一种可认证的动态秘密共享方案 [1]

刘 媛 尹 青 张利民

(信息工程大学信息工程学院 郑州 450002)

摘 要 该文基于椭圆曲线加密的安全性提出了一种改进的秘密共享方案。该方案可防欺骗、防参与者数据误发，参与者和管理者相互之间能相互进行身份认证，并且较好地解决了秘密共享的更新和复用问题。该方案在现在网络通信中有较高的应用价值。

关键词 秘密共享，门限体制，椭圆曲线加密，认证

中图号 TN918

1 引 言

现实生活中有一些重要的事情或信息，如果只由某个人单独保管，那是极其危险的，容易被破坏、篡改、丢失。所以，它需要多人分开掌管。比如银行或政府机要库门的开启、导弹的发射、网络密钥的管理等等。由此建立了秘密共享体制：将要保管的密钥 s 分成 n 个子密钥 (shares)，分发给 n 个参与者 P 分开保管，当且仅当 l 个或更多的参与者 P 出示他们的子密钥时才能恢复出密钥 s，而少于 l 个子密钥则得不到关于密钥 s 的任何信息。

在计算机网络迅速发展的今天，安全性问题越来越重要，为防止欺骗行为，密钥的管理者与参与者身份的相互认证，已经成为网络安全的关键问题。而在以前的秘密共享方案中 [1,2]，它假定管理者 D 和参与者 P 都是诚实可信的，认为由他们提供的子密钥或管理者分发的子密钥都是正确的，这显然不合理，它不能防止欺诈者和非法成员的参与，同时参与者 P 也无法认证管理者 D 的合法身份。

另外，秘钥共享体制为适应现代的发展，提出了密钥的更新和复用问题，即不修改子密钥就不能更新所保管的密钥或在恢复旧密钥后所有用过的密钥都不再用。文献 [3–6] 初步对密钥的认证及签名进行了探讨，但没有有效地解决密钥的更新和复用问题。或者引入了较多的参数选取，给方案的实施和计算以一定的烦琐，参与者与管理者也无法认证相互的身份合法性。

本文基于椭圆曲线加密的安全性提出了一种新的秘密共享方案，椭圆曲线加密 [7] 是对曲线上的点进行加密，明文为两个参数，这样就有效地解决了密钥的更新和复用问题。并且使管理者 D 和参与者 P 可以互相认证身份，防止了非法成员的参与及欺诈。而且椭圆曲线加密速度快，安全性高，方便简洁。

2 方案设计

本方案首先有一个管理者或管理中心 D(dealer)， n 个参与者 $P=\{P_1,P_2,\cdots,P_n\}$。

首先 D 选取一个大素数 p，设 E 为一个定义在 Z_p 上的椭圆曲线 $(y^2=(x^3+h_1x+h)(\mathrm{mod}p)$，这里 $h_1,h\in Z_p$ 是一个满足 $4h_1^3+27h^2\neq 0(\mathrm{mod}p)$ 的常数)，则 E 包含一个循环子群 H，其阶至少被一个大素因子整除。令 $\tilde{P}=Z_p^*\times Z_p^*$, $C=E\times Z_p^*\times Z_p^*$，定义 $K=\{E,\alpha,a,\beta|\beta=a\alpha\}$，其中 $\alpha\in E, a(1\leq a<\mathrm{ord}(\alpha))$ 为私钥 (其中 $\mathrm{ord}(\alpha)$ 是 α 元的阶)，公开 α,β。然后每个参与者 P_i 选取 $\alpha_i\in E, a_i$, $\beta_i=a_i\alpha_i$，公开 α_i,β_i。

D 按下述步骤发送密钥 (1) 在 Z_p 中随机选取 $l-1$ 个数 $b_1,b_2,\cdots,b_{l-1}(b_{l-1}\neq 0)$，构成多项式：

$$f(x)=s_0+b_1x+b_2x^2+\cdots+b_{l-1}x^{l-1}\mathrm{mod}p \tag{1}$$

[1] 2002-06-10 收到，2002-12-25 改回

"九五" 国家密码发展基金资助、河南省高校杰出科研人才创新工程项目 (HAIPURT2001KYCX007)、河南省自然科学基金 (0111060100)、中国博士后基金资助

(2) 随机选取 $x_i \in Z_p$, $k_i \in Z_{|H|}$, $(1 \le i \le n)$, 计算 $f(x_i)$；取 t_0 为即时时间，将明文设为 $m_i = (z_{i1}, z_{i2}) = (f(x_i), t_0 \bmod p)$，加密明文：

$$e_i(m_i) = (y_{i0}, y_{i1}, y_{i2}) \tag{2}$$

其中 $y_{i0} = k_i\alpha_i$, $(c_{i1}, c_{i2}) = k_i\beta_i$, $y_{i1} = c_{i1}z_{i1}$, $y_{i2} = c_{i2}z_{i2}$。

