基于椭圆曲线的密钥共享方案

张 永,张 欢
ZHANG Yong, ZHANG Huan

兰州理工大学 计算机与通信学院,兰州 730050
School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

ZHANG Yong, ZHANG Huan. Secret sharing scheme based on elliptic curve. Computer Engineering and Applications, 2014, 50(8):90-92.

Abstract: In order to resolve the key distributor and participants cheating problem in the secret sharing scheme, a multi-key sharing scheme which based on the elliptic curve cryptosystem and the cheaters can be detected is presented. The key distribution cheat and participants cheat can effectively be prevented, and the master key can be renewed without renewing the sub-keys of the participants. The scheme can increase a new participant and reduce a participant freely. The security of the new scheme is based on Shamir's threshold scheme and the elliptic curve discrete logarithm problem.
Key words: master key; sub-key; secret sharing scheme; elliptic curve discrete logarithm problem

摘 要: 针对门限密钥共享体制中存在的密钥分发者欺诈和参与者欺诈问题,采用椭圆曲线密码体制(ECC),提出一种可防欺诈的多密钥共享方案。该方案可以阻止密钥分发者、参与者的欺诈问题,且能实现更新主密钥时无需更改参与者的子密钥。方案可以灵活地增加或减少参与者,其安全性基于Shamir门限机制和椭圆曲线离散对数难题。
关键词: 主密钥;子密钥;密钥共享;椭圆曲线离散对数难题
文献标志码: A **中图分类号:** TP309 doi:10.3778/j.issn.1002-8331.1206-0353

1 引言

1979年,Shamir和Blakey分别提出了基于多项式插值算法的门限 (t,n) 密钥共享体制[1]和基于几何算法的门限密钥共享体制[2]。由于门限密钥共享体制简单、有效、易于实现等优点,因此得到了广泛的应用。(t,n) 门限密钥共享体制是指:n 个参与者共享主密钥 S,需要一个密钥管理中心 P_0,以及满足重构要求和安全性要求的两个算法。密钥管理中心 P_0 利用分配算法和主密钥 S 生成 n 个子密钥 $a_1, a_2, \cdots, a_n$,并将子密钥 $a_1, a_2, \cdots, a_n$ 秘密地分发给参与者。重构算法必须满足集合 $a_i(1\leqslant i\leqslant n)$ 中的任何 t 个或多于 t 个参与者的子密钥放在一起时,可以重构出主密钥 S。安全性要求是指少于 t 个参与者的子密钥放在一起时,不能重构出主密钥 S。通常密钥共享是假定密钥分发者和密钥参与者都是诚实的[3],但在现实中这是不切实际的。因此该体制不能有效地阻止密钥分发者欺诈(密钥分发者给参与者分发假的子密钥)和参与者欺诈(密钥恢复时参与者提供假的子密钥)。McEliece和Sarwate[4]在1981年提出了门限密钥共享体制的防欺骗问题。Chor和Goldwasser等[5]在1985年提出了可验证的密钥共享体制(verifiable secret sharing scheme)的概念。2004年,C C Yang,T Y Chang和M S Hwang(YCH)[6]通过多个密钥嵌入到多项式中的方法,构造了一种新的多重密钥共享方案。基于YCH多重密钥共享方案,SHAO等人[7]提出了一种有效的可验证多密钥共享方案,该方案的安全性基于离散对数问题的难解性。许春香、魏仕民和肖国镇[8]基于离散对数问题的难解性提出了一个定期更新防欺诈的密钥共享方案。它能对密钥份额进行更新,从而有效地防止攻击者获取密钥,并可以防止参与者之间的相互欺诈。但是该方案也存在着一定的不足。因为该方案一次密钥共享过程只能共享一个密钥,当该密钥泄漏时 n 个参与者的子密钥也就作废,用 n 个子密钥来共享一个主密钥,

作者简介: 张永(1963—),男,教授,硕士生导师,研究领域为信息安全、密码学、图像识别与处理等;张欢(1986—),男,硕士研究生,研究方向为信息安全、密码学。E-mail:82430893@qq.com
收稿日期: 2012-06-25 **修回日期:** 2012-10-16 **文章编号:** 1002-8331(2014)08-0090-03
CNKI **网络优先出版:** 2012-11-12, http://www.cnki.net/kcms/detail/11.2127.TP.20121112.1436.005.html

