基于中国剩余定理的前向安全的聚合签名方案

韦性佳,芦殿军*
(青海师范大学 数学与统计学院,青海 西宁 810008)

摘 要:随着信息技术的发展,信息安全研究成为目前国内外急需解决的突出问题。数字签名技术作为信息安全领域的关键技术之一,能有效地解决由于密钥泄露与敌手攻击等对用户造成的危害。该文利用中国剩余定理,结合双线性对技术,基于椭圆曲线循环群提出了一种具有前向安全性质的聚合签名方案。该方案具备如下特点:第一,利用强 RSA 假设实现了签名信息的前向安全性,即使敌手获取第 j 个时间段的签名信息,也无法得到关于之前签名的任何信息;第二,实现可信中心与签名用户的双向验证,可以有效甄别出方案中的伪造者,提高方案的安全性;第三,在随机预言模型下,证明了该方案抗存在性伪造;第四,方案的实现基于椭圆曲线循环群,能有效减少签名的计算量与存储空间。

关键词:中国剩余定理;前向安全性;聚合签名;强 RSA 假设;随机预言模型;抗存在性伪造
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2021)04-0137-05
doi:10.3969/j.issn.1673-629X.2021.04.023

Forward Secure Aggregated Signature Scheme Based on Chinese Remainder Theorem

WEI Xing-jia, LU Dian-jun*
(School of Mathematics and Statistics, Qinghai Normal University, Xining 810008, China)

Abstract: With the development of information technology, information security research has become an outstanding problem that needs to be solved urgently at home and abroad. As one of the key technologies in the field of information security, digital signature technology can effectively solve the harm caused to users due to key leakage and adversary attacks. Using the Chinese residual theorem, combined with bilinear pairing technology, based on the elliptic curve cyclic group, we propose an aggregate signature scheme with forward security properties. The scheme has the following characteristics: Firstly, using the strong RSA assumption to achieve forward security of the signature information, even if the adversary obtains the signature information of the j time period, he cannot get any information about the previous signature; secondly, the implementation of the trusted center and the signature user two-way verification can effectively identify the forgers in the scheme and improve the safety of the scheme; thirdly, under the random oracle model, it is proved that the scheme is resistant to existence forgery; fourthly, the realization of the scheme is based on the elliptic curve cyclic group, effectively reducing the amount of signature calculation and storage space.

Key words: Chinese remainder theorem; forward security; aggregated signature; strong RSA hypothesis; random oracle model; anti-existence forgery

0 引 言

随着时代的发展,信息安全问题目前已经成为制约中国乃至全球经济发展的重要问题。随着中国第一部《密码法》的颁布,信息安全领域的发展迎来了新的机遇和挑战。

数字签名作为信息安全领域的重要内容之一,已经成为国内外研究的热点课题之一[1-2]。

聚合签名作为一种多方参与的数字签名方案,在保障数据的安全传递与高效存储方面具有较强的实践价值[3-4]。聚合签名的概念最早由 Boneh 等人[5]在2003年的欧密会上提出,并且基于双线性对技术构造了第一个抗存在性伪造的聚合签名方案,对聚合签名的发展具有深远的影响。但是 Shao 等人[6]通过安全性分析指出 Boneh 等人的方案在安全性方面存在漏洞,可以被模拟敌手攻击。Cheon 等[7]提出了第一个基于身份的聚合签名方案,将身份信息作为验证工具,

收稿日期:2020-06-08 **修回日期**:2020-10-11
基金项目:青海省基础研究计划项目(2019-ZJ-7099)
作者简介:韦性佳(1991-),男,助教,硕士,研究方向为代数组合与密码学、数字签名;通信作者:芦殿军(1970-),男,教授,研究方向为代数组合与密码学、多项式理论、数字签名等。

提高了方案的安全性。近年来,区块链与云计算技术的不断发展,聚合签名已经广泛应用于许多现实领域,2018 年苑超等人[8]将区块链中共识算法的改进算法 dBFT 为研究对象,结合聚合签名技术以及双线性映射技术对该算法的共识过程进行优化,有效降低了区块链系统签名的空间复杂度,为区块链的发展提供了重要的实践依据。2020 年杨小东等人[9]针对车载自组网(VANET)中的隐私泄露和签名验证效率较低等问题,结合聚合签名技术,提出了一种基于身份聚合签名的车载自组网消息认证方案,有效缩短了车辆对通信消息的认证响应时间。

