可公开验证可更新的多秘密共享方案

尚雪娇, 杜伟章
(长沙理工大学 计算机与通信工程学院, 长沙 410114)

摘 要: 针对现有的多秘密共享方案不能同时满足秘密份额的动态更新和可公开验证性的问题,提出一种可公开验证可更新的多秘密共享方案。该方案利用单向散列链构造更新多项式,使得参与者的秘密份额能够定期更新,并且在秘密分发的同时生成验证信息,任何人都可以根据公开信息对秘密份额和更新份额的有效性进行验证,及时检测成员之间的相互欺诈行为。分析表明,在椭圆曲线上的离散对数问题和计算性 Diffie-Hellman 问题困难的假设下,该方案能有效地抵抗内外部攻击,具有较好的安全性。

关键词: 多秘密共享; 动态更新; 可公开验证性; 单向散列链; Diffie-Hellman 问题
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3794-03
doi:10.3969/j.issn.1001-3695.2013.12.071

Publicly verifiable and renewable multi-secret sharing scheme

SHANG Xue-jiao, DU Wei-zhang
(*College of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha* 410114, *China*)

Abstract: In order to solve the problem that the proactive refreshment of secret shares and public verifiability could not be satisfied simultaneously in previous multi-secret sharing schemes, this paper proposed a publicly verifiable and renewable multi-secret sharing scheme. It constructed the updated polynomials by a one-way hash chain, which could make secret shares be updated periodically, and generated the verification information during the process of secret distribution. According to the public information, anyone could verify the validity of secret shares and renewed shares. Cheating of dealer and participants could be detected in time. Under the assumptions of elliptic curve discrete logarithm problem (ECDLP) and computational Diffie-Hellman problem (CDLP), this scheme can effectively resist internal and external attacks and has better security.

Key words: multi-secret sharing; proactive refreshment; public verifiability; one-way hash chain; Diffie-Hellman problem

0 引言

秘密共享是现代密码学的重要研究内容,在密钥托管、电子商务、电子投票等领域有着广泛的应用。秘密共享体制最早是由 Shamir[1] 和 Blakley[2] 于 1979 年分别基于 Lagrange 插值多项式和射影几何理论提出的。其基本思想是将共享秘密 s 分割成 n 份(每一份称为一个秘密份额),并分发给 n 个参与者持有,当且仅当 t 个或 t 个以上参与者合作才能重构秘密。为了防止不诚实的分发者和参与者的欺诈行为,Chor 等人[3] 于 1985 年提出了可验证秘密共享(verifiable secret sharing, VSS)方案。在可验证秘密共享方案中,参与者本人可以验证自己所得到的秘密份额的正确性,但不能验证其他参与者的秘密份额的有效性。Stadler[4] 于 1996 年提出了可公开验证秘密共享(publicly verifiable secret sharing, PVSS)的概念。可公开验证秘密共享方案允许任何人对参与者的秘密份额的有效性进行验证,而且验证过程中不会泄露共享秘密的任何信息。

2011 年,张建中等人[5] 提出了一个公开可验证的多秘密共享方案,该方案利用双线性对的双线性特性使任何一方都可以验证秘密份额的正确性。文献[6]基于双线性对的性质,给出了一个可验证可更新的秘密共享方案。该方案利用单向散列链构造更新多项式,使得秘密份额能够定期更新;但该方案不具有可公开验证性,一次秘密共享过程只能共享一个秘密。文献[7]提出了一种基于双线性对的可公开验证秘密共享方案,该方案利用双线性对的性质实现了秘密份额的可公开验证,但该方案的秘密份额不能动态更新。

近年来,虽然学者们提出了不少新的秘密共享方案[8~11],但目前还没有满足秘密份额可以动态更新并具有可公开验证性的多秘密共享方案被提出。本文基于双线性对的性质,构造了一个可公开验证可更新的多秘密共享方案。该方案通过对秘密份额和更新份额的加密,使秘密分发不需要安全信道,利用公开的验证信息和双线性对的性质实现了秘密份额的公开验证,并且一次秘密共享过程可以共享多个秘密,秘密份额能够定期更新,在一定程度上提高了方案的安全性和实用价值。