(3) 计算

$$\gamma_0 = s_0\alpha, \quad \gamma_i = b_i\alpha, \qquad 1 \le i \le l-1 \tag{3}$$

公开 $\gamma_i (1 \le i \le l-1)$, 将 $(x_i, e(m_i))$ 发送给参与者 $P_i (1 \le i \le n)$。

恢复密钥　(1) l 个参与者 $P_{i_j} (1 \le j \le l)$ 先计算：$a_{i_j}y_{i_j0} = (c_{i_j1}, c_{i_j2})$，然后进行解密：

$$d(m_{i_j}) = (z_{i_j1}, z_{i_j2}) = (f(x_{i_j}), t_0) = (y_{i_j1}c_{i_j1}^{-1} \bmod p, y_{i_j2}c_{i_j2}^{-1} \bmod p) \tag{4}$$

再将解密后的明文用 D 的密钥进行加密：

$$e_{i_j}(d(m_{i_j})) = (y_{i_j0}, y_{i_j1}, y_{i_j2}) (\bmod p) \tag{5}$$

其中 $y_{i_j0} = k_{i_j}\alpha$, $(c_{i_j1}, c_{i_j2}) = k_{i_j}\beta$, $y_{i_j1} = c_{i_j1}z_{i_j1}$, $y_{i_j2} = c_{i_j2}z_{i_j2}$, $k_{i_j} \in Z_{|H|}$ 为 $p_{i_j} (1 \le j \le l)$ 随机选取。将 $(y_{i_j0}, y_{i_j1}, y_{i_j2})$ 回送给 D；

(2) D 通过 $(c_{i_j1}, c_{i_j2}) = ay_{i_j0}$，解密 $m_{i_j} = (y_{i_j1}c_{i_j1}^{-1} \bmod p, y_{i_j2}c_{i_j2}^{-1} \bmod p)$ 算出 $f(x_{i_1}), f(x_{i_2}), \cdots, f(x_{i_l})$，检验 $f(x_{i_j})$ 的正确与否可认证出参与者 P_{i_j} 的合法身份，再利用 Lagrange 插值多项式：$s_0 = f(0) = \sum_{j=1}^{l} f(x_{i_j}) \prod_{h=1, h\ne j}^{l} \frac{-x_{i_h}}{x_{i_j} - x_{i_h}}$，即可恢复出密钥 s_0。

身份认证　(1) 管理者 D 对参与者 $P_i (1 \le i \le n)$ 的身份进行认证：先检查 t_0 是否正确。t_0 不对则参与者为非法入侵者，如 t_0 正确再检验 $f(x_i)$ 正确与否，如不成立，则参与者数据错误，为欺诈者。

(2) 参与者 $P_i (1 \le i \le n)$ 对管理者 D 的身份进行认证：计算：$F(x_i) = f(x_i)\alpha$，检验 $F(x_i) = \gamma_0 + \sum_{j=1}^{l-1} \gamma_j x_i^j$ 是否正确，则可认证出 D 身份的合法性。

密钥更新　D 在分配了 i 个密钥 $s_0, s_1, \cdots, s_{i-1}$ 后，要分配第 $i+1$ 个密钥，D 只要重复发送密钥的步骤即可。因为此时时间参数为 t_i，分配密钥 $s_0, s_1, \cdots, s_{i-1}$ 时每次对应分配的 $t_0, t_1, \cdots, t_{i-1}$ 各不相同，所以 $(x_i, e(m_i))$ 各不相同，子密钥数据间没有任何联系。

定理 1　经上述的选取，加密 $e(m) = (y_0, y_1, y_2)$ 后，用 $d(e(m)) = (y_1c_1^{-1} \bmod p, y_2c_2^{-1} \bmod p)$ 能解出明文。

证明　因为 $y_0 = k\alpha$, $y_1 = c_1z_1$, $y_2 = c_2z_2$, $(c_1, c_2) = k\beta$, 而 $\beta = a\alpha$, $m = (z_1, z_2)$, 则 $ay_0 = ak\alpha = ka\alpha = k\beta = (c_1, c_2)$, $d(e(m)) = (y_1c_1^{-1} \bmod p, y_2c_2^{-1} \bmod p) = (c_1z_1c_1^{-1} \bmod p, c_2z_2c_2^{-1} \bmod p) = (z_1 \bmod p, z_2 \bmod p)$。　证毕

定理 2　每个参与者 $P_i (1 \le i \le n)$ 都能通过检验 $F(x_i) = \gamma_0 + \sum_{j=1}^{l-1} \gamma_j x_i^j$ 来认证管理者 D 的合法身份。

