

基于 ECC 的具有前向安全性的 VSS 方案

韦性佳,张京花,芦殿军

(青海师范大学 数学与统计学院,青海 西宁 810008)

摘要:秘密共享作为密码学的重要手段,已经广泛应用于安全的多方计算和分布式的密码学系统之中,但目前大多数秘密共享方案不具备前向安全性。基于有限域上的椭圆曲线离散对数困难问题,结合前向安全性理论与向量空间存取结构,提出了一种新的具有前向安全性的可验证的秘密共享方案。该方案可验证秘密与子秘密的准确性,实现可信中心与用户的双向验证;能够检测出系统中的欺诈行为,使得敌手无法伪造共享秘密;具有前向安全性,即使敌手掌握前一时间段的秘密也无法获取关于之前时间段秘密的任何信息,保障了共享秘密的安全性;具有门限性质,任何少于 t 个用户无法恢复共享秘密。最后对方案的安全性和效率进行了分析,证明了该方案的安全性。

关键词:椭圆曲线;前向安全性;可验证性;秘密共享;向量空间

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2018)04-0157-04

doi:10.3969/j.issn.1673-629X.2018.04.033

A Forward Security Secret Sharing Scheme Based on ECC

WEI Xing-jia, ZHANG Jing-hua, LU Dian-jun

(School of Mathematics and Statistics, Qinghai Normal University, Xining 810008, China)

Abstract: Secret sharing, as an important means of cryptography, has been widely used in secure multi-party computation and distributed cryptography. However, most secret sharing schemes do not have the character of forward security. In this paper, based on the discrete logarithm problem of elliptic curve over finite fields, combined with the forward security theory and the vector space access structure, we put forward a new verifiable secret sharing scheme with forward security. It verifies the accuracy of the secret and sub-secret and realizes the bidirectional authentication between trusted center and users. Moreover, it could detect the fraud of the system and makes it impossible for an adversary to forge a shared secret. With the forward security, even if the enemy has mastered the secret of the previous period of time, it cannot obtain any information, which guarantees the security of the shared secret. Having the property of threshold, any less than t users cannot recover the shared secret. Finally, the security and efficiency of the scheme are analyzed, and its security is proved.

Key words: elliptic curve; forward security; verifiable; secret sharing; vector space

0 引言

秘密共享作为一种基础的密码学手段,在信息安全方面扮演着非常重要的角色。自从 1979 年 Shamir^[1]提出基于拉格朗日插值多项式门限秘密共享方案之后,有关秘密共享方面的研究受到了广大研究者的高度关注。

1985 年 Chor 等^[2]提出了可验证的秘密共享方案(VSS)的理念。1992 年 Pedersen^[3]在前人的基础上提出了一种更为简洁、实用的 VSS 方案。起初的 VSS 方案存在计算量大、效率相对较低等缺陷,直到 Neal Koblitz 等^[4]发现有限域上椭圆曲线离散对数问题是

难解的以后,椭圆曲线(elliptic curve, ECC)以它计算量小、效率高等优势迅速成为密码学研究的一个重要工具。

1989 年,Brickell^[5]提出了一种基于向量空间存取结构的秘密共享方案。在这方面,张福泰等^[6-8]基于双线性变换提出的秘密共享方案对文中的研究具有重要的启发作用。

1997 年,Anderson^[9]提出了前向安全性(forward security)理论,该理论可以有效地减少因为秘密泄露对系统安全所带来的隐患。在此基础上,1999 年 Bellare^[10]提出了一种前向安全的数字签名方案。近年

收稿日期:2017-04-25

修回日期:2017-08-30

网络出版时间:2017-12-05

基金项目:教育部春晖计划资助项目(教外司留[2014]1310号);青海省科技创新能力促进计划资助项目(2015-ZJ-724)

作者简介:韦性佳(1991-),男,硕士研究生,研究方向为代数组合与数字签名、秘密共享;芦殿军,硕士,教授,硕导,研究方向为信息安全与代数组合。

网络出版地址: <http://cnki.net/kcms/detail/61.1450.TP.20171205.0906.058.html>

来,王彩芬等^[11]提出了具有前向安全性的秘密共享方案,基于有限域上离散对数难解问题和强 RSA 假设^[12-13],有效地实现了秘密的前向安全性,并且该方案具有很强的实践价值。