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

在资源上也是一种浪费。在实际应用过程中,当需要共享一个大密钥时,直接利用文献[8]中的方案会导致计算空间过大从而引起计算复杂度变大。

新方案基于文献[1]中 Shamir 的 (t,n) 门限密钥共享体制的思想,利用椭圆曲线密码体制(ECC)及线性方程组方法和多项式插值方法给出了阻止欺诈的方案。该方案可以在不改变参与者子密钥的情况下,共享多个不同的主密钥。灵活地增加、删减子密钥,灵活地变更主密钥。新方案可以识别子密钥的真假,有效地防止密钥中心、参与者及参与者相互之间的欺诈行为。

2　基于椭圆曲线的密钥共享方案

2.1　椭圆曲线数学基础

密钥管理中心在有限域 $GF(q)$(q 为素数或为 2^m 的整数)上选取一条安全的椭圆曲线方程 $E_q(a,b)$ 即

$$y^2=x^3+ax+b,q>3 \tag{1}$$

其中 $a,b\in GF(q)$, 且 $4a^3-27b^2\neq 0$。G 为 $E_q(a,b)$ 上选定的一基点,G 点的阶为大素数 n(n 至少是 160 bit 的素数)。

椭圆曲线的离散对数难题(ECDLP):方程 $Q=kP$,其中 $P,Q\in E_p(a,b)$ 且 $k<p$。对给定的 k 和 p 计算 Q 比较容易,但给定 Q 和 p 计算 k 则比较困难。

2.2　方案描述

2.2.1　系统初始化

密钥管理中心 P_0, 参与者 $P=\{P_1,P_2,\cdots,P_n\}$, $H(x)$ 为单向 hash 函数,主密钥为 S。密钥管理中心 P_0 在椭圆曲线 $E_q(a,b)$ 上选取 n 个参数,记为 $k_1,k_2,\cdots,k_n$ 作为参与者的子密钥,通过安全信道秘密地分配给 P_i。P_0 计算 $G_i'=k_iG(1\leqslant i\leqslant n)$, 并公开公开参数 $(E,G,n,H(x),G')$。

2.2.2　密钥分发

步骤 1　密钥管理中心 P_0 在椭圆曲线 $E_q(a,b)$ 中随机选一点 Q,与一个 $t-1$ 次多项式 $f(x)$:

$$f(x)=a_0+\sum_{i=1}^{t-1}a_ix^i(\bmod n) \tag{2}$$

其中 $f(0)=a_0=S$, Q 公开, $f(x)$ 保密。

步骤 2　密钥管理中心 P_0 计算 $f(i)=y_i$ 和 $A_l=a_lG(\bmod n),1\leqslant l\leqslant t-1$, 并计算 $D_i=(i,f(i))-k_iQ$, P_0 公开 A_l,D_i。

步骤 3　P_0 计算并公开 $F_i=H(k_iQ)$ 供参与者之间互相检验子密钥真伪。

2.2.3　子密钥验证

当参与者 $P=\{P_1,P_2,\cdots,P_n\}$ 收到子密钥后,首先验证子密钥及参与者之间身份的真实性,找到公开参数 Q,A_l,D_i, 计算 $C_i=k_iQ(\bmod n)$, 和 $(i,y_i)=(D_i+C_i)(\bmod n)$ 并验证 $y_iG=\sum_{k=0}^{t-1}A_li_i^l(\bmod n)$,公式如果成立,则参与者得到的子密钥是真实的。验证 $F_i=H(C_i)$,等式成立则代表参与者之间身份的真实性。

2.2.4　主密钥的重构

参与者根据公开参数计算子密钥集合:$(i,y_i)=(D_i+C_i)$,而此时的 (i,y_i) 是真实的。当 $l(l>t)$ 个参与者想要重构主密钥时,参与者根据线性方程组方法和多项式插值方法分别重构出主密钥 S。

(1)线性方程组方法密钥重构方案

$$\begin{cases}y_1=s+a_1+\cdots+a_{t-1}\\ y_2=s+2a_1+\cdots+2^{t-1}a_{t-1}\\ \quad\vdots\\ y_l=s+la_1+\cdots+l^{t-1}a_{t-1}\end{cases} \tag{3}$$

即

$$\begin{bmatrix}1&1&\cdots&1\\1&2&\cdots&2^{t-1}\\\vdots&\vdots&&\vdots\\1&l&\cdots&l^{t-1}\end{bmatrix}\begin{bmatrix}s\\a_1\\\vdots\\a_{t-1}\end{bmatrix}=\begin{bmatrix}y_1\\y_2\\\vdots\\y_l\end{bmatrix} \tag{4}$$

