高效的可证明安全的无证书聚合签名方案

杜红珍[1],黄梅娟[1],温巧燕[2]
(1.宝鸡文理学院数学系,陕西宝鸡 721013;2.北京邮电大学网络与交换技术国家重点实验室,北京 100876)

摘 要: 利用双线性对构造了一个高效的无证书聚合签名方案,在随机预言机模型下给出了方案的安全性证明,其安全性基于计算 Diffie-Hellman 难题.与已有的无证书聚合签名方案相比,本文方案更能提高签名验证与传输效率,因聚合签名的验证只需要计算 4 个双线性对,签名的长度是固定的,仅有 320bits,是目前最短的无证书聚合签名.

关键词: 无证书公钥密码体制; 聚合签名; 计算 Diffie-Hellman 难题; 双线性对
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2013)01-0072-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.01.014

Efficient and Provably-Secure Certificateless Aggregate Signature Scheme

DU Hong-zhen[1], HUANG Mei-juan[1], WEN Qiao-yan[2]
(1. *Department of Mathematics, Baoji University of Arts and Sciences, Baoji, Shaanxi* 721013, *China*;
2. *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: This paper proposes an efficient certificateless aggregate signature scheme from bilinear pairings. Its security proof is given in the random oracle model and it can be reduced to computational Diffie-Hellman problem. Compared with the existing certificateless aggregate signature schemes, our scheme drastically improves the efficiency of signature communication and verification since the verification algorithm only requires 4 pairings, and the length of the signature generated by our scheme is only about 320 bits, which is the shortest certificateless aggregate signature.

Key words: certificateless public key cryptography; aggregate signature; computational Diffie-Hellman problem; bilinear pairings

1 引言

为了简化基于证书的公钥密码体制中的密钥管理以及证书撤消问题,Shamir[1]提出了基于身份的公钥密码体制(Identity-based Public Key Cryptography, ID-PKC).目前已有很多基于身份的加密、签名方案[2~5]被提出,但 ID-PKC 存在 1 个固有的缺陷,即密钥托管问题.为了解决该问题,Al-Riyami 和 Paterson[6]于 2003 年提出了无证书公钥密码体制(Certificateless Public Key Cryptography, CLPKC),CLPKC 有效地解决了 ID-PKC 的密钥托管问题,同时也避免了证书公钥体制中的存储和管理证书的问题,对 CLPKC 的研究是密码学的前沿和热点.

聚合签名(Aggregate Signature)的概念是由 Boneh 等[7]在 2003 年提出的,所谓聚合签名,就是 $n(>1)$个用户 $P_i(1\leqslant i\leqslant n)$分别对 n 个不同的消息 m_i 进行签名,这 n 个签名可以被聚合成一个签名,而验证方只需要检验聚合后的这一个签名便可以确认是否是 P_i 对 m_i 做的签名.目前,已有若干无证书聚合签名(Certificateless Aggregate Signature, CLAS)方案[8~10]被提出,在文献[8]中,Gong 等构造了两个 CLAS 方案,但在方案Ⅰ中,聚合签名的长度随签名人数的增加而变长,还有签名的验证计算量很大.方案Ⅱ仍是效率低,签名验证需要计算$(n+2)$个很费时的双线性对,且这两个方案的安全性证明是在弱的敌手模型假设下进行的,其安全性有待进一步检测.2009 年,Zhang 等[9]提出了一个 CLAS 方案,但方案还是效率低,生成的聚合签名的长度依赖于签名人数,且签名验证需计算$(n+3)$个双线性对.2010 年,Zhang 等[10]又在文献[9]的基础上给出了一个改进方案,该方案与文献[9]的方案相比效率提高了,但仍有不足:如需要密钥生成中心 KGC 为每个签名人生成的部分私钥增加成 2 个群元素,且每次签名都要求每个签名人维护一个共同的状态信息.

