q^*$,$H_3:\{0,1\}^*\rightarrow G_1$. KGC 随机选择 $s\in Z_q^*$,计算 $P_{pub}=sP$. 公开系统参数 $params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2,H_3\}$,保密系统主密钥 s.

(2)部分私钥提取算法 输入 $P_i(i=1,2,\cdots,n)$ 的身份 ID_i,KGC 验证 ID_i 后,选择随机数 $r_i\in Z_q^*$,计算 $R_i=r_iP$,$h_i=H_1(ID_i\parallel R_i)$,$d_i=r_i+h_is$,将部分私钥 d_i 秘密发送给 P_i,R_i 作为 P_i 公钥的一部分.

(3)用户密钥生成算法 $P_i(i=1,2,\cdots,n)$ 随机选择 $x_i\in Z_q^*$ 作为秘密值,计算 $pk_i=x_iP$,将 (pk_i,R_i) 作为公钥.

(4)签名算法 输入参数 $params$,$P_i(i=1,2,\cdots,n)$ 的身份 ID_i,私钥 (d_i,x_i) 和公钥 (pk_i,R_i),消息 m_i,不失一般性假设 P_i 对消息 m_i 进行如下签名:

(a) 计算 $T_i=H_2(m_i\parallel ID_i\parallel pk_i\parallel R_i\parallel P_{pub})$,$Q=H_3(P_{pub})$.

(b) 选择随机数 w_i,计算 $W_i=w_iP$.

(c) 计算 $\sigma_i=(T_ix_i+d_i+w_i)Q$,将 (σ_i,W_i) 作为 P_i 对消息 m_i 的签名.

(5)聚合 聚合人对 $P_i(i=1,\cdots,n)$ 发来的签名 (m_i,σ_i) 进行验证然后聚合.

***(a)*验证** 计算 $T_i=H_2(m\parallel ID_i\parallel pk_i\parallel R_i\parallel P_{pub})$,$Q=H_3(P_{pub})$,验证等式 $e(P,\sigma_i)=e(Q,T_ipk_i+R_i+h_iP_{pub}+W_i)$ 是否成立,若成立则接受 (σ_i,W_i) 否则终止算法.

***(b)*聚合** 计算 $\sigma=\sum_{i=1}^{n}\sigma_i$,$W=\sum_{i=1}^{n}W_i$,$(\sigma,W)$ 是 n 个签名者 $P_i(i=1,2,\cdots,n)$ 对不同消息 m_i 的聚合签名.

(6)验证算法 输入 $\sigma,W,(m_i,ID_i,pk_i,R_i)|_{i=1,\cdots,n}$,验证者计算 $Q=H_3(P_{pub})$,$T_i=H_2(m\parallel ID_i\parallel pk_i\parallel R_i\parallel P_{pub})$,接受 σ 为 P_i 对消息 m_i 的聚合签名当且仅当等式成立 $e(P,\sigma)=e(Q,\sum_{i=1}^{n}(T_ipk_i+R_i+h_iP_{pub})+W)$

4.2 方案分析

(1)正确性

方案的正确性证明如下.

证明 假设由签名方案得到聚合签名 (σ,V),则

$$\begin{aligned}e(P,\sigma)&=e(P,\sum_{i=1}^{n}\sigma_i)=e(P,\sum_{i=1}^{n}(T_ix_i+d_i+w_i)Q)\\&=e(P,\sum_{i=1}^{n}(T_ix_i+r_i+h_is+w_i)Q)\\&=e(Q,\sum_{i=1}^{n}(T_ix_i+r_i+h_is+w_i)P)\\&=e(Q,\sum_{i=1}^{n}(T_ipk_i+R_i+h_iP_{pub}+W_i))\\&=e(Q,\sum_{i=1}^{n}(T_ipk_i+R_i+h_iP_{pub})+W)\end{aligned}$$

(2)抗伪造性

下面证明在随机预言模型下,本方案对攻击者 A_1,A_2 都是不可伪造的.