1 预备知识

1.1 双线性对

定义 1 设 G_1、G_2 是阶为 q(q 为素数)的加法循环群和乘法循环群,假设 G_1 和 G_2 上的离散对数问题是难解的。对任意的 $a, b \in Z_q^*$,如果映射 $e: G_1 \times G_1 \to G_2$ 满足下列性质,则称该映射为双线性映射:

a)双线性性,对任意 $P, Q \in G_1$,有 $e(aP, bQ) = e(P, Q)^{ab}$。

b)非退化性,存在 $P, Q \in G_1$,使得 $e(P, Q) \neq 1$。

收稿日期: 2013-03-23; **修回日期**: 2013-04-27

作者简介:尚雪娇(1988-),女,河南周口人,硕士研究生,主要研究方向为信息安全(wbjsxj_2012@163.com);杜伟章(1965-),女,湖南长沙人,教授,硕导,博士,主要研究方向为密码学、纠错编码、计算数学.

c)可计算性,对任意 $P,Q\in G_1$,存在有效算法计算 $e(P,Q)$。

1.2 GDH 群

定义 2 设 G 是阶为 q(q 为素数)的加法循环群,其生成元为 P,对任意的 $a,b,c\in Z_q^*$,定义如下数学问题:

a)离散对数问题(DLP),给定(P,aP),求 a。

b)计算性 Diffie-Hellman 问题(CDHP),给定(P,aP,bP),计算 abP。

c)判定性 Diffie-Hellman 问题(DDHP),给定(P,aP,bP,cP),判定 $c=ab \bmod q$ 是否成立。

如果在群 G 上,DDHP 是易解的,而 CDHP 难解,则称群 G 为 GDH 群。

1.3 单向散列链

定义 3 设单向散列函数为 H,随机选取种子 $\alpha\in Z_q^*$,通过递归散列运算 $H^k(\alpha)=H(H^{k-1}(\alpha))$得到一系列散列值 α,$H(\alpha),H^2(\alpha),\cdots,H^N(\alpha)$称为单向散列链,其中 $H^N(\alpha)$称为散列链的根。在不知道 α 的情况下,获得 $H^k(\alpha)$,无法得到 $H^{k-1}(\alpha)$。

2 方案描述

设 D 为秘密分发者,参与者集合 $P=\{P_1,P_2,\cdots,P_n\}$,$S_1,S_2,\cdots,S_m$ 为共享的 m 个秘密。

2.1 系统初始化

D 选取阶为 q(q 为素数)的加法循环群 G_1 和乘法循环群 G_2,它们之间存在双线性映射 $e:G_1\times G_1\to G_2$,P、Q 为 G_1 的生成元,选取系统私钥 $s\in Z_q^*$,计算系统公钥 $P_{pub}=sP$。哈希函数 $H:Z_q^*\to Z_q^*$,$H_1:G_2\to Z_q^*$,随机选取 $\alpha\in Z_q^*$,通过递归散列运算 $H^k(\alpha)=H(H^{k-1}(\alpha))$生成单向散列链 $L:\alpha,H(\alpha),H^2(\alpha),\cdots,H^N(\alpha)$,公布$(q,P,Q,P_{pub},e,H,H_1)$。

参与者 $P_i(i=1,2,\cdots,n)$随机选取私钥 $x_i\in Z_q^*$ 及公开身份信息 $ID_i\in[m+1,q-1]$,计算公钥 $R_i=x_iP$,并且对不同的参与者 P_i 和 P_j 有 $ID_i\neq ID_j$,$R_i\neq R_j$。

2.2 秘密分发

a)参与者 P_i 随机选取秘密份额 $s_i^{(0)}\in Z_q^*$,计算 $a_i=s_i^{(0)}H_1(e(x_iP_{pub},Q))$,$M_{1i}^{(0)}=s_i^{(0)}Q(i=1,2,\cdots,n)$,公布数据信息$(a_i,M_{1i}^{(0)})$。

b)D 利用私钥 s 解密 $a_i=s_i^{(0)}H_1(e(x_iP_{pub},Q))$得到 $s_i^{(0)}=a_i(H_1(e(sR_i,Q)))^{-1}$,并确保 $s_i^{(0)}\neq s_j^{(0)}(i\neq j)$,否则要求参与者重新选取。

c)D 根据点$(k,S_k)_{k=1,2,\cdots m}$和$(ID_i,s_i^{(0)})_{i=1,2,\cdots,n}$构造一个 Z_q 上的 $n+m-1$ 次多项式 $f^{(0)}(x)=\sum_{j=0}^{n+m-1}a_jx^j$,则共享秘密 $S_k=f^{(0)}(k)(k=1,2,\cdots,m)$,秘密份额 $s_i^{(0)}=f^{(0)}(ID_i)(i=1,2,\cdots,n)$,公开系数承诺 $E_j^{(0)}=a_jP(j=0,1,\cdots,n+m-1)$。