针对以上不足,本文利用双线性对构造了一个 CLAS 方案,它在随机预言机模型和计算 Diffie-Hellman

收稿日期:2011-12-28;修回日期:2012-08-14
基金项目:国家自然科学基金(No.61170270);陕西省自然科学基础基金(No.2010JQ8027);陕西省教育厅科学研究基金(No.12JK1003)

困难假设下是存在性不可伪造的,跟已有文献[8~10]相比较,本文方案的优点如下:(1)聚合签名长度是固定的,不会随签名人数的改变而改变,其长度仅有320bits,是目前最短的无证书聚合签名;(2)签名的验证仅需4个双线性对的计算,是目前效率最高的.

2 无证书聚合签名的定义及安全模型

2.1 CLAS 定义

定义 1 1个CLAS方案由6个算法构成:Setup, Partial-Private-Key-Extract, UserKeyGen, CL-Sign, Aggregate和Verify.

Setup 该算法由KGC执行,输入安全参数 k,输出系统主密钥 s 和系统参数 params.

Partial-Private-Key-Extract 由KGC执行,输入 params, s 和用户身份 ID_i,返回部分私钥 d_{IDi}.

UserKeyGen 由用户 ID_i 执行,输入 params、ID_i 和秘密值 x_i(x_i 由用户 ID_i 选取),输出秘密值/公钥(x_i/pk_{IDi}).

CL-Sign 由用户 ID_i 执行,输入 params, d_{IDi}, x_i, pk_{IDi}及消息 m_i,输出(普通)签名 σ_i.

Aggregate 由聚合人执行,输入 n 个有效的身份-消息-公钥-签名对(ID_i, m_i, pk_{IDi}, σ_i)($1\leqslant i\leqslant n$),输出这 n 个签名 σ_i 的聚合签名 σ.

Verify 输入 params, n 个身份-消息-公钥对(ID_i, m_i, pk_{IDi})($1\leqslant i\leqslant n$)及聚合签名 σ,输出"1"表示签名有效,而"0"则签名无效.

2.2 CLAS 的安全模型

定义 2 一个CLAS方案在适应性选择消息攻击下是存在性不可伪造的(EUF-CLAS-CMA),如果存在敌手 A_1、A_2 在以下两个Game中获胜的概率是可以忽略的.

Game 1

挑战者 C 输入安全参数 k,运行 Setup 算法产生系统主密钥 s 和系统参数 params,发送 params 给 A_1,秘密保存 s. A_1 询问以下预言机:

– Hash 询问:A_1 可以访问方案中所有 Hash 预言机并得到 Hash 值.

– Partial-Private-Key-Extract 询问:当 A_1 查询用户 ID_i 的部分私钥时,C 运行 Partial-Private-Key-Extract 算法生成部分私钥 d_{IDi}并返回给 A_1.

– Secret-Value 询问:当 A_1 询问 ID_i 的秘密值时,C 运行 UserKeyGen 算法生成 x_i 并返回给 A_1,若 ID_i 的公钥已被替换,则输出"⊥".

– Public-Key 询问:当查询 ID_i 的公钥时,C 运行 UserKeyGen 算法产生 pk_{IDi}并返回给 A_1.

– Replace-Public-Key 询问:对任意用户 ID_i, A_1 能用自己选取的公钥 pk'_{IDi}代替 ID_i 的公钥 pk_{IDi}.

– CL-Sign 询问:输入消息 m_i,身份 ID_i 和公钥 pk_{IDi}, C 运行 CL-Sign 算法生成签名 σ_i 并返回给 A_1.

最后,A_1 输出 1 个有效的身份-公钥-聚合签名(ID_i^*, pk_{IDi}^*, σ^*)($1\leqslant i\leqslant n$),且满足以下条件,则 A_1 获胜:

(1)至少有一个 $ID_I^*\in\{ID_1^*, ID_2^*, \cdots ID_n^*\}$ 没有既提交给 Replace-Public-Key 预言机又同时提交给 Partial-Private-Key-Extract 预言机;

(2)(m_I^*, ID_I^*)没有经过 CL-Sign 询问.