定理 1 在随机预言模型下,如果第一类攻击者 A_1 能够以不可忽略的概率伪造出聚合签名,则 C 能以不可忽略的概率解决 CDH 问题.

证明 假设存在攻击者 A_1 满足 2.3 节 Game 1 中的条件,即 A_1 不对 P_k 的身份 ID_k 进行部分私钥询问,不对 (m_k^*,P_k) 进行无证书签名询问. 如果 A_1 能以不可忽略的概率 ε 攻破我们的方案,则挑战者 C 能利用 A_1 解决 CDH 问题. 即 C 已知 $P_1=aP,P_2=bP$,最终能输出 abP.

初始化 C 按照 4.1 节选择系统参数 $params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2,H_3\}$,其中 $P_{pub}=P_1$. C 将 $params$ 发送给攻击者 A_1. A_1 执行如下询问,为模拟询问 C 维护表 L_1,L_2,L_3 分别对应对 H_1,H_2,H_3 的询问,表 L_{k1},L_{k2} 分别对应部分私钥和秘密值的询问:

散列询问:

***H_1* 询问** A_1 输入 (ID_i,R_i),如果 L_1 包含 (ID_i,R_i,h_i) 则 C 返回 h_i 给 A_1. 否则 C 选择随机数 $h_i\in Z_q^*$,将 (ID_i,R_i,h_i) 写入 L_1,返回 h_i 给 A_1.

***H_2* 询问** A_1 输入 $(m_i,ID_i,pk_i,R_i,P_{pub})$,如果 L_2 包含 $(m_i,ID_i,pk_i,R_i,P_{pub},c_i,T_i)$,$C$ 返回 T_i 给 A_1. 否则,C 选择随机数 $c_i\in\{0,1\}$ 满足 $\Pr[c_i=1]=(1/(q_E+1))$,$\Pr[c_i=0]=(q_E/(q_E+1))$. 如果①$c_i=0$,C 选择随机数

$T_i \in Z_q^*$;否则②$c_i = 1$,C 计算 $T_i = -(r_i + w_i)/x_i$. C 返回 T_i 给 A_1,同时将$(m_i, ID_i, pk_i, R_i, P_{pub}, c_i, T_i)$写入 L_2.

H_3 询问　A_1 输入 P_{pub},如果 L_3 包含(P_{pub}, Q)则 C 返回 Q 给 A_1. 否则,C 令 $Q = P_2$ 并发送给 A_1,同时将(P_{pub}, Q)写入 L_3.

部分私钥询问　A_1 询问 ID_i的部分私钥. 如果①$c_i = 1$ 则失败退出;否则②$c_i = 0$,C 选择随机数 $d_i \in Z_q^*$,并计算 $R_i = d_iP - t_iP_{pub}$,最终 C 将(ID_i, d_i, R_i)添加至 L_{k1},并返回部分私钥(d_i, R_i)给 A_1. 其中部分私钥满足 $d_iP = R_i + H_1(ID_i \| R_i)P_{pub}$.

秘密值询问　A_1 询问 ID_i的秘密值. 如果 L_{k2}存在(ID_i, pk_i, x_i),则返回 x_i,否则 C 选择随机数 $x_i \in Z_q^*$,计算 $pk_i = x_iP$,将 x_i 返回给 A_1 同时将(ID_i, pk_i, x_i)写入 L_{k2}.

公钥询问　A_1 询问 ID_i的公钥. 如果 L_{k2}存在(ID_i, pk_i, x_i),则返回 pk_i,否则 C 选择随机数 $x_i \in Z_q^*$,计算 $pk_i = x_iP$,将 pk_i 返回给 A_1 同时将(ID_i, pk_i, x_i)写入 L_{k2}.

公钥替换询问　A_1 输入自己选取的公钥 pk'_i 替换 ID_i 的公钥. C 将$(ID_i, pk'_i, \perp)$写入 L_{k2}.