在已有秘密共享方案^[14-16]研究成果的基础上,文中提出了一种基于 ECC 的具有前向安全性质的 VSS 方案。该方案利用椭圆曲线计算量小、效率高的优点,同时充分发挥前向安全理论在秘密保护方面的优势,为秘密共享方案提供了双重的安全保障。同时该方案是基于向量空间的存取结构,在秘密的重构中更加安全、有效。

1 基础知识

1.1 椭圆曲线离散对数问题(ECDLP)

给定有限域 $GF(q)$ 上的椭圆曲线 E ,生成元 $P \in E(GF(q))$,阶 q , $\forall Q \in \langle P \rangle$,寻找 $a \in [0, q-1]$,使得 $Q = aP$,称为椭圆曲线离散对数问题。

1.2 前向安全性理论

前向安全性理论(forward security theory)具体分析如下:

(1) $H_i(i=1,2,\dots,n)$ 将 S 的有效期分为 $T(1,2,\dots,T)$ 个时间段;

(2)在整个有效期内,公钥 PK_U 不变,但第 j 个时间段私钥 SK_U 随着时间段 j 的改变而改变;

(3)在第 j 个时段, H_i 计算 $S_j = f(S_{j-1})$,其中 f 是一个单向函数;

(4)算出 S_j 后,立即删除 S_{j-1} ,这样即使攻击者 A 获得了第 j 个时间段的 S_j 后也不能获得关于 S_0, S_1, \dots, S_{j-1} 的任何信息。

1.3 系统中的记号与参数

H :参与者集合;

H_i :第 i 个参与者($H_i \in H, i=1,2,\dots,n$);

D :可信中心,且 $D \notin H$;

S_0 :初始秘密;

S_j :第 j 个时间段的秘密;

T :时间周期;

G_1 :椭圆曲线加法群; P, Q, R 为 G_1 生成元,其中 $Q = aP, R = bP(a, b \in Z_q^*)$;

SP_i :验证子秘密; $g, h \in Z_q^*$ 且 $c = \log_g^h$;

h_1 :表示 Hash 函数,且 $h_1: G_1 \rightarrow Z_q^*$ 。

1.4 向量空间存取结构

设 Γ 是 H 上的单调存取结构,如果存在一个映射 $\psi: H \cup \{D\} \rightarrow Z_q^*$,使得 H 的一个子集 $A \in \Gamma$,当且仅当向量 $\psi(D)$ 可由 $\{\psi(H) \mid H \in A\}$ 中的向量线性表示时,称 Γ 为一个向量空间存取结构(vector access structure)。

2 提出的方案

2.1 系统初始化

(1) D 公布映射 $\psi: H \cup \{D\} \rightarrow Z_q^*$,且有: $\psi(D) = (a_1, a_2, \dots, a_t)(a_i \in Z_q^*), \psi(H_i) = (a_{i1}, a_{i2}, \dots, a_{it})(a_{ij} \in Z_q^*)$ 。

然后, D 广播 $\psi(D)$,并将 $\psi(H_i)$ 发送给 $H_i(i=1,2,\dots,n)$ 。

(2) D 随机选择向量 $x = \{x_1, x_2, \dots, x_t\}, x_i \in Z_q^*$,然后计算秘密向量 $A = (P + x_1Q, P + x_2Q, \dots, P + x_tQ) = (A_1, A_2, \dots, A_t)$, $B = (P + x_1R, P + x_2R, \dots, P + x_tR) = (B_1, B_2, \dots, B_t)$ 。初始秘密 $S_0 = (A + B) \cdot \psi(D) = (K_0 + R_0)$;其中 $K_0 = A \cdot \psi(D) = (P + x_1Q)a_1 + \dots + (P + x_tQ)a_t, R_0 = B \cdot \psi(D) = (P + x_1R)a_1 + \dots + (P + x_tR)a_t$ 。

初始子秘密 $S_{i0} = (A + B) \cdot \psi(H_i) = K_{i0} + R_{i0}(i=1,2,\dots,n)$,其中 $K_{i0} = \psi(H_i) \cdot A = a_{i1}(P + x_1Q) + \dots + a_{it}(P + x_tQ) = a_{i1}A_1 + \dots + a_{it}A_t, R_{i0} = \psi(H_i) \cdot B = a_{i1}(P + x_1R) + \dots + a_{it}(P + x_tR) = a_{i1}B_1 + \dots + a_{it}B_t$ 。