d)D 随机选择 $d_1,d_2,\cdots,d_{n+m-t}\in[m+1,q-1]$,且 $d_j(j=1,2,\cdots,n+m-t)$不同于 $ID_i(i=1,2,\cdots,n)$,计算并公布$(d_j,f^{(0)}(d_j))$。

e)验证者可以通过式(1)来检验秘密份额 $s_i^{(0)}$ 是否有效。

$$e(M_{1i}^{(0)},P)=\prod_{j=0}^{n+m-1}e(Q,E_j^{(0)})^{ID_i^j} \tag{1}$$

2.3 秘密份额更新

假设在 $\tau=1,2,\cdots$时刻要对参与者的秘密份额进行更新,则分发者 D 按以下步骤执行:

a)从单向散列链 L 上提取散列值 $H^{N-\tau}(\alpha)$,构造多项式:

$$g^{(\tau)}(x)=H^{N-\tau}(\alpha)(x-1)(x-2)\cdots(x-m)=\sum_{j=0}^{m}b_j^{(\tau)}x^j$$

b)计算 $t_i^{(\tau)}=g^{(\tau)}(ID_i)(i=1,2,\cdots,n)$,公开系数承诺 $E_j^{(\tau)}=b_j^{(\tau)}P(j=0,1,\cdots,m)$。

c)随机选取 $b\in Z_q^*$,计算 $V=bP$,$M_i^{(\tau)}=H_1(e(bR_i,Q))+t_i^{(\tau)}$,$M_{2i}^{(\tau)}=t_i^{(\tau)}Q(i=1,2,\cdots,n)$,公布数据信息$(V,M_i^{(\tau)},M_{2i}^{(\tau)})$。

d)定义多项式 $f^{(\tau)}(x)=f^{(\tau-1)}(x)+g^{(\tau)}(x)$,计算并更新$(f^{(\tau)}(d_j))(j=1,2,\cdots,n+m-t)$。

e)任何人都可以通过式(2)验证更新份额 $t_i^{(\tau)}$ 是否正确。

$$e(M_{2i}^{(\tau)},P)=\prod_{j=0}^{m}e(Q,E_j^{(\tau)})^{ID_i^j} \tag{2}$$

f)参与者 P_i 利用私钥 x_i 解密 $M_i^{(\tau)}$ 得到更新份额 $t_i^{(\tau)}=M_i^{(\tau)}-H_1(e(x_iV,Q))$,则更新后的秘密份额 $s_i^{(\tau)}=s_i^{(\tau-1)}+t_i^{(\tau)}$。计算并公布 $W_i^{(\tau)}=s_i^{(\tau)}Q$,销毁 $s_i^{(\tau-1)}$。

2.4 秘密重构

假设有 t 个参与者 $P_1,P_2,\cdots,P_t$ 合作重构 m 个秘密 $S_1,S_2,\cdots,S_m$。

初始状态($\tau=0$ 时刻):

a)验证者通过式(1)来检验 P_i 提供的秘密份额 $s_i^{(0)}(i=1,2,\cdots,t)$是否正确。

b)若 t 个参与者提供了正确的秘密份额 $s_i^{(0)}$,则可以利用 $n+m$ 个点$(d_j,f^{(0)}(d_j))_{j=1,2,\cdots,n+m-t}$和$(ID_i,s_i^{(0)})_{i=1,2,\cdots,t}$根据 Lagrange 插值法重构多项式 $f^{(0)}(x)$。

c)计算秘密 $S_k=f^{(0)}(k)(k=1,2,\cdots,m)$。

$\tau=1,2,\cdots$时刻:

a)验证者通过式(3)来检验 P_i 的秘密份额 $s_i^{(\tau)}$ 是否正确。

$$e(W_i^{(\tau)},P)=e(M_{1i}^{(0)},P)\prod_{j=1}^{\tau}e(M_{2i}^{(j)},P) \tag{3}$$