签名询问　A_1 询问(m_i, ID_i)的签名. C 在列表 L_{k1},L_{k2}查找 ID_i的部分私钥(ID_i, d_i, R_i)和秘密值(ID_i, pk_i, x_i). 随后 C 查找 L_1, L_2, L_3,如果①$c_i = 1$,C 报错并停止执行,否则②$c_i = 0$,C 返回签名 $\sigma_i = (T_ix_i + d_i + w_i)Q$.

伪造　最后 A_1 输出一个有效的 n 个消息-身份对(m_i^*, ID_i)的聚合签名(m_i^*, ID_i, σ^*). C 查找 L_1, L_2, L_3,如果 L_2 对应的 n 条记录$(m_i^*, ID_i^*, pk_i^*, R_i^*, P_{pub}, c_i^*, T_i^*)$中所有 $c_i^* = 0$ 则失败退出,否则假设$(m_k^*, ID_k^*, pk_k^*, R_k^*, P_{pub}, c_k^*, T_k^*)$的 $c_k^* = 1$. 根据等式 $e(\sigma^*, P) = e(\sum_{i=}^{n}(T_i^*pk_i^* + R_i^* + h_i^*P_{pub} + W_i^*), Q) \Rightarrow e(\sigma_k^*, P) = e(T_k^*pk_k^* + R_k^* + h_k^*P_{pub} + W_k^*, Q)$. 由 $c_k^* = 1$ 代入 $T_k^* = -(r_k^* + w_k^*)/x_k^*$ 得到 $e(\sigma_k^*, P) = e(h_k^*P_{pub}, Q)$,最终 C 得到 $abP = \sigma_k^*/h_k^*$. 所以,如果 A_1 能成功伪造合法的聚合签名,则挑战者 C 能够解决 CDH 困难问题.

挑战者 C 成功的条件为部分私钥询问,签名询问没有失败,且伪造聚合签名时至少有一个 $c_i^* = 1$,故 C 成功的概率 ε' 为 $\varepsilon' \geqslant \varepsilon(1 - (q_E/q_E + 1)^n)(q_E/q_E + 1)^{q_E+q_S}$,$\varepsilon$ 为 A_1 伪造签名成功的概率,q_E, q_S 分别为执行部分私钥询问和签名询问的次数.

定理 2　在随机预言模型下,如果第二类攻击者 A_2 能够以不可忽略的概率伪造出聚合签名,则 C 能以不可忽略的概率解决 CDH 问题.

证明　假设存在攻击者 A_2 满足 2.3 节 Game2 中的条件,如果 A_2 能以不可忽略的概率 ε 攻破我们的方案,则挑战者 C 能利用 A_2 解决 CDH 问题. 即 C 已知 $P_1 = aP, P_2 = bP$,最终能输出 abP.

初始化　C 按照 4.1 节选择系统参数 $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$,其中 $P_{pub} = sP$. C 将 $params$ 和系统主密钥 s 发送给攻击者 A_2. A_2 执行如下询问,为模拟询问 C 维护表 L_1, L_2, L_3 分别对应对 H_1, H_2, H_3 的询问,表 L_{k1}, L_{k2}分别对应部分私钥和秘密值的询问:

散列询问:

H_1 询问　A_2 输入(ID_i, R_i),如果 L_1 包含(ID_i, R_i, c_i, h_i)则 C 返回 h_i 给 A_2. 否则 C 选择随机数 $c_i \in \{0, 1\}$ 满足 $\Pr[c_i = 1] = (1/(q_E + 1))$,$\Pr[c_i = 0] = (q_E/(q_E + 1))$. 如果①$c_i = 0$,$C$ 选择随机数 $h_i \in Z_q^*$;否则②$c_i = 1$,C 计算 $h_i = -(r_i + w_i)/s$. C 返回 h_i 给 A_2,同时将(ID_i, R_i, c_i, h_i)写入 L_1.