$E_0 = gK_0 + hR_0, E_j = gA_j + hB_j$ 后, D 广播 $g, h, E_0, E_j(j=1,2,\dots,t)$,且通过秘密信道将 $(R_{i0}, K_{i0}), S_{i0}$ 发送 $H_i(i=1,2,\dots,n)$ 。

(3)第 j 个时间段的共享秘密 $S_j = 2^j(A + B) \cdot \psi(D)(j=0,1,\dots,T)$

2.2 子秘密更新

令 $S_{ij} = 2S_{i(j-1)}$ (i 表示第 i 个参与者, j 表示第 j 个时间段)。

注:(1)每个成员 H_i 通过非交互式的方式来更新自己在第 j 个时间段的子秘密;

(2)当更新 S_{ij} 后,立即删除 $S_{i(j-1)}$ 。

2.3 秘密的验证

2.3.1 初始阶段秘密的验证

(1)验证可信中心 D 的正确性(初始阶段)。

对于任意一个参与者 H_i ,通过式(1)来验证可信中心 D 的正确性:

$$E_0 \stackrel{?}{=} \sum_{i=1}^t E_i a_i \quad (1)$$

(2)参与者 H_i 通过式(2)验证可信中心 D 发送给自己的信息的正确性:

$$gK_{i0} + hR_{i0} \stackrel{?}{=} \sum_{k=1}^t a_{ik} E_k \quad (2)$$

若式(1)不成立,即 $E_0 \neq \sum_{i=1}^t E_i a_i$,则说明 D 有欺诈行为,该协议就终止;若式(1)成立,但是式(2)不成立,即 $gK_{i0} + hR_{i0} \neq \sum_{k=1}^t a_{ik} E_k$,则用户 H_i 就公开广播对可信中心 D 的质疑,与此同时广播由 D 发送给自己的

秘密份额 (K_0, R_0) , 并且要求 D 分发本应属于自己的有效份额, 如果 D 受到超过 $n - t$ 个参与成员的质疑, 则协议自行终止; 在授权子集恢复秘密时, 秘密重构者可以通过式(2)检验每个成员提交份额的有效性。

2.3.2 验证更新秘密

D 计算 $S = h_1(2^{T+1}S_0)$, $SP_i = h_1(2^{T+1}S_0)$ ($i = 1, 2, \dots, n$), 并广播 S, SP_i 。

(1) 用户 H_i 验证自己在第 j 个时间段的子秘密进化是否有效。

每个成员 H_i 检验:

$$h_1(2^{T+1-j}S_{ij}) = SP_i \quad (3)$$

若式(3)成立, 则 H_i 证明自己在第 j 个时间段的子秘密进化是有效的。

(2) 合格子集验证第 j 个时间段所恢复的秘密 S_j 是否正确。

$$h_1(2^{T+1-j}S_j) = S \quad (4)$$

若式(4)成立, 则合格子集可以确定在第 j 个时间段恢复的共享秘密 S_j 是正确的。

2.4 秘密的恢复

任意一个授权子集(成员个数必须 $\geq t$) 联合起来, 利用每个成员的秘密份额可以恢复秘密, 其过程为:

(1) 为不失一般性, 取重构成员 $H = \{H_1, H_2, \dots, H_t\}$, 这 t 个成员利用 $\psi(H_i)$, 根据向量空间存取结构, 有如下等式:

$$\psi(D) = \psi(H) \cdot C^T \quad (5)$$

其中, $C = (c_1, c_2, \dots, c_t)$; $\psi(H) = \{\psi(H_1), \psi(H_2), \dots, \psi(H_t)\}$ 。

然后利用式(5)解出向量 C 。

(2) 重构成员 H_i ($i = 1, 2, \dots, t$) 用自己在第 j 个时间段的子秘密 S_{ij} 和式(5)中的向量 C , 可重构出秘密:

$$S_j = \sum_{i=1}^t c_i S_{ij}。$$

3 安全性及正确性分析

3.1 方案的正确性

定理1: 在初始阶段, 式(1)可验证可信中心 D 的正确性, 式(2)可验证 D 发给参与者 H_i 的信息的正确性。

证明: 根据已知条件 $E_j = gA_j + hB_j$, 代入等式右侧, 则有:

$$\begin{aligned} \sum_{i=1}^t a_i E_i &= a_1 E_1 + a_2 E_2 + \dots + a_t E_t = \\ &g(a_1 A_1 + \dots + a_t A_t) + \\ &h(a_1 B_1 + \dots + a_t B_t) = \\ &gK_0 + hR_0 = E_0 \end{aligned}$$