若式(3)成立,则说明参与者提供的秘密份额是有效的。

b)设 t 个参与者提供了正确的秘密份额 $s_i^{(\tau)}(i=1,2,\cdots,t)$,则可以利用 $n+m$ 个点$(d_j,f^{(\tau)}(d_j))_{j=1,2,\cdots,n+m-t}$和$(ID_i,s_i^{(\tau)})_{i=1,2,\cdots,t}$根据 Lagrange 插值公式恢复出多项式 $f^{(\tau)}(x)$。

c)计算秘密 $S_k=f^{(0)}(k)(k=1,2,\cdots,m)$。

3 方案分析

3.1 正确性分析

1)验证式的正确性

验证式(1):

由于 $M_{1i}^{(0)}=s_i^{(0)}Q$,$s_i^{(0)}=f^{(0)}(ID_i)$,$E_j^{(0)}=a_jP$,则

$$e(M_{1i}^{(0)},P)=e(s_i^{(0)}Q,P)=e(Q,s_i^{(0)}P)=e(Q,f^{(0)}(ID_i)P)=e(Q,(a_0+a_1ID_i+\cdots+a_{n+m-1}ID_i^{n+m-1})P)=\prod_{j=0}^{n+m-1}e(Q,a_jID_i^jP)=\prod_{j=0}^{n+m-1}e(Q,a_jP)^{ID_i^j}=\prod_{j=0}^{n+m-1}e(Q,E_j^{(0)})^{ID_i^j}$$

因此,验证式(1)是正确的。

验证式(2):

由于 $M_{2i}^{(\tau)}=t_i^{(\tau)}Q, t_i^{(\tau)}=g^{(\tau)}(\mathrm{ID}_i), E_j^{(\tau)}=b_j^{(\tau)}P$,则

$$e(M_{2i}^{(\tau)},P)=e(t_i^{(\tau)}Q,P)=$$
$$e(Q,t_i^{(\tau)}P)=e(Q,g^{(\tau)}(\mathrm{ID}_i)P)=$$
$$e(Q,\sum_{j=0}^{m}b_j^{(\tau)}\mathrm{ID}_i^jP)=\prod_{j=0}^{m}e(Q,b_j^{(\tau)}\mathrm{ID}_i^jP)=$$
$$\prod_{j=0}^{m}e(Q,E_j^{(\tau)})^{\mathrm{ID}_i^j}$$

因此,验证式(2)是正确的。

验证式(3):

由于 $W_i^{(\tau)}=s_i^{(\tau)}Q$,又知

$$s_i^{(\tau)}=s_i^{(\tau-1)}+t_i^{(\tau)}=s_i^{(\tau-2)}+$$
$$t_i^{(\tau-1)}+t_i^{(\tau)}=\cdots=s_i^{(0)}+$$
$$t_i^{(1)}+t_i^{(2)}+\cdots+t_i^{(\tau)}$$

故

$$e(W_i^{(\tau)},P)=e(s_i^{(\tau)}Q,P)=$$
$$e((s_i^{(\tau-1)}+t_i^{(\tau)})Q,P)=$$
$$e(s_i^{(0)}Q,P)e(t_i^{(1)}Q,P)e(t_i^{(2)}Q,P)\cdots e(t_i^{(\tau)}Q,P)=$$
$$e(M_{1i}^{(0)},P)\prod_{j=1}^{\tau}e(M_{2i}^{(j)},P)$$

因此,验证式(3)是正确的。

2)秘密重构的正确性 任意 t 个或 t 个以上的参与者合作可以重构出 m 个秘密。

初始状态:

利用 t 个参与者提供的 t 个点$(\mathrm{ID}_i,s_i^{(0)})_{i=1,2,\cdots,t}$和 $n+m-t$ 个公开值$(d_j,f^{(0)}(d_j))_{j=1,2,\cdots,n+m-t}$,由 Lagrange 插值法可重构 $n+m-1$ 次多项式$f^{(0)}(x)$。计算 $S_k=f^{(0)}(k)(k=1,2,\cdots,m)$,即得到 m 个秘密。

$\tau=1,2,\cdots$时刻:

秘密份额 $s_i^{(\tau)}=s_i^{(\tau-1)}+t_i^{(\tau)}$,此时的秘密多项式为

$$f^{(\tau)}(x)=f^{(\tau-1)}(x)+g^{(\tau)}(x)=$$
$$f^{(\tau-2)}(x)+g^{(\tau-1)}(x)+g^{(\tau)}(x)=$$
$$\vdots$$
$$f^{(0)}(x)+g^{(1)}(x)+\cdots+g^{(\tau)}(x)$$