H_2 询问　A_2 输入$(m_i, ID_i, pk_i, R_i, P_{pub})$,如果 L_2 包含$(m_i, ID_i, pk_i, R_i, P_{pub}, T_i)$,$C$ 返回 T_i 给 A_2. 否则,C 选择随机数 $T_i \in Z_q^*$ 返回给 A_2,同时将$(m_i, ID_i, pk_i, R_i, P_{pub}, T_i)$写入 L_2.

H_3 询问,部分私钥询问,秘密值询问,签名询问与定理 1 中挑战应答相同.

公钥询问　A_2 询问 ID_i的公钥. 如果 L_{k2}存在(ID_i, pk_i, x_i),则返回 pk_i. 否则,如果①$c_i = 0$,则 C 选择随机数 $pk_i \in Z_q^*$,否则②$c_i = 1$,则 C 计算 $pk_i = P_1$,将 pk_i 返回给 A_2 同时将(ID_i, pk_i, x_i)写入 L_{k2}.

伪造　最后 A_2 输出一个有效的 n 个消息-身份对(m_i^*, ID_i)的聚合签名(m_i^*, ID_i, σ^*). C 查找 L_1, L_2, L_3,如果 L_1 对应的 n 条记录$(ID_i^*, R_i^*, c_i^*, h_i^*)$中所有 $c_i^* = 0$ 则失败退出,否则假设$(ID_k^*, R_k^*, c_k^*, h_k^*)$的 $c_k^* = 1$. 根据等式 $e(\sigma^*, P) = e(\sum_{i=}^{n}(T_i^*pk_i^* + R_i^* + h_i^*P_{pub} + W_i^*), Q) \Rightarrow e(\sigma_k^*, P) = e(T_k^*pk_k^* + R_k^* + h_k^*P_{pub} + W_k^*, Q)$. 由 $c_k^* = 1$ 代入 $h_k^* = -(r_k^* + w_k^*)/s$ 得到 $e(\sigma_k^*, P) = e(T_k^*pk_k^*, Q)$,最终 C 得到 $abP = \sigma_k^*/T_k^*$. 所以,如果 A_2 能成功伪造合法的聚合签名,则挑战者 C 能够解决 CDH 困难问题.

挑战者 C 成功的条件为部分私钥询问,签名询问没有失败,且伪造聚合签名时至少有一个 $c_i^* = 1$,故 C 成功的概率 ε' 为 $\varepsilon' \geqslant \varepsilon(1 - (q_E/q_E + 1)^n)(q_E/q_E + 1)^{q_E+q_S}$,$\varepsilon$ 为 A_2 伪造签名成功的概率,q_E, q_S 分别为执行部分私钥询问和签名询问的次数.

(3)效率分析

将一次双线性运算记为 BP,群 G_1 的乘法运算记为 M,G_1 中元素的长度记为 L. 假设方案中有 n 个签名者. 可以看出本文方案最终的聚合签名为 σ,方案在验证时需要 2 次双线性运算和 $2n + 1$ 次加法运算,相比双线性运算和乘法运算,加法运算的时间较小可忽略不计,因

此我们可将方案的验证代价记为 2BP. 从表 1 可以看出本文方案的效率要高于已有方案[14,15]. 同时聚合签名的长度不随签名人数的变化而变化.

表 1 效率比较

方案	签名	验证	签名长度
文献[14]方案	$4n$M	4BP + $2n$M	$2L$
文献[15]方案	$3n$M	4BP + $2n$M	$2L$
本文方案	$3n$M	2BP	$2L$

5 结束语

聚合签名能够减少验证者的工作量,在资源受限的无线网络中有着重要应用. 杜红珍等利用双线性对提出一个高效的无证书聚合签名方案(Du-Huang 方案),并在随机预言模型下证明方案的安全性可归约 CDH 问题. 然而本文研究发现该方案难以抵抗伪造攻击,并具体指出其安全性证明存在的不足. 随后提出一个新的无证书聚合签名方案,相比 Du-Huang 方案,我们的方案计算量更小. 最后在随机预言模型下证明了方案的安全性.