由此可推知, 数据 E_j ($j = 1, 2, \dots, t$) 是正确的。

同理可证式(2)成立, 如下:

$$\begin{aligned} \sum_{k=1}^t a_{ik} E_k &= a_{i1} E_1 + \dots + a_{it} E_t = \\ &(gA_1 + hB_1)a_{i1} + (gA_2 + hB_2)a_{i2} + \dots + \\ &(gA_t + hB_t)a_{it} = g(a_{i1}A_1 + \dots + a_{it}A_t) + \\ &h(a_{i1}B_1 + \dots + a_{it}B_t) = \\ &gK_{i0} + hR_{i0} \end{aligned}$$

因此 D 发给参与者 H_i 的信息是正确的。

定理2: 方案中子秘密更新阶段的验证过程是正确的, 即: 式(3)、式(4)是正确的。

证明: $S_{ij} = 2^j S_{i0}$

$$h_1(2^{T+1-j}S_{ij}) = h_1(2^{T+1-j} \cdot 2^j S_{i0}) = h_1(2^T S_{i0}) = SP_i$$

即式(3)成立, 则说明子秘密的更新是正确的。

同理

$$S_j = 2^j(A + B) \cdot \psi(D) = 2^j S_0$$

$$h_1(2^{T+1-j}S_j) = h_1(2^{T+1-j} \cdot 2^j S_0) = S$$

即等式(4)成立, 说明合格子集恢复的共享秘密是正确的。

3.2 方案的安全性

定理3: 系统中的公开信息不会揭示关于共享秘密 S_j 与子秘密 S_{ij} 的任何信息。

证明: 根据已知条件有 $E_0 = gK_0 + hR_0$ 和 $E_j = gA_j + hB_j$ ($j = 1, 2, \dots, t$), 假设 $R_0 = rK_0$, $r \in Z_q^*$, 若敌手想要破解出 K_0 (或 R_0), 则需要计算 $E_0 = gK_0 + hR_0 = gK_0 + hrK_0 = (g + hr)K_0$, 即敌手必须获得 r , 但求解 r 是椭圆曲线离散对数难解问题, 所以攻击者无法获得关于初始秘密 S_0 的任何信息, 同理, 也无法揭示关于子秘密 S_{ij} 以及秘密向量 A, B 的任何信息。

定理4: 只有有效的合格子集(成员个数必须 $\geq t$) 方能构造出秘密 S_j 。

证明: 根据向量空间存取结构的定义, 不失一般性地取重构成员为 H_1, H_2, \dots, H_t , 于是有: $\psi(D) = c_1 \psi(H_1) + \dots + c_t \psi(H_t)$ 。

如果秘密重构成员的个数小于 t , 根据线性方程组的性质, 方程组(6)的解不唯一, 即存在无穷多个解, 则要解出系数 c_1, c_2, \dots, c_t 是不可行的, 所以至少需要 t 个合格成员联合起来, 方能解下列方程组:

$$\begin{cases} c_1 a_{11} + c_2 a_{21} + \dots + c_t a_{t1} = a_1 \\ \vdots \\ c_1 a_{1t} + c_2 a_{2t} + \dots + c_t a_{tt} = a_t \end{cases} \quad (6)$$

计算出系数 c_1, c_2, \dots, c_t 后, 利用式(7)计算并恢复出在第 j 个时间段的秘密。

$$\begin{aligned} S_j &= 2^j(A + B)\psi(D) = \\ &2^j(A + B)(c_1 \psi(H_1) + \dots + c_t \psi(H_t)) = \\ &c_1 2^j S_{1j} + c_2 2^j S_{2j} + \dots + c_t 2^j S_{tj} = \\ &c_1 S_{1j} + c_2 S_{2j} + \dots + c_t S_{tj} \end{aligned} \quad (7)$$

定理 5:方案具有前向安全性。

证明:该方案所具有的前向安全性具体体现在参与者所持子秘密的前向安全性及秘密信息的前向安全性。

在子秘密的更新阶段,假设敌手通过某种方式获得参与者 H_i 在第 j 个时间段的子秘密 S_{ij} ,若要计算 $S_{ik}(k=1,2,\cdots,j-1)$,由于子秘密是参与成员通过非交互的方式更新产生的,并且参与者在更新子秘密后,立即删除了前一时间段的秘密。所以即使敌手掌握了第 j 个时间段的子秘密 S_{ij} ,要想破解前 j 个时间段内的子秘密就必须面对椭圆曲线离散对数的难解问题,这样就保障了子秘密的前向安全性。