Game 2

挑战者 C 输入安全参数 k,运行算法 Setup 来产生系统主密钥 s 和系统参数 params,然后发送 params 和 s 给 A_2. A_2 询问以下预言机:

– Hash 询问, – Secret-Value 询问, – Public-Key 询问和 – CL-Sign 询问:分别与 Game 1 中的相应预言机应答相同.

最后,A_2 输出 1 个有效的身份-公钥-聚合签名(ID_i^*, pk_{IDi}^*, σ^*)($1\leqslant i\leqslant n$),且满足以下条件,则 A_2 获胜:

(1)至少有一个 $ID_I^*\in\{ID_1^*, ID_2^*, \cdots ID_n^*\}$ 没有经过 Secret-Value 询问;

(2)(m_I^*, ID_I^*)没有经过 CL-Sign 询问.

3 本文方案

3.1 方案构造

本节提出了1个CLAS方案,由以下6个算法构成:

Setup 给定安全参数 k,KGC 选择两个阶为大素数 $q>2^k$ 的群 G_1 和 G_2, P 是群 G_1 的 1 个生成元,一个修正的 Weil 对映射 $e: G_1\times G_1\rightarrow G_2$($e$ 具有对称性),4 个安全 Hash 函数 $H_1\sim H_3: \{0,1\}^*\rightarrow G_1$, $H_4: \{0,1\}^*\rightarrow Z_q^*$,再选随机数 $s\in Z_q^*$ 作为系统主密钥,令系统公钥 $P_{pub}=sP$. 公开系统参数 params: $\{k, e, G_1, G_2, P, P_{pub}, H_1, H_2, H_3, H_4\}$,秘密保存 s.

Partial-Private-Key-Extract 对身份 ID_i,KGC 计算其部分私钥 $d_{IDi}=sQ_i$,其中 $Q_i=H_1(ID_i)$.

UserKeyGen 用户 ID_i 选随机数 $x_i\in Z_q^*$ 作为秘密值,计算 $pk_{IDi}=x_iP$ 作为公钥.

CL-Sign 给定 params,消息 m_i,用户 P_i 的身份 ID_i 和公钥 pk_{IDi}(便于描述,本文假定用户 P_i 要签名的消息就是 m_i),P_i 签名如下:

(1)选随机数 $r_i\in Z_q^*$,计算 $U_i=r_iP$, $T=H_2(P_{pub})$, $W=H_3(P, P_{pub})$, $h_i=H_4(m_i, ID_i, pk_{IDi})$;

(2)计算 $V_i=r_iT+h_i(d_{ID_i}+x_iW)$.

则 $\sigma_i=(U_i, V_i)$就是 P_i 对消息 m_i 的签名.

Aggregate 聚合人收到 n 个签名 $\sigma_i=(U_i,V_i)(1\leqslant i\leqslant n)$后,计算 $T=H_2(P_{pub})$, $W=H_3(P,P_{pub})$和 $h_i=H_4(m_i,ID_i,pk_{IDi})$,接受 σ_i 当且仅当

$e(P,V_i)=e(U_i,T)e(P_{pub},h_iQ_i)e(h_ipk_{IDi},W)$成立.

验证 n 个 σ_i 有效后,计算 $U=\sum_{i=1}^{n}U_i$ 和 $V=\sum_{i=1}^{n}V_i$,则 $\sigma=(U,V)$就是身份-公钥为$(ID_i/pk_{IDi})(1\leqslant i\leqslant n)$的 n 个签名人对 n 个消息 m_i 的聚合签名.

Verify 给定$(m_i,ID_i,pk_{IDi})(1\leqslant i\leqslant n)$及聚合签名 $\sigma=(U,V)$,验证人操作如下:

1)计算 $T=H_2(P_{pub})$, $W=H_3(P,P_{pub})$,

$h_i=H_4(m_i,ID_i,pk_{IDi})(1\leqslant i\leqslant n)$;

2)接受 σ 当且仅当

$$e(P,V)=e(U,T)e(P_{pub},\sum_{i=1}^{n}h_iQ_i)e(\sum_{i=1}^{n}h_ipk_{IDi},W).$$

3.2 方案的安全性分析

定理 1 在随机预言机模型和计算 Diffie-Hellman 困难假设下,本文的 CLAS 方案在适应性选择消息攻击下是存在性不可伪造的(EUF-CLAS-CMA).