证明　因为 $\gamma_0 = s_0\alpha$, $\gamma_i = b_i\alpha (1 \le i \le l-1)$, 则 $\gamma_0 + \sum_{j=1}^{l-1} \gamma_j x_i^j = s_0\alpha + \sum_{j=1}^{l-1} b_j\alpha x_i^j = \alpha(s_0 + \sum_{j=1}^{l-1} b_j x_i^j) = \alpha f(x_i) = F(x_i)$。　证毕

3 性能分析

(1) 此方案的安全性是基于椭圆曲线上离散对数难解问题。发送的数据 $(x_i, e(m_i))$ 公开，任何人都可以得到，但是并不能解出 $f(x_i)$ 和 t_0。其他人要得到 a_i, a，则必须解椭圆曲线上离散对数问题，是难解的。所以 $f(x_i)$ 和 t_0 是安全的；

(2) 即使参与者中有欺骗者，或想用错误数据得到其它的数据，但通过检验 $f(x_i)$ 和 t_0 可认证出其合法身份来，所以欺骗不能成功，也可防止非法成员的参与；

(3) 此方案可以让参与者 $P_i(1 \le i \le n)$ 通过验证 $F(x_i) = \gamma_0 + \sum_{j=1}^{l-1} \gamma_j x_i^j$ 来认证 D 的合法性，它防止了非法者从管理中心进行的破坏参与。在网络通信中有很重要的应用；

(4) 若由于某种情况，j 个密钥 $f(x_j)$ 已被公开，也不会影响到其它 $n-j$ 个密钥 $f(x_i)$ 的安全，因为 x_i 各不相同，所以 $f(x_i)$，e_i 各不相同，相互之间没有任何联系，且 a_i 与 a_j 不同，所以从 $f(x_j)$ 不能得到 $f(x_i)$ 的任何信息，则是安全的；

(5) 此方案分配密钥是按 Shamir 秘密共享体制分配的，并对密钥 $f(x_i)$ 进行了加密，传送的数据都是经过椭圆曲线加密的，在通信过程中是安全的。少于 l 个子密钥 $f(x_i)$ 是得不到密钥 s_0 的任何信息的，所以此方案没有降低门限值；

(6) 从发送数据的规模可得，此方案的信息率为 1/4；

(7) 此方案引入了即时时间 t 作为参数，减少了其他参数的选取，进行的解密、加密、验证都是椭圆曲线上的加减法运算，且是在椭圆曲线上的加密，长度为 160bit 的素数 p 仅相当于大数分解 RSA 中长度为 1024bit 素数的难度。因而此方案速度快、安全性高、方便简洁。

参 考 文 献

[1] A. Shamir , How to share a secret, Communications of the ACM, 1979, 22(11), 612–613.

[2] G. R. Blakley, Safeguarding cryptographic keys, In Proc. of the AFIPS 1979 National Computer Conference, New York, June 1979, vol.48, 313–317.

[3] Wakaha Ogate, Karu Kurosawa, Optimum secret sharing scheme secure against cheating, EURO-CRYPT'96 Proceedings, Berlin Heidelberg, Springer-Verlag, 1996, 200–211.

[4] Markus Stadler, Publicly verifiable secret sharing, EURO-CRYPT'96 Proceedings, Berlin Heidelberg, Springer-Verlag, 1996, 190–199.

[5] 张建中，谢淑翠，一个新的可防止欺诈的动态秘密共享方案，密码学进展，CHINACRYPT'2000, 北京，科学出版社，2000, 108–111.

[6] 卢建朱，陈火炎，具有 (t,n) 共享验证的认证加密方案及其安全性，计算机研究与发展，2001, 38(9), 1042–1054.

[7] 冯登国，裴定一，密码学导引，北京，科学出版社，1999, 166–167.

A VERIFIABLE DYNAMIC SECRET SHARING SCHEME

Liu Yuan Yin Qing Zhang Limin

(*Info. Security Institute, Information Engineering University, Zhengzhou* 450002, *China*)

Abstract In the paper, an improved secret sharing scheme based on elliptic curve cryptography is proposed. It guarantees the mutual identity authentication between the legal dealer and the participating parties and can protect against the cheating action. The problems of renew and reuse are properly treated. The scheme may be applicable in practical network communication.

Key words Secret sharing, Threshold scheme, Elliptic Curve Cryptograph (ECC), Authentication

刘 媛：女，1965 年生，博士生，研究方向为密码学与信息安全.

尹 青：女，1968 年生，博士生，研究方向为计算机网络安全.

张利民：男，1952 年生，教授，博士生导师，研究方向为密码学与信息安全.