同理即便攻击者得到了第 j 个时间段的秘密 $S_j=2^j(A+B)\cdot\psi(D)$,若要通过 S_j 计算 $S_k(k=1,2,\cdots,j-1)$,他将面临同样的问题。

4 方案的计算成本

设 ρ 代表 G_1 中的标量乘法运算,结果如表 1 所示。该方案的运行时间复杂度为 $O(n)$,即在多项式时间范围内。说明方案的计算成本较低。

表 1 方案的计算量分析

	秘密分配	秘密验证	秘密重构
初始阶段	$[(4t-2)n-2]\rho$	$[(n+1)t]\rho$	$t\rho$
子秘密更新阶段	$[n(T+1)]\rho$	$n\rho$	

5 结束语

在文献[6,11]的基础上,基于向量空间存取结构提出了一种具有前向安全性的秘密共享方案,无论是在系统的安全性方面,还是在计算效率方面都有一定的提升。如果秘密在被动泄露的情况下,该方案可以避免秘密持有者的抵赖行为,检查出欺诈行为,同时该方案利用前向安全性理论保障了系统的前向安全性。

参考文献:

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

[2] CHOR B,DOLDWASSER S,MICALI S,et al. Verifiable se-

and data management. New York, NY, USA: ACM,2005:67-74.

[12] WILLIAMS C,MOBASHER B,BURKE R. Defending recommender systems:detection of profile injection attacks[J]. Service Oriented Computing and Applications,2007,1(3):157-170.

[13] ZHANG F,ZHOU Q. A meta-learning-based approach for

cret sharing and achieving simultaneity in the presence of faults[C]//Proceedings of the 26th IEEE symposium on foundations of computer sciences. Washington, DC, USA: IEEE Computer Society,1985:383-395.

[3] PEDERSON T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Proceedings of the 11th annual international cryptology conference on advances in cryptology. London, UK:Springer-Verlag,1992:129-140.

[4] NEAL K. Elliptic curve cryptosystems[J]. Mathematics of Computation,1987,48(177):203-209.

[5] BRICKELL E F. Some ideal secret sharing schemes[J]. Journal of Combinatorial Mathematics & Combinatorial Computing,1989,434:468-475.

[6] ZHANG F,ZHANG J. Efficient and information-theoretical secure verifiable secret sharing over bilinear groups[J]. Chinese Journal of Electronics,2014,23(1):13-17.

[7] 张福泰. 基于向量空间接入结构的分布式密钥生成[J]. 电子学报,2005,33(5):816-819.

[8] 张福泰,王育民. 适用于任意接入结构的可验证多秘密分享方案[J]. 通信学报,2007,28(11):59-64.

[9] ANDERSON R. Two remarks on public-key cryptography [C]//Fourth ACM conference on computer and communications security. [s. l.]:[s. n.],1997.

[10] BELLARE M,MINER S. A forward-secure digital signature scheme[C]//Proceedings of CRYPTO'99. Berlin:Springer-Verlag,1999:431-448.

[11] 王彩芬,刘军龙,贾爱库,等. 具有前向安全性质的秘密共享方案[J]. 电子与信息学报,2006,28(9):1714-1716.

[12] 汪保友,胡运发. 基于强 RSA 假设的签名方案[J]. 软件学报,2002,13(8):1729-1734.

[13] 徐文华,贺前华,李 韬. 基于强 RSA 假设的数字签名方案[J]. 华中科技大学学报:自然科学版,2008,36(12):24-26.

[14] 芦殿军,张秉儒,赵海兴. 基于多项式秘密共享的前向安全门限签名方案[J]. 通信学报,2009,30(1):45-49.

[15] 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.

[16] 李慧贤,蔡皖东,裴庆祺. 可验证秘密共享方案的设计与分析[J]. 西安电子科技大学学报:自然科学版,2008,35(1):148-151.

(上接第 156 页)

detecting profile injection attacks in collaborative recommender systems[J]. Journal of Computers,2012,7(1):226-234.

[14] MILLER B N,ALBERT I,LAM S K,et al. MovieLens unplugged:experiences with an occasionally connected recommender system[C]//Proceedings of the international conference on intelligent user interfaces. New York, NY, USA: ACM,2003:263-266.