而

$$f^{(\tau)}(\mathrm{ID}_i)=f^{(0)}(\mathrm{ID}_i)+g^{(1)}(\mathrm{ID}_i)+\cdots+g^{(\tau)}(\mathrm{ID}_i)=$$
$$s_i^{(0)}+t_i^{(1)}+\cdots+t_i^{(\tau)}=s_i^{(1)}+t_i^{(2)}+\cdots+t_i^{(\tau)}=$$
$$\vdots$$
$$s_i^{(\tau-1)}+t_i^{(\tau)}=s_i^{(\tau)}$$

所以,$(\mathrm{ID}_i,s_i^{(\tau)})$ 为多项式 $f^{(\tau)}(x)$ 上的点。利用 $n+m$ 对数$(\mathrm{ID}_i,s_i^{(\tau)})_{i=1,2,\cdots,t}$和$(d_i,f^{(\tau)}(d_i))_{i=1,2,\cdots,n+m-t}$,可由 Lagrange 插值法重构 $n+m-1$ 次多项式$f^{(\tau)}(x)$。令 $x=k(k=1,2,\cdots,m)$,易知 $g^{(\tau)}(k)=0$,所以共享秘密 $S_k=f^{(\tau)}(k)=f^{(0)}(k)$。

3.2 安全性分析

1)秘密分发过程的安全性

基于离散对数问题和计算 Diffie-Hellman 问题的难解性,本方案对秘密份额 $s_i^{(0)}$ 和更新份额 $t_i^{(\tau)}$ 的加密算法是安全的。

用反证法。假设对 $s_i^{(0)}$ 的加密算法不安全,则存在算法 A:把 $H_1(e(x_iP_{\mathrm{pub}},Q))$ 和 R_i 作为输入,算法 A 以概率 ε 成功输出 $H_1(e(sR_i,Q))=H_1(e(x_iP_{\mathrm{pub}},Q))$,进而计算秘密份额 $s_i^{(0)}$,即算法 A 在给定输入 sP、x_iP 的情况下,能以概率 ε 成功输出 sx_iP,这与计算 Diffie-Hellman 问题的困难性相矛盾,假设不成立,所以秘密分发阶段 $s_i^{(0)}$ 的加密算法是安全的。在不知道系统私钥 s 的情况下,任何攻击者无法通过公开信息 a_i 计算出秘密份额 $s_i^{(0)}=a_i(H_1(e(sR_i,Q)))^{-1}$,同理可证更新份额 $t_i^{(\tau)}$ 的加密算法也是安全的。

2)秘密份额更新阶段的安全性

在 τ 时刻,更新多项式 $g^{(\tau)}(x)=H^{N-\tau}(\alpha)(x-1)(x-2)\cdots(x-m)=\sum_{j=0}^{m}b_j^{(\tau)}x^j$,根据单向散列链的性质,即使攻击者窃取到 $H^{N-\tau}(\alpha)$ 也无法计算出下一时刻 $H^{N-\tau-1}(\alpha)$ 的值,因此攻击者窃取的信息在该更新周期结束后不会对下一周期系统的安全造成威胁。

任何人都可以通过式(2)验证更新份额的有效性,从而防止秘密分发者的欺骗。基于离散对数问题和计算 Diffie-Hellman 问题的难解性,恶意攻击者无法通过公开信息 $M_{2i}^{(\tau)}=t_i^{(\tau)}Q$ 和 $M_i^{(\tau)}=H_1(e(bR_i,Q))\oplus t_i^{(\tau)}$ 计算出更新份额 $t_i^{(\tau)}$,故无法通过等式 $s_i^{(\tau)}=s_i^{(\tau-1)}+t_i^{(\tau)}$ 得到更新后的秘密份额 $s_i^{(\tau)}$。

3)秘密重构过程的安全性

(1)任何人都可以检验参与者有无欺诈行为

验证者根据公开信息 $M_{1i}^{(0)}=s_i^{(0)}Q, M_{2i}^{(\tau)}=t_i^{(\tau)}Q, W_i^{(\tau)}=s_i^{(\tau)}Q$,由式(3)来检验参与者提供的秘密份额是否正确,从而有效防止参与者之间的欺诈行为。基于离散对数困难问题,验证过程不会泄露秘密份额的相关信息。