在实践应用中,由于敌手计算能力的提升以及签名成员的变动导致签名过程是动态的,在这个背景下,前向安全性理论由此产生。1997 年,Anderson[10]首次提出了前向安全性理论,解决了传统数字签名中因秘密的被动或主动泄露对系统安全所带来的隐患问题。1999 年,Bellare 和 Miner[11]提出了第一个具有前向安全性质的数字签名方案,为前向安全性理论的进一步发展奠定了基础。随着前向安全性理论的不断发展,各种前向安全的数字签名方案不断提出[12-14]。2018 年,王岩等人[15]基于中国剩余定理提出了一种动态门限签名方案,该方案实现了签名私钥的前向安全性,能有效地抵抗移动攻击,同时具有较高的效率与实践价值。同年,Jihye K 等人[16]提出了一种前向安全的顺序聚合签名方案,该方案可以有效地应用于计算机审核日志的安全管理中,为计算机网络安全提供了重要的安全保障。2019 年,洪璇等人[17]基于中国剩余定理提出一种前向安全的群签名方案,为该文提供了重要的研究思路。

但是,目前将前向安全性结合到聚合签名方案中的文献相对较少,由于聚合签名具有较强的实践价值,该文基于中国剩余定理提出了一种具有前向安全性质的聚合签名方案,方案的签名,验证过程基于椭圆曲线循环群,能有效降低数据的存储空间。同时,在随机预言模型下,方案具有抗存在性伪造的特性。

1 基础知识

1.1 双线性映射

令 $(G_1,+)$,$(G_2,\cdot)$ 是两个循环群,且 $|G_1|=|G_2|=q$(q 是大素数),P 是 G_1 的生成元,存在双线性映射 $e:G_1\times G_1\to G_2$ 满足下列的性质:

(1)双线性性:$\forall P,Q,Q_1,Q_2\in G_1,a,b\in Z_q^*$ 有如下的性质:

(i) $e(aP,bQ)=e(P,Q)^{ab}$;

(ii) $e(P,Q_1+Q_2)=e(P,Q_1)e(P,Q_2)$。

(2)非退化性:$\exists P\in G_1$,使得 $e(P,P)\neq 1$。

(3)可计算性:$\forall P,Q\in G_1$,存在有效的算法能够计算 $e(P,Q)$。

1.2 椭圆曲线离散对数问题(ECDLP 问题)

给定一个椭圆曲线加法群 G_1,已知任意的两个元素 $P,Q\in G_1$,求解 $a\in Z_q^*$ 使得 $Q=aP$ 成立,则称该问题就是椭圆曲线离散对数问题。

1.3 计算性 Diffie-Hellman(CDH)问题

对于 $\forall x,y\in Z_q^*$,给定 $P,xP,yP\in G_1$,其中 P 是 G_1 的生成元,称计算 $xyP\in G_1$ 为 G_1 上的计算性 Diffie-Hellman(CDH)问题,并且对于一个多项式敌手 O,定义 O 在时间 T 内针对 G_1 中 CDH 问题的优势为:$\mathrm{adv}_{\mathrm{CDH}}(T)=\Pr[O(P,xP,yP)=xyP:P,xP,yP\in G_1]$。

计算性 Diffie-Hellman(CDH)假设:对于任意一个概率多项式时间运算 O,$\mathrm{adv}_{O,G_1}^{\mathrm{CDH}}$ 是可忽略的。

1.4 强 RSA 问题与假设

强 RSA 问题:给定一个 RSA 模数 $N=pq$,随机选择 $z\in_R Z_N^*$,计算 $r,y\in Z_N^*$,使得满足条件 $y^r=z\bmod N$(其中 $r>1,y\in Z_n^*$),称为强 RSA 问题。

强 RSA 假设:在不清楚 N 的因子分解的前提下,强 RSA 问题是难于求解的。

1.5 前向安全性理论

前向安全性理论:(1)参与者首先通过可信中心的广播信息得到验证子秘密 SP_i;(2)通过秘密信道从可信中心得到并保密自己的初始子秘密 S_{i0};(3)将秘密的有效期分为 T 个时间段,1,2,…,T。在整个有效期内验证子秘密 SP_i 保持不变,但第 j 个时段子秘密 S_{ij} 随着时间段 j 的改变而变换,具体如下:进入第 j 个时段时,参与者首先通过非交互式方式计算出 $S_{ij}=f(S_{i(j-1)})$,其中 f 是一个单向函数(类似于 Hash 函数),在计算出 S_{ij} 后,参与成员 H_i 立即删除前一时间段的子秘密 $S_{i(j-1)}$,这样就保证了即使攻击者获得了第 j 个时段的子秘密 S_{ij} 后也不能获得 $S_{i0},S_{i1},\cdots,S_{i(j-1)}$ 的任何信息。