定理 1 由引理 1 和引理 2 推导出.

引理 1 在随机预言机模型下,假定敌手 A_1 在时间 t 内以不可忽略的优势 ε 攻破了本文方案,记 A_1 访问 H_1 预言机, Partial-Private-Key-Extract 预言机, Public-Key 预言机, CL-Sign 预言机的次数分别为 q_{H_1}, q_E, q_{pk}, q_S, 则存在一个算法 C, 以 $\varepsilon'\geqslant\varepsilon\left(1-(\frac{q_E}{q_E+1})^n\right)\left(\frac{q_E}{q_E+1}\right)^{q_E+q_S}$的优势,在时间 $t'<t+(q_{H_1}+q_E+q_{pk}+3q_S+2n+2)t_{sm}+t_{inv}$内解决 CDH 难题, t_{sm}是计算群上 1 个标量乘所用时间, t_{inv}是计算 Z_q^* 上 1 个求逆的时间.

证明 算法 C 调用A_1 为子程序在 1 个概率多项式时间内解决 CDH 难题.设(aP,bP)是群 G_1 上一个任意的 CDH 问题的实例, C 将扮演为 A_1 的挑战者进行以下 Game:

C 运行 Setup 算法,定义系统公钥 $P_{pub}=aP$,生成系统参数 params:$\{k,e,G_1,G_2,P,P_{pub},H_1\sim H_4\}$,发送 params 给 A_1, A_1 执行以下询问:

Hash 询问 为了模拟 Hash 询问, C 需维护四张列表 L_1,L_2,L_3,L_4 分别跟踪对 H_1,H_2,H_3,H_4 的询问.

***H_1* 询问** 当 A_1 输入 $ID_i(1\leqslant i\leqslant q_{H_1})$, C 调出列表 L_1,若 L_1 中有记录(ID_i,Q_i,t_i,c),则返回 Q_i.否则 C 任选 $t_i\in Z_q^*$,抛掷偏心硬币 $c\in\{0,1\}(\Pr[c=0]=\frac{q_E}{q_E+1},\Pr[c=1]=\frac{1}{q_E+1})$,若 $c=0$,定义 $Q_i=t_iP$,否则 $Q_i=t_i(bP)$,添加(ID_i,Q_i,t_i,c)到 L_1 中,返回 Q_i 给 A_1.

***H_2* 询问** 当 A_1 输入 P_{pub}, C 调出 L_2,若 L_2 中有记录(P_{pub},l,T),则输出 T,否则选一随机数 $l\in Z_q^*$,定义 $T=lP$,添加(P_{pub},l,T)到 L_2 中,返回 T.

***H_3* 询问** 当 A_1 输入(P,P_{pub}), C 调出L_3,若 L_3 中有(P,P_{pub},j,W),则输出 W,否则选一随机数 $j(\neq l)\in Z_q^*$,定义 $W=jP$.返回 W,添加(P,P_{pub},j,W)到 L_3 中.

***H_4* 询问** A_1 输入(m_i,ID_i,pk_{IDi}),若 L_4 中已有相应的记录,返回以前定义的值.否则,任选 $h_i\in Z_q^*$,添加(m_i,ID_i,pk_{IDi},h_i)到 L_4 中,返回 h_i.

Partial-Private-Key-Extract 询问 给定 ID_i, C 从 L_1 中调出相应的记录(ID_i,Q_i,t_i,c),若 $c=1$,则失败退出.否则,计算 $d_{ID_i}=t_i(aP)$,添加(ID_i,d_{ID_i})到列表 E^{list} 中,返回 d_{ID_i}.