参考文献

[1] Zhu H, Lin X, Lu R, et al. AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks[A]. Proceedings of the 8th International Conference on Communications[C]. IEEE, 2008. 1436 – 1440.

[2] Zhang C, Lu R, Lin X, et al. An efficient identity-based batch verification scheme for vehicular sensor networks [A]. Proceedings of INFOCOM 2008[C]. IEEE, 2008. 816 – 824.

[3] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[A]. Proceedings of EUROCRYPT 2003[C]. Berlin. Springer, 2003. 416 – 432.

[4] Lysyanskaya A, Micali S, Reyzin L, et al. Sequential aggregate signatures from trapdoor permutations[A]. Proceedings of EUROCRYPT 2004[C]. Berlin: Springer, 2004. 74 – 90.

[5] Gentry C, Ramzan Z. Identity-based aggregate signatures [A]. Proceedings of Public Key Cryptography-PKC 2006 [C]. Berlin: Springer, 2006. 257 – 273.

[6] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A]. Proceedings of ASIACRYPT 2003[C]. Berlin: Springer, 2003. 452 – 473.

[7] Tian M M, Yang W, Huang L S. Cryptanalysis and improvement of a certificateless multi-proxy signature scheme [J]. Fundamenta Informaticae, 2014, 129(4): 365 – 375.

[8] Tian M M, Huang L S, Yang W. Practical certificateless short signature scheme[J]. International Journal of Electronic Security and Digital Forensics, 2014, 6(3): 204 – 218.

[9] Gong Z, Long Y, Hong X, et al. Two certificateless aggregate signatures from bilinear maps[A]. Proceedings of the IEEE SNPD 2007[C]. IEEE, 2007. 188 – 193.

[10] Zhang L, Zhang F T. A new certificateless aggregate signature scheme[J]. Computer Communications, 2009, 32(6): 1079 – 1085.

[11] Zhang L, Qin B, Wu Q, et al. Novel efficient certificateless aggregate signatures[A]. Proceedings of AAECC 2009 [C]. Berlin: Springer, 2009. 235 – 238.

[12] Zhang L, Qin B, Wu Q, et al. Efficient many-to-one authentication with certificateless aggregate signatures[J]. Computer Networks, 2010, 54(14): 2482 – 2491.

[13] Xiong H, Guan Z, Chen Z, et al. An efficient certificateless aggregate signature with constant pairing computations [J]. Information Sciences, 2013, 219: 225 – 235.

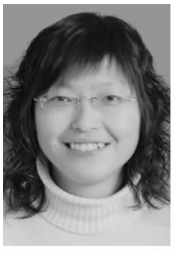
[14] 杜红珍, 黄梅娟, 温巧燕. 高效的可证明安全的无证书聚合签名方案[J]. 电子学报, 2013, 41(1): 72 – 76.
DU Hong-zhen, HUANG Mei-juan, WEN Qiao-yan. Efficient and Provably-secure certificateless aggregate signature scheme[J]. Acta Electronica Sinica, 2013, 41(1): 72 – 76. (in Chinese)

[15] Zhou M, Zhang M, Wang C, et al. CCLAS: A practical and compact certificateless aggregate signature with share extraction[J]. International Journal of Network Security, 2014, 16(2): 157 – 164.

[16] He D B, Tian M M, Chen J H. Insecurity of an efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2014, 268: 458 – 462.

[17] Cheng L, Wen Q Y, Jin Z, et al. Cryptanalysis and improvement of a certificateless aggregate signature scheme [J]. Information Sciences, 2015, 295: 337 – 346.

作者简介



许 艳 女,1982 年生,现为中国科学技术大学计算机科学与技术学院博士生,研究方向为信息安全和密码学.
E-mail: xuyan@ahu.edu.cn

黄刘生 男,1957 年生,现为中国科学技术大学计算机科学与技术学院教授,博士生导师,主要研究方向为无线传感网络、信息安全和分布式计算.