密钥更新流程如图 1 所示。

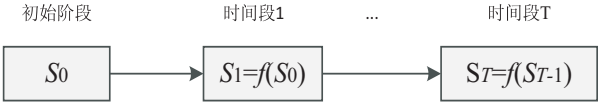

图 1 密钥更新流程

2 方案的构造

2.1 系统初始化

(1)PKG:密钥分配中心;

(2)$\{P_1,P_2,\cdots,P_n\}$:签名用户集合;

(3)G_1:有限域上的乘法循环群,G_2:椭圆曲线上

的加法循环群, P : G_2 的生成元;

(4)抗碰撞的哈希函数 $H_1, H_2: \{0,1\}^* \times G_2 \to G_1$;

(5) T 时间周期,分为 $1,2,\cdots,T$ 时间段;

(6)选择 $s \in Z_q^*$ 作为系统主密钥,计算 $P_{\text{pub}} = sP$,最终 PKG 公开 $\Omega = \{e, G_1, G_2, P, P_{\text{pub}}, H_1, H_2, T\}$,秘密保存 s。

2.2　私钥生成运算

(1)PKG 选择 $q_1, q_2, \cdots, q_n \in Z_q^*$, $q = q_1 q_2 \cdots q_n$,其中 q_i 是大素数,且 $(q_i, q_j) = 1$,当 $i \neq j$ 时,然后将 $q_1, q_2, \cdots, q_n$ 分别发送给用户 $P_1, P_2, \cdots, P_n$。

(2)用户 P_i 选择 $r_i \in Z_{q_i}^*$,在第 j 个时间段计算:

(i) $P_{i,j} = x_{i,j} P$, $i = 1,2,\cdots,n; j = 0,1,2,\cdots,T$;

(ii) $y_{i,0} = H_1(P_{i,0}, \text{ID}_i)$,公开 $(P_{i,j}, y_{i,0})$;

(iii)PKG 收到 $(P_{i,j}, y_{i,0})$ 后:

(a)利用这 n 个同余方程式计算 c:

$$\begin{cases} c = y_{1,0} \bmod q_1 \\ c = y_{2,0} \bmod q_2 \\ \cdots \\ c = y_{n,0} \bmod q_n \end{cases}$$

利用中国剩余定理可以计算该同余方程组的解为:

$$c \equiv y_{1,0} Q_1' Q_1 + y_{2,0} Q_2' Q_2 + \cdots + y_{n,0} Q_n' Q_n \bmod q,$$

其中, $q = q_1 q_2 \cdots q_n$, $Q_i = q/q_i$, $Q_i Q_i' \equiv 1 \bmod q_i$, $i = 1,2,\cdots,n$。

(b)PKG 计算 $P^{(i)} = q_i P$, $k_i = s^{y_{i,0}}$, $(i = 1,2,\cdots,n)$ 公开 $P^{(i)}$,秘密保存 k_i,通过秘密信道发送给用户 P_i。

2.3　签名运算

(1)签名用户 P_i 选择 $r_i \in_R Z_q^*$,对于待签名的消息 $m_i (i = 1,2,\cdots,n)$,计算:

(i) $U_i = r_i P$;

(ii) $h_i = H_2(m_i, \text{ID}_i, U_i)$;

(iii) $V_{i,j} = x_{i,j} h_i P_{\text{pub}} + r_i k_i^{-y_{i,0}} P$。

(2)则 $\sigma_{i,j} = (U_i, V_{i,j})$ 就是用户 P_i 在第 j 个时间段对消息 m_i 的签名。

2.4　聚合签名运算

(1)聚合签名者首先验证 n 个单一签名 $\sigma_{i,j} = (U_i, V_{i,j})$ 的有效性,通过检验如下 n 个等式是否成立:

$$e(P, V_{i,j}) = e(h_i P_{i,j} + U_i, P_{\text{pub}}), i = 1,2,\cdots,n$$

(2)如果上述等式都有效,则聚合者计算:

(i) $U = \sum_{i=1}^{n} U_i$, $V_j = \sum_{i=1}^{n} V_{i,j}$;

(ii)则 $\sigma_j = (U, V_j)$ 就是第 j 个时间段对消息 $m = \{m_1, m_2, \cdots, m_n\}$ 的聚合签名。

2.5　聚合验证运算

验证者收到聚合签名 $\sigma_j = (U, V_j)$, $m = \{m_1, m_2, \cdots, m_n\}$, $\text{ID} = \{\text{ID}_1, \text{ID}_2, \cdots, \text{ID}_n\}$ 后:

(1)计算 $h_i = H_2(m_i, \text{ID}_i, U_i)$;

(2)验证等式:

$$e(P, V_j) = e(\sum_{i=1}^{n} h_i P_{i,j}, P_{\text{pub}}) e(U, P_{\text{pub}})$$

2.6　签名者的加入

假设存在一个用户 B 想要成为合法的签名者,首先 B 向可信中心 PKG 发出申请,PKG 为其选择大素数 $q_{n+1} \in Z_q^*$,然后发送给用户 B,用户 B 选择自己的初始签名私钥 $x_{n+1,0}$,计算 $P_{n+1,0} = x_{n+1,0} P$, $y_{n+1,0} = H(P_{n+1,0}, \text{ID}_{n+1})$,发送 $y_{n+1,0}$ 给 PKG,PKG 重新计算 c, $P_{\text{pub}} = sP$, $P^{(n+1)} = q_{n+1} P$, $k_{n+1} = s^{y_{n+1,0}}$,秘密保存 k_{n+1},通过秘密信道发送给用户 B。

2.7　签名者撤销

如果有签名成员 P_k 未通过聚合签名者的验证,则说明该签名者是伪造者,因此可信中心 PKG 需要撤销该成员,具体如下:PKG 将 P_k 发送过来的 $y_{k,0}$ 修改为 $y_{k,0}'$,重新计算 c,而其他签名用户信息不需再改变。

2.8　密钥更新

对于第 j 个时间段的签名用户私钥 $x_{i,j}$,在第 $j+1$ 个时间段的私钥为 $x_{i,j+1} = x_{i,j}^2 \bmod q_i$,更新完后,签名用户立即销毁第 j 个时间段的签名私钥 $x_{i,j}$。

3　方案的正确性与安全性

3.1　方案的正确性

定理 1:方案在聚合签名阶段的验证是正确的,即等式: $e(P, V_{i,j}) = e(h_i P_{i,j} + U_i, P_{\text{pub}})$, $i = 1,2,\cdots,n$ 成立。

证明:因为 $V_{i,j} = x_{i,j} h_i P_{\text{pub}} + r_i k_i^{-y_{i,0}} P$,利用双线性对性质有:

$$\begin{aligned} e(P, V_{i,j}) &= e(P, x_{i,j} h_i P_{\text{pub}} + r_i k_i^{-y_{i,0}} P) = \\ &\quad e(P, x_{i,j} h_i P_{\text{pub}}) e(P, r_i k_i^{-y_{i,0}} P) = \\ &\quad e(x_{i,j} P, h_i P_{\text{pub}}) e(r_i P, (s^{y_{i,0}})^{-y_{i,0}} P) = \\ &\quad e(x_{i,j} P, h_i P_{\text{pub}}) e(r_i P, sP) = \\ &\quad e(x_{i,j} h_i P, P_{\text{pub}}) e(U_i, P_{\text{pub}}) = \\ &\quad e(U_i + x_{i,j} h_i P, P_{\text{pub}}) \end{aligned}$$

证毕。

定理 2:方案在聚合验证阶段的验证是正确的,即等式: $e(P, V_j) = e(\sum_{i=1}^{n} h_i P_{i,j}, P_{\text{pub}}) e(U, P_{\text{pub}})$ 成立。