(2)任何少于 t 个参与者的集合都无法恢复秘密

在秘密分发初始时刻和秘密份额更新时刻,初始多项式 $f^{(0)}(x)$ 和更新多项式 $f^{(\tau)}(x)$ 都是 $n+m-1$ 次的,若想由 Lagrange 插值公式重构多项式 $f^{(0)}(x)$ 或 $f^{(\tau)}(x)$,必须要知道多项式上的 $n+m$ 个点,而分发者给出的公开值 $f^{(0)}(d_i)$($f^{(\tau)}(d_i)$)只有 $n+m-t$ 个,所以需要至少 t 个参与者提供 t 个秘密份额才能由 Lagrange 插值法重构多项式 $f^{(0)}(x)$ 或 $f^{(\tau)}(x)$,进而恢复出秘密。若攻击者获得少于 t 个正确的秘密份额企图重构秘密,其难度相当于攻破 Shamir 秘密共享方案。

3.3 计算复杂度

该方案由系统初始化、秘密分发、秘密份额更新和秘密重构四部分组成。从计算复杂度方面分析,计算量主要集中在双线性对运算、Lagrange 插值、点乘运算等方面,如表 1 所示。

表 1 方案计算量

操作	秘密分发	份额更新	份额验证	秘密重构
e 运算	n	n	$2m+n+3$	$t(\tau+1)$
hash 运算	2	1	0	0
插值多项式	1	0	0	0
点乘运算	$m+n$	$m+n+2$	0	0
Lagrange 插值	0	0	0	1

目前可利用 Boneh 等人[12]提出的基于有限域内超奇异椭圆曲线的 Weil Pairing 算法来求解双线性映射,其计算复杂度为 $O(\log_2 q)$。与 e 运算和点乘运算相比,Lagrange 插值多项式的计算复杂度更高一些,构造经过 n 点的插值多项式需要 $O(n\lg^2 n)$次乘运算,由 Lagrange 插值法重构 n 次多项式的计算复杂度为 $O(n\log_2^2 n)$。由表 1 可知,该方案由于使用双线性对的性质实现秘密份额的公开验证而引入了较多的 e 运算和点乘运算,增加了方案的计算代价。插值多项式的计算复杂度与多项式的次数有关,该方案在秘密分发阶段构造了一个经过 $n+m$ 个点的插值多项式,故需要 $O((n+m)\lg^2(n+m))$次乘法运算,重构时的复杂度为 $O((n+m)\log_2^2(n+m))$。

(下转第 3799 页)

难题。

c)任何人(包括授权人 A 和 KGC)不能伪造一个不包括自己的环签名。因为由式(1)可知,σ 是代理密钥 SK_i' 的签名与代理人的私钥 $SK_i=(x_i,y_i)$ 签名之和,任何人(包括授权人 A 和 KGC)都无法通过 σ 解出代理密钥 SK_i' 和代理人的私钥 SK_i,除非他能解决离散对数难题。因此,攻击者所伪造的环签名不可能通过验证式(2)。所以,任何人(包括授权人 A 和 KGC)不能伪造一个不包括自己的环签名。

因此,本文提出的方案满足不可伪造性。

2.2.4　可区分性

定理 4　提出的方案满足可区分性。

证明　可区分性。因代理签名密钥 SK_i' 与代理签名人的私钥 SK_i 不同,代理环签名与代理人的一般环签名具有结构上的区别,所以提出的方案满足可区分性。

2.3　效率分析

由于系统建立、用户密钥生成的时间开销不大,而且可以通过预处理来完成,所以本方案的效率分析主要考虑签名和验证两个阶段。用 P_g 表示双线性对运算,M_u 表示在循环加法群 G 上的乘法运算,则本文方案与文献[6,7]的比较如表 1 所示。假设进行比较的方案的环成员数量都是 n。

表 1　本文方案与文献[6,7]的比较

方案	M_u	P_g
罗大文等人[6]	$4n$	2
张小萍等人[7]	$3n+2$	2
本文方案	$2n+1$	0

由表 1 可得,文献[6]需要进行 $4n$ 次乘法和 2 次双线性对运算,文献[7]需要进行 $3n+2$ 次乘法和 2 次双线性对运算,而本文方案无须对运算和指数运算,仅需要 $2n+1$ 次乘法运算,是目前已知方案中效率最高的。

3　结束语

本文基于无证书密码体制提出了一种高效的代理环签名方案。该方案无双线性对运算和指数运算,只需进行 $2n+1$ 次乘法运算,既极大地提高了效率,又能满足环签名的安全需求。如何设计标准模型下无双线性对运算和指数运算的无证书代理环签名方案,是值得进一步研究的课题。

参考文献:

[1] Al-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]//Advance in Cryptology. Berlin: Springer-Verlag, 2003: 452-473.