方程(4)可以看作 t 个变元线性方程组,由于 $1,2,\cdots,n$ 在 $E_q(a,b)$ 中两两不相同和范德蒙矩阵的性质,可知系数矩阵的秩是 t。因此当 $(l\geqslant t)$ 时 $s,a_1,a_2,\cdots,a_{t-1}$ 有唯一的解,于是能得到唯一的主密钥 S。即系数矩阵 $\boldsymbol{A}=\begin{vmatrix}1&1&\cdots&1\\1&2&\cdots&2^{t-1}\\\vdots&\vdots&&\vdots\\1&l&\cdots&l^{t-1}\end{vmatrix}$,则 $|\boldsymbol{A}|$ 是一个范德蒙行列式,故 $|\boldsymbol{A}|=\prod_{1\leqslant j\leqslant m\leqslant t}(x_m-x_j)$, 令 $d_j=\begin{vmatrix}1&1&\cdots&1\\1&2&\cdots&2^{t-1}\\\vdots&\vdots&&\vdots\\1&l&\cdots&l^{t-1}\end{vmatrix}$, $j=1,2,\cdots,t$ 其中 d_j 是由 $\begin{vmatrix}y_1\\y_2\\\vdots\\y_l\end{vmatrix}$ 替换 $|\boldsymbol{A}|$ 的第 j 列得到的,根据克莱姆法则线性方程组(4)的解为:

$$s=\frac{d_1}{|\boldsymbol{A}|},a_1=\frac{d_2}{|\boldsymbol{A}|},\cdots,a_{t-1}=\frac{d_{t-1}}{|\boldsymbol{A}|}$$

各参与者得到主密钥 S。

(2)多项式插值方法密钥重构方案

选择有限域中 n 个互不相同的 $x_1,x_2,\cdots,x_n$, P_0 秘密地将 $(x_i,y_i=f(x_i))$ 分配给 $P_i,1\leqslant i\leqslant n$。对于任意 l 个参与者 $P_{i_1},P_{i_2},\cdots,P_{i_l}$ 与式(4)对应的方程组为:

$$\begin{bmatrix}1&x_{i_1}&x_{i_1}^2&\cdots&x_{i_1}^{t-1}\\1&x_{i_2}&x_{i_2}^2&\cdots&x_{i_2}^{t-1}\\\vdots&\vdots&\vdots&&\vdots\\1&x_{i_l}&x_{i_l}^2&\cdots&x_{i_l}^{t-1}\end{bmatrix}\begin{bmatrix}s\\a_1\\\vdots\\a_{t-1}\end{bmatrix}=\begin{bmatrix}y_{i_1}\\y_{i_2}\\\vdots\\y_{i_l}\end{bmatrix} \tag{5}$$

其中 $y_{i_j}=f(x_{i_j}),1\leqslant j\leqslant l$。

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

对于任意 t 个子密钥,记为 (x_i, y_i),其中 $y_i = f(x_i)$, $i = 1, 2, \cdots, t$,参与者 $P_1, P_2, \cdots, P_l$ 共同计算:

$$h(x) = y_1\frac{(x-x_2)(x-x_3)\cdots(x-x_t)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_t)} + y_2\frac{(x-x_1)(x-x_3)\cdots(x-x_t)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_t)} + \cdots + y_t\frac{(x-x_1)(x-x_3)\cdots(x-x_{t-1})}{(x_t-x_1)(x_t-x_2)\cdots(x_t-x_{t-1})}$$

$h(x)$ 是个 $t-1$ 次多项式,根据域上多项式的性质,如果在 t 个不同点的取值相同,可得出这两个多项式恒等,推出 $h(x) = f(x)$,故有 $h(0) = f(0) = S$,得到主密钥。由上可知 t 个或以上参与者共同重构主密钥,只需知道 t 个参与者的子密钥。

2.2.5 主密钥与子密钥的更新

当主密钥需要更新时,密钥管理中心 P_0 只需重新在椭圆曲线有限域上选择一点 $Q'(Q' \neq Q)$ 及一个新的多项式 $f'(x) = S' + \sum_{i=1}^{t-1} a_i x^i (f'(x) \neq f(x))$,满足 $f'(0) = S'$,其中 S' 为新的主密钥。利用 Q' 和 $f'(x)$ 更新公开参数 Q' 及 A_l, D_i,而无需更改参与者的子密钥。