Public-Key 询问 当查询用户 ID_i 的公钥时, C 调出列表pk^{List},若已有相应的记录,返回以前定义的值.否则随机选 $x_i\in Z_q^*$,计算 $pk_{IDi}=x_iP$,返回 pk_{IDi}给A_1,添加(m_i,ID_i,x_i,pk_{IDi})到 pk^{List}中.

Secret-Value 询问 当询问 ID_i 的秘密值时, C 调出pk^{List},返回以前定义的秘密值.否则随机选 $x_i\in Z_q^*$,计算 $pk_{IDi}=x_iP$,返回 x_i 给 A_1,添加(m_i,ID_i,x_i,pk_{IDi})到 pk^{List}中.如果 ID_i 的公钥被替换,则输出"$\perp$".

Replace-Public-Key 询问 A_1 能用自己选取的公钥 pk'_{IDi}代替 ID_i 的公钥 pk_{IDi},当 A_1 输入(ID_i,pk'_{IDi})时, C 添加$(m_i,ID_i,\perp,pk'_{IDi})$到 pk^{List}中.

CL-Sign 询问 当 A_1 输入消息-身份-公钥(m_i,ID_i,pk_{IDi})查询签名时, C 调出列表 L_1,L_2,L_3,找出相应的记录(ID_i,Q_i,t_i,c)和(P_{pub},l,T),(P,P_{pub},j,W),若 $c=0$, C 调出 L_4,找到(m_i,ID_i,pk_{IDi},h_i),任选元素 $U_i\in G_1$,计算 $V_i=lU_i+h_it_iP_{pub}+jh_ipk_{IDi}$,返回$(U_i,V_i)$给 A_1,否则 C 失败退出.

最后, A_1 停止模拟,输出一个有效的在 $n(\leqslant q_{H1})$个消息-身份-公钥$(m_i^*,ID_i^*,pk_{IDi}^*)(1\leqslant i\leqslant n)$上的聚合签名$(U^*,V^*)$,且该签名满足 2.2 节 Game 1 中的两个条件. C 调出列表 L_1,找出相应的 n 个记录$(ID_i^*,Q_i^*,t_i^*,c^*)(1\leqslant i\leqslant n)$,如果这 n 个数据中所有 $c^*=0$ 则失败退出.否则这 n 条记录只要有 1 个 $c^*=1$ 就可以进行以下计算:假设是(ID_I^*,Q_I^*,t_I^*,c^*)中的 $c^*=1$, C 在列表 L_2 中找出(P_{pub},l^*,T^*),在列表 L_3 中找出(P,P_{pub},j^*,W^*),在列表 L_4 中找出$(m_i^*,ID_i^*,pk_{IDi}^*,h_i^*)(1\leqslant i\leqslant n)$,根据等式:

$$e(P,V^*)=e(U^*,T^*)e(P_{pub},\sum_{i=1}^{n}h_i^*Q_i^*)\cdot e(\sum_{i=1}^{n}h_i^*pk_{IDi}^*,W^*)$$

即 $e(P,V^*)=e(U^*,l^*P)e(\sum_{i=1,i\neq I}^{n}h_i^*t_i^*P+h_I^*t_I^*bP,aP)e(\sum_{i=1}^{n}j^*h_i^*pk_{IDi}^*,P)$

即 $e\left(P,V-l^*U-\sum_{i=1,i\neq I}^{n}h_i^*t_i^*(aP)-\sum_{i=1}^{n}j^*h_i^*pk_{IDi}^*\right)=e(P,h_I^*t_I^*abP)$.

$abP=(h_I^*t_I^*)^{-1}\left(V-l^*U-\sum_{i=1,i\neq I}^{n}h_i^*t_i^*(aP)-\sum_{i=1}^{n}j^*h_i^*pk_{IDi}^*\right)$

C 能求出 abP 值,从而解决 CDH 难题.