[2] SHAMIR A. Identity-Based cryptosystems and signature schemes [C]//Proc of Cryptology-Crypto'84. New York: Springer-Verlag, 1984:47-53.

[3] 张福泰,孙银霞,张磊,等. 无证书公钥密码体制研究[J]. 软件学报,2011,22(6):1316-1332.

[4] 余婷,赵泽茂,任锡洋. 标准模型下基于身份的高效环签名[J]. 计算机应用,2012,32(7):2015-2017,2026.

[5] ZHANG Fang-guo, SAFAVI-NAINI R, LIN C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from blinear pairings[EB/OL]. (2003-05-20)[2013-04-20]. http://eprint.iacr.org/2003/.

[6] 罗大文,何明星,李琥. 一种新的可证明安全的代理环签名方案[J]. 计算机工程与应用,2009,45(7):100-102.

[7] 张小萍,钟诚. 改进的代理环签名方案[J]. 计算机应用研究,2011,28(9):3505-3507.

[8] 张俊茸,任平安,李文莉. 一种新的无证书的代理环签名方案[J]. 计算机工程与应用,2012,48(2):63-65.

[9] 刘文浩,许春香. 无双线性配对的无证书签密方案[J]. 软件学报,2011,22(8):1918-1926.

[10] CHEN L, CHENG Z, SMART N P. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(4): 213-241.

(上接第 3796 页)

4　结束语

本文构造了一种双线性对上的可公开验证可更新多秘密共享方案,给出了秘密份额的动态更新过程,基于椭圆曲线上的离散对数问题的难解性和双线性对的性质,任何人都可以对秘密份额和更新份额的有效性进行验证。与传统的秘密共享方案相比,该方案有以下优点:a)秘密份额 $s_i^{(0)}$ 由参与者自己选取,避免了分发者对参与者的欺骗;b)秘密份额 $s_i^{(0)}$ 可以被重复使用,当变更共享秘密时,无须重新选择;c)参与者与分发者之间不需要维护安全信道,降低了系统代价;d)方案具有可公开验证性,能有效地防止内外部攻击;e)秘密份额可定期更新,并且一次秘密共享过程可以共享多个秘密。本方案虽然在运行效率上没有太大优势,但在一定程度上提高了系统的安全性和实用价值,为今后研究更高效的可公开验证可更新多秘密共享方案奠定了基础。

参考文献:

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C]//Proc of AFIPS 1979 National Computer Conference. 1979: 313-317.

[3] CHOR B, GOLDWASSER S, MICALI S, *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Proc of the 26th IEEE Symposium on the Foundations of Computer Science. [S.l.]: IEEE Press, 1985: 383-395.

[4] STADLER M. Publicly verifiable secret sharing[C]//Advances in Cryptology, Eurocryptp'96. Berlin: Springer-Verlag, 1996: 190-199.

[5] 张建中,张艳丽. 一个双线性对上公开可验证多秘密共享方案[J]. 计算机工程与应用,2011,47(25):82-84.

[6] 肖艳萍,杜伟章. 基于双线性对的可验证可更新的秘密分享方案[J]. 计算机应用研究,2011,28(9):3519-3521.

[7] WU T Y, TSENG Y M. A pairing-based publicly verifiable secret sharing scheme[J]. Journal of Systems Science and Complexity, 2011, 24(1): 186-194.

[8] 田有亮,马建峰,彭长根,等. 椭圆曲线上的信息论安全的可验证秘密共享方案[J]. 通信学报,2011,32(12):96-102.

[9] 秦华旺,朱晓华,戴跃伟. 访问结构上的动态先应式秘密共享方案[J]. 电子科技大学学报,2012,41(6):927-931.

[10] 李婧,李志慧,赖红. 基于 hash 函数的无分发者的多秘密共享方案[J]. 计算机工程与应用,2012,48(18):64-65,131.

[11] MIAO Fu-you, DU Xian-chang, RUAN Wen-jing, *et al*. A strong PVSS scheme[C]//Lecture Notes in Electrical Engineering, vol 131. New York: Springer-Verlag, 2013: 521-528.

[12] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology, CRYPTO 2001. Berlin: Springer-Verlag, 2001: 213-229.