当参与者需要增加一个时,密钥管理中心 P_0 只需为新增参与者随机生成一个子密钥 k_{i+1},并公开参数 $G'_{i+1} = k_{i+1}G$ 及 $D_{i+1} = ((i+1, y_{i+1}) - k_{i+1}Q) \pmod n$ 即可。当需要减少一个参与者时,密钥管理中心 P_0 需要重新选择多项式 $f'(x)(f'(x) \neq f(x))$,满足 $f'(0) = S'$,其中 S' 为新的主密钥。利用新的多项式公开参数 A_l, D_i 即可。

3 安全性分析

方案中使用的多项式(2)是一个 $t-1$ 次多项式,参与者要重构主密钥,必须 t 个或者 t 个以上参与者提供子密钥。当 $l(l < t)$ 个参与者要恢复主密钥 S 时,方程组含有 t 个变元的 $l(l < t)$ 个线性方程组,假设 $l = t-1$,$t-1$ 个参与者含有 $t-1$ 个子密钥。由于将 $s_0 = f(0)$ 和关于子密钥的 $t-1$ 个方程放在一起,可得到唯一的解,因此主密钥的任何假设值 s_0 都存在唯一的多项式 $f_{s_0}(x)$ 使得 $y_j = f_{s_0}(j), 1 \leqslant j \leqslant l$ 和 $s_0 = f_{s_0}(0)$,故没有一个主密钥值可能被排除,所以 $l < t$ 个参与者得不到主密钥的任何信息。因此新方案相对于传统方案没有降低门限值。

方案的安全性基于ECDLP的难解性。在主密钥重构时,首先对子密钥进行验证,而每个参与者提供的是屏蔽子密钥 $C_i = k_i Q \pmod n (i = 1, 2, \cdots, t)$,由于ECDLP的难解性,所以攻击者无法获取每个参与者的子密钥 k_i,从而无法获取 (i, y_i)。攻击者若想从公开参数 $A_l = a_l G \pmod n$, $1 \leqslant l \leqslant t-1$ 和 $D_i = (i, f(i)) - k_i Q$ 中获取子密钥 $k_1, k_2, \cdots, k_n$,必须求解ECDLP难题,所以无法重构主密钥。

当每个参与者收到各自的子密钥 k_i 后,计算 $C_i = k_i Q$,和 $(i, y_i) = (D_i + C_i) \pmod n$,并通过公式 $y_i G = \sum_{k=0}^{t-1} A_l i_i^l \pmod n$ 判断子密钥的真实性,从而可以有效地防止密钥管理中心的欺诈行为。在密钥的重构过程中,参与者之间可以通过单向hash函数 $F_i = H(C_i)$ 来验证参与者之间子密钥的真实性,从而可以有效地防止恶意参与者提供虚假子密钥的可能性。

4 结束语

密钥共享是密码学的一个重要的研究课题,具有广泛的应用前景。由于具有密钥短、强度高、参数少等优点椭圆曲线密码也正得到越来越多的应用。本文提出了一个基于椭圆曲线密码系统的多秘密共享方案,该方案安全性基于Shamir门限机制和椭圆曲线难题(ECDLP),能有效地阻止密钥分发者欺诈和参与者欺诈,并可以灵活地对主密钥及子密钥进行更新。

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, Kabatianski G A.Ideal perfect threshold schemes and MDS codes[C]//IEEE International Symposium on Information Theory,ISIT'5,1995.

[3] Wang F, Gu L, Zheng S, et al.A novel verifiable dynamic multi-policy secret sharing scheme[C]//The 12th International Conference on Advanced Communication Technology(ICACT2010).Paris,France:IEEE,2010:1474-1479.

[4] McEliece R J, Sarwate D.On sharing secrets and Reed-Solomon codes[J].Communications of the ACM,1981,24:583-584.

[5] 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 Symp on the Foundations of Computer Science(FOCS),1985:383-395.

[6] Yang Chouchen, Chang Tingyi, Hwang Minshiang.A (t, n) multi-secret sharing scheme[J].Appl Math Comput,2004,151(2):483-490.

[7] Shao Jun, Cao Zhenfu.A new efficient (t, n) Verifiable Multi Secret Sharing(VMSS) based on YCH scheme[J].Appl Math Comput,2005,168(1):135-140.

[8] 许春香,魏仕民,肖国镇.定期更新防欺诈的秘密共享方案[J].计算机学报,2002,25(6):657-660.

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net