下面分析 C 在 Game 中成功的概率:

定义 4 个事件 E_1,E_2,E_3,E_4.其中 E_1 表示 C 回应 Partial-Private-Key-Extract 询问时没有失败;E_2 表示 C 回应 CL-Sign 询问时没有失败;E_3 表示 A_1 成功的伪造了 1 个消息-身份-公钥$(m_i^*,ID_i^*,pk_{IDi}^*)(1\leqslant i\leqslant n)$上的聚合签名$(U^*,V^*)$;$E_4$ 为 n 条记录$(ID_i^*,Q_i^*,t_i^*,c^*)(1\leqslant i\leqslant n)$中至少有一个 $c^*=1$.

显然 $\Pr[E_1]\geqslant\left(\frac{q_E}{q_E+1}\right)^{q_E}$;$\Pr[E_2|E_1]\geqslant\left(\frac{q_E}{q_E+1}\right)^{q_S}$;

$\Pr[E_3|E_1\wedge E_2]\geqslant\varepsilon$;

$\Pr[E_4|E_1\wedge E_2\wedge E_3]\geqslant 1-\left(\frac{q_E}{q_E+1}\right)^{n}$;

则 $\Pr[E_1\wedge E_2\wedge E_3\wedge E_4]=\Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_1\wedge E_2]\Pr[E_4|E_1\wedge E_2\wedge E_3]\geqslant\varepsilon\left(1-(\frac{q_E}{q_E+1})^{n}\right)\left(\frac{q_E}{q_E+1}\right)^{q_E+q_S}$.

当事件 E_1,E_2,E_3,E_4 都发生时,C 获胜,他的概率为 $\varepsilon'\geqslant\varepsilon\left(1-(\frac{q_E}{q_E+1})^{n}\right)\left(\frac{q_E}{q_E+1}\right)^{q_E+q_S}$,显然 C 在 Game 中所用时间为

$$t'<t+(q_{H_1}+q_{H_4}+q_E+q_{pk}+3q_S+n+3)t_{sm}+t_{inv}.$$

引理 2　在随机预言机模型下,假定敌手 A_2 在时间 t 内以不可忽略的优势 ε 攻破了本文方案,记 A_2 访问 H_1 预言机,Partial-Private-Key-Extract 预言机,Public-Key 预言机,CL-Sign 预言机的次数分别为 q_{H_1},q_E,q_{pk},q_S,则存在一个算法 C,以 $\varepsilon'\geqslant\varepsilon\left(1-(\frac{q_E}{q_E+1})^{n}\right)\left(\frac{q_E}{q_E+1}\right)^{q_{pk}+q_S}$ 的优势,在时间 $t'<t+(q_{H_1}+q_E+q_{pk}+3q_S+2n+2)t_{sm}+t_{inv}$ 内解决 CDH 问题.

证明　C 运行 Setup 算法,定义 $P_{pub}=sP$,生成 params:$\{k,e,G_1,G_2,P,P_{pub},H_1\sim H_4\}$,,将 params 和系统主密钥 s 发给 A_2,A_2 执行以下询问:

H_1 询问　输入 ID_i,C 调出 L_1.若 L_1 中有(ID_i,t_i,Q_i),则返回 Q_i.否则 C 任选 $t_i\in Z_q^*$,令 $Q_i=t_iP$,添加(ID_i,t_i,Q_i)到 L_1 中,返回 Q_i 给 A_2.

$H_2\sim H_4$ 询问　与引理 1 中相应预言机应答相同.

Partial-Private-Key-Extract 询问　给定 ID_i,C 从 L_1 中调出(ID_i,t_i,Q_i),计算 $d_{ID_i}=t_isP$.添加(ID_i,d_{ID_i})到 E^{list}中,返回 d_{ID_i}.

Public-Key 询问　当查询 ID_i 公钥时,C 抛掷偏心硬币 $c\in\{0,1\}$,若 $c=0$,随机选 $x_i\in Z_q^*$,定义 $pk_{IDi}=x_iP$,否则定义 $pk_{IDi}=x_i(aP)$,返回 pk_{IDi}给 A_2,添加(ID_i,x_i,pk_{IDi},c)到 pk^{List}中.