证明:因为 $U = \sum_{i=1}^{n} U_i$, $V_j = \sum_{i=1}^{n} V_{i,j}$,则有:

$$\begin{aligned} e(P, V_j) &= e(P, \sum_{i=1}^{n} V_{i,j}) = \\ &\quad e(P, \sum_{i=1}^{n} x_{i,j} h_i P_{\text{pub}} + r_i k_i^{-y_{i,0}} P) = \end{aligned}$$

$$e(P,\sum_{i=1}^{n}x_{i,j}h_iP_{\text{pub}})e(P,\sum_{i=1}^{n}r_ik_i^{-y_{i,0}}P)$$

$$\{\prod_{i=1}^{n}e(P,x_{i,j}h_iP_{\text{pub}})\}e(P,\sum_{i=1}^{n}r_ik_i^{-y_{i,0}}P)=$$

$$\{\prod_{i=1}^{n}e(P,x_{i,j}h_iP_{\text{pub}})\}e(\sum_{i=1}^{n}r_iP,sP)=$$

$$\{\prod_{i=1}^{n}e(x_{i,j}P,h_iP_{\text{pub}})\}e(\sum_{i=1}^{n}U_i,P_{\text{pub}})=$$

$$\prod_{i=1}^{n}e(P_{i,j},h_iP_{\text{pub}})e(U,P_{\text{pub}})=$$

$$e(\sum_{i=1}^{n}h_iP_{i,j},P_{\text{pub}})e(U,P_{\text{pub}})$$

3.2 方案的安全性

定理 3:方案具有前向安全性。

该方案的前向安全性的保障基于签名私钥的前向安全性,若敌手掌握了第 j 个时间段的所有的签名信息 $\sigma_j=(U,V_j)$ 以及签名私钥 $x_{i,j},r_i,k_i$,目的是想获取之前的签名信息 $\sigma_k=(U,V_k),k=1,2,\cdots,j-1$。首先,根据条件,由于 $V_{i,k}=x_{i,k}h_iP_{\text{pub}}+r_ik_i^{-y_{i,0}}P$,则必须获得私钥 $x_{i,k},r_i,k_i$,虽然敌手已经掌握私钥 r_i,k_i,但是 $x_{i,j}=x_{i,k}^{2^{j-k}}\bmod q_i$,求解 $x_{i,k}$ 将面对解决强 RSA 假设,由于强 RSA 假设是难解问题,因此敌手无法获取关于 $\sigma_k=(U,V_k),k=1,2,\cdots,j-1$ 的任何信息,这就保证了签名信息的前向安全性。

定理 4:方案实现了可信中心与签名用户的双向验证。

可信中心与签名用户的双向验证分为两个方面:

第一:可信中心的诚实性。对于签名用户 P_i 要验证可信中心 PKG 的诚实性,通过如下的等式:

$k_i^{-y_{i,0}}P=P_{\text{pub}}$,若等式成立,则说明 PKG 是诚实的,假设有人冒充 PKG,选择 k_i' 发送给用户 P_i,但是由于 $k_i=s^{y_{i,0}}$,$k_i^{-y_{i,0}}P=(s^{y_{i,0}})^{-y_{i,0}}P=sP=P_{\text{pub}}$,而 s 是 PKG 自己的私钥,则用户 P_i 验证等式必然有 $(k_i')^{-y_{i,0}}P\neq P_{\text{pub}}$,则可以证明可信中心 PKG 的诚实性。

第二:签名用户的诚实性。对于可信中心 PKG 要验证签名用户 P_i 的诚实性,通过如下的过程:

(1)可信中心计算 $P_C=cP$,然后公开 P_C;

(2)可信中心或者用户 $P_j(i\neq j)$ 通过等式 $(y_{i,0}\bmod p_i)P=P_C$ 验证用户 P_i 的诚实性,假设有人冒充签名用户 P_i 选择 $y_{i,0}'$,由于 $(y_{i,0}\bmod p_i)P=cP=P_C$,这里 c 是由 PKG 利用中国剩余定理结合签名用户发送的 $y_{i,0},(i=1,2,\cdots,n)$ 产生,则 PKG 或者用户 $P_j(i\neq j)$ 验证上述等式必然有 $(y_{i,0}'\bmod p_i)P\neq P_C$,则可以证明签名用户 P_i 的诚实性。

定理 5:在随机预言模型下,假设存在一个敌手 A 以不可忽略的优势 ε 攻破了该方案,则存在一个算法 C,以优势 $\varepsilon'>\varepsilon+negl(n)$ 内解决 CDH 问题。

证明:由定理可知,敌手 A 通过调用算法 C,在一个概率多项式时间内解决了 CDH 难题。假设 (aP,bP) 是椭圆曲线加法循环群 G_1 上 CDH 难题的一个实例,则算法 C 的目标就是输出该 CDH 问题的解 abP:

(1)C 维护三张列表 L_1,L_2,E^{list} 分别保存对 H_1,H_2,私钥的询问,然后 C 运行系统初始化算法,定义系统的公钥 $P_{\text{pub}}=aP$,生成系统参数 $\Omega=\{e,G_1,G_2,P,P_{\text{pub}},H_1,H_2,T\}$,并将其发送给敌手 A;

(2)敌手 A 收到系统参数后,执行如下询问:

(i) H_1 询问。

敌手 A 以 $(\text{ID}_i,P_{i,0})$ 作为输入,C 调出列表 L_1,若列表中有记录则返回定义的值,否则选择 $y_{i,0}'\in Z_{q_i}^*$,添加 $(y_{i,0}',\text{ID}_i,P_{i,0})$,$i=1,2,\cdots,n$ 到列表 L_1 中,最后返回 $y_{i,0}'$ 给敌手 A。

(ii) H_2 询问。

敌手 A 以 (m_i,ID_i,U_i) 作为输入,C 调出列表 L_2,若列表中有记录则返回定义的值,否则选择 $h_i'\in Z_q^*$,添加 $(m_i,\text{ID}_i,U_i,h_i')$,$i=1,2,\cdots,n$ 到列表 L_2 中,最后返回 h_i' 给敌手 A。

(iii)私钥解析询问。

敌手 A 以 $\text{ID}_i,P_{i,0}$ 作为输入,C 从列表 L_1 中调出记录 $(y_{i,0}',\text{ID}_i,P_{i,0})$,如果列表 E^{list} 中存在记录,则返回记录,否则计算 $k_i'=a^{y_{i,0}'}$,添加到列表 E^{list} 中,任选 $t_i\in Z_q^*$,计算 $P_{i,j}=t_ibP$,最后返回 $k_i',P_{i,j}$ 给敌手 A。

(iv)签名询问。

当以 (ID_i,m_i) 进行签名询问时,C 调出列表 L_1,L_2,E^{list},任选 $\alpha_{i,j}\in Z_q^*$,计算 $V_{i,j}'=\alpha_{i,j}P_{\text{Pub}}$,则计算 $U_i'=(k_i')^{y_{i,0}'}(V_{i,j}'-h_i'aP_{i,j})$,由单个验证等式得:

$$e(P,V_{i,j}')=e(h_i'P_{i,j}+U_i',P_{\text{pub}})=e(h_i'P_{i,j}+V_{i,j}'-ah_i'P_{i,j},P_{\text{pub}})$$

$$\Leftrightarrow e(P,\alpha_{i,j}P_{\text{pub}})=e(h_i't_ibP+V_{i,j}'-ah_i't_ibP,P_{\text{pub}})\Leftrightarrow e(\alpha_{i,j}P,aP)=e(h_i't_ibP+V_{i,j}'-ah_i't_ibP,P_{\text{pub}})$$

$$\Leftrightarrow e(\alpha_{i,j}P,P_{\text{pub}})=e(h_i't_ibP+V_{i,j}'-h_i't_iabP,P_{\text{pub}})\Leftrightarrow\alpha_{i,j}P=h_i't_ibP+V_{i,j}'-h_i't_iabP$$

$$\Leftrightarrow h_i't_iabP=h_i't_ibP+V_{i,j}'-\alpha_{i,j}P$$

$$\Leftrightarrow abP=(h_i't_i)^{-1}(h_i't_ibP+V_{i,j}'-\alpha_{i,j}P)=bP+(h_i't_i)^{-1}(\alpha_{i,j}aP-\alpha_{i,j}P)$$

最终,C 输出 abP 作为对敌手 A 的挑战的应答,因此 C 解决了 CDH 难题的一个实例。

定理 6:方案可以抗存在性伪造。

由定理 5 可知,假设存在敌手以不可忽略的优势伪造了该方案的签名,则说明 CDH 也能以不可忽略的优势被解决,当时 CDH 问题是一个难解问题,故不存在敌手 C 在多项式时间内能破解该方案,因此方案是抗存在性伪造。

4　效率分析

本方案的效率与文献[18]进行比较,如表 1 所示,其中 T_S 表示标量乘法, T_E 表示双线性运算, T_R 表示指数运算, $|G_1|$ 加法循环群的阶。