Secret-Value 询问,CL-Sign 询问　与引理 1 中相应预言机应答相同.

最后,若 A_2 输出伪造的有效签名(U^*,V^*),则 C 能求出 abP 值,解决 CDH 难题.

$$abP=(jh_It_I)^{-1}\left(V-lU-\sum_{i=1}^{n}sh_it_iP-\sum_{i=1,i\neq I}^{n}jbh_ix_iP\right)$$

3.3　方案的效率分析

若用 s 表示群 G_1 上 1 次标量乘计算,p 表示 1 个双线性对的计算,L 表示 G_1 群元素的长度,$\{0,1\}^*$ 是 1 个 0、1 比特串,则本文签名长度仅为 $2L$,签名与验证计算总量为 $6ns+4p$,文献[8]中方案Ⅰ的签名长度$(n+1)L$,总计算量 $2ns+(2n+1)p$,方案Ⅱ的签名长度 $3L$,总计算量 $4ns+(n+2)p$,文献[9]的签名长度$(n+1)L$,总计算量 $3ns+(n+3)p$,文献[10]的签名长度 $2L+\{0,1\}^*$,总计算量 $7ns+5p$.

显然,本文方案就聚合签名的长度及计算量来说,其效率明显高于文献[8~10]中方案.

4　结论

利用双线性对提出了一个新的无证书聚合签名方案,经证明该方案在适应性选择消息攻击下是存在性不可伪造的,且方案就计算量与签名长度来说是目前效率最高的.以后的工作是构造在标准模型下可证明安全的无证书聚合签名方案.

参考文献

[1] A Shamir. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology-CRYPTO 1984 [C]. Berlin: Springer, 1984. 47 – 53.

[2] 王竹,戴一奇,叶顶锋.普适安全的基于身份的签名机制[J].电子学报,2011,39(7):1613 – 1617.
WANG Zhu, DAI Yi-qi, YE Ding-feng. Universally composable identity-based signature[J]. Acta Electronica Sinica, 2011, 39(7):1613 – 1617. (in Chinese)

[3] Du Hongzhen, Wen Qiaoyan. An efficient identity-based short signature scheme from bilinear pairings[A]. Proceedings of CIS 2007[C]. USA: IEEE, 2007, 725 – 729.

[4] 蔡永泉,张雪迪,姜 楠.一种新的基于身份的门限签名方案[J].电子学报,2009,37(4A):102 – 105.
CAI Yong-quan, ZHANG Xue-di, JIANG Nan. A novel identity-based threshold signature [J]. Acta Electronica Sinica, 2009, 37(4A): 102 – 105. (in Chinese)

[5] 李进,张方国,王燕鸣.两个高效的基于分级身份的签名方案[J].电子学报,2007,35(1):150 – 152.
LI Jin, ZHANG Fang-guo, WANG Yan-ming. Two efficient hierarchical identity-based signature schemes [J]. Acta Electronica Sinica, 2007, 35(1): 150 – 152. (in Chinese)

[6] S S Al-Riyami, KG Paterson. Certificateless Public Key Cryptography[A]. Advances in Cryptology-Asiacrypt 2003[C]. Berlin: Springer, 2003. 452 – 474.

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

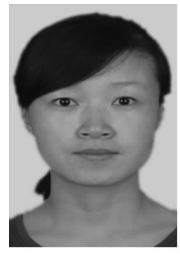
[8] Z Gong, Y Long, et al. Two certificateless aggregate signatures from bilinear maps[A]. Proceedings of IEEE SNPD 2007[C]. USA: IEEE, 2007. 188 – 193.

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

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

作者简介

杜红珍 女,1978 年 12 月出生,陕西扶风人,副教授、博士,主要从事密码学、数字签名研究.
E-mail: hongzhendu@163.com



黄梅娟 女,1980 年 3 月出生,陕西岐山人,讲师、硕士,主要从事密码学研究.