表 1　方案效率比较

运算	MPO 方案[18]	文中方案
Sign	$T_S + T_R + T_E$	$3T_S$
Verify	$T_S + T_E$	$T_S + 2T_E$
Signature size	$n \mid G_1 \mid$	$2 \mid G_1 \mid$
Forward security	No	Yes

通过比较发现,该文在签名阶段与验证阶段相较文献[18]效率相对较高,同时提出的方案签名的长度是固定的,而文献[18]签名长度不固定,随着签名人数的增加呈现线性增长,这也体现了聚合签名方案的优势:能有效降低数据的存储空间。

5　结束语

目前结合中国剩余定理构造的聚合签名方案相对较少,由于聚合签名方案的优越性,该文在文献[15,17]的基础上,基于中国剩余定理,提出了一种新的具有前向安全性质的聚合签名方案。然后对方案的安全性与正确性进行了详细的分析,在随机预言模型下证明了方案抗存在性伪造,同时实现了签名方案的可撤销性,签名用户与可信中心的双向验证性以及签名信息的前向安全性等特性。最后通过方案的效率分析,证明方案具有较好的运行效率。

参考文献:

[1] ZHANG C M, ZHU Y, CHEN J J, et al. Practical quantum digital signature with configurable decoy states[J]. Quantum Information Processing, 2020, 19(5): 1-7.

[2] KHURANA M, SINGH H. Two level phase retrieval in fractional Hartley domain for secure image encryption and authentication using digital signatures[J]. Multimedia Tools and Applications, 2020, 79: 13967-13986.

[3] KAMILI A, OGUNDOYIN S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks[J]. Journal of Information Security and Applications, 2019, 44(FEB.): 184-200.

[4] LU Y, LI J G. A forward-secure certificate-based signature scheme with enhanced security in the standard model[J]. Ksii Transactions on Internet and Information Systems, 2019, 13(3): 1502-1522.

[5] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Proceedings of the 22nd international conference on theory and applications of cryptographic techniques. Warsaw, Poland: Springer-Verlag, 2003: 416-432.

[6] SHAO Z. Enhanced aggregate signatures from pairings[C]// Information security and cryptology; lecture notes in computer science. Beijing: [s. n.], 2005: 140-149.

[7] CHEON J H, KIM Y, YOON H J. A new ID-based signature with batch verification[J]. Trends in Mathematics Information Center for Mathematical Sciences, 2005, 8(1): 119-131.

[8] 苑　超,徐蜜雪,斯雪明. 基于聚合签名的共识算法优化方案[J]. 计算机科学,2018,45(2):53-56.

[9] 杨小东,裴喜祯,安发英,等. 基于身份聚合签名的车载自组网消息认证方案[J]. 计算机工程,2020,46(2):170-174.

[10] ANDERSON R. Two remarks on public-key cryptology[C]//Fourth ACM conference on computer and communications security. Zurich, Switzerland: ACM, 1997.

[11] BELLARE M, MINER S K. A forward-secure digital signature scheme[C]//Proceedings of the 19th annual international cryptology conference on advances in cryptology. Santa Barbara, California, USA: Springer, 1999: 431-448.

[12] 徐　潜,谭成翔,冯　俊,等. 基于格的前向安全无证书数字签名方案[J]. 计算机研究与发展,2017,54(7):1510-1524.

[13] 左黎明,胡凯雨,张梦丽,等. 一种具有双向安全性的基于身份的短签名方案[J]. 信息网络安全,2018(7):47-54.

[14] 程亚歌,胡明生,公　备,等. 具有强前向安全性的动态门限签名方案[J]. 计算机工程与应用,2020,56(5):125-134.

[15] 王　岩,侯整风,章雪琦,等. 基于中国剩余定理的动态门限签名方案[J]. 计算机应用,2018,38(4):1041-1045.

[16] JIHYE K, HYUNOK O. FAS: forward secure sequential aggregate signatures for secure logging[J]. Information Sciences, 2018, 471: 115-131.

[17] 洪　璇,张绪霞. 基于中国剩余定理的前向安全群签名方案[J]. 计算机应用研究,2020,37(9):2806-2810.

[18] MESHRAM C Y, POWAR P L, OBAIDAT M S. An UF-IB-SS-CMA protected online/offline identity-based short signature technique using PDL[J]. Procedia Computer Science, 2016, 93: 847-853.