文章编号:1005－0523(2005)04－0155－03

一个新的防欺诈动态门限秘密分享方案

韩金广,亢保元,王庆菊

(中南大学 数学科学与计算技术学院,湖南 长沙 410075)

摘要:一个门限方案是将一个秘密分成个子秘密,并将这些子秘密分发给个参与者,使得:知道任意个或更多个子秘密可以将该秘密恢复,而知道任意个或更少个子秘密却不能将该秘密恢复的一种秘密分享方案.动态门限方案是一种特殊的门限方案,其特点是:更新要分享的秘密无需修改和收回任何子秘密.本文将离散对数、整数分解、求高次方根等数学难题相结合,提出了一个新的防欺诈动态门限秘密分享方案,并讨论了其安全性.

关 键 词:密码学; 秘密分享; 动态门限方案

中图分类号:TN918.1 **文献标识码**:A

0 引 言

随着知识经济、信息产业的发展,信息的安全保密问题日益突出并受到社会的广泛关注.一些重要的秘密信息若由一个人保管,易引起丢失、损坏或窜改,是很不安全的.为此提出了门限方案,即秘密分享方案,是实现重要秘密分散保管的好方法.一个(t,n)门限方案是指把一个秘密分拆成个子秘密(也称影子),使得

1) 知道任意 t 个或更多的子秘密可以恢复秘密 S;

2) 知道任意 $t-1$ 个或更少子秘密却无法恢复秘密 S.

1979 年A·Shamir[1] 和G·R· Blakley[2] 各自独立地提出了一个简单的(t,n)门限秘密分享方案,这两个方案都可以用于重要秘密的分散保管.到目前,已有许多(t,n)门限方案被提出来[3－8].但有些方案在效率和实现方面都有缺点[4].同时,还有更新和复用问题.所谓更新问题是指如果不修改密钥就不能更新所分享的秘密;复用问题是指在恢复了旧秘密之后,所用过的子秘密不能重复用来分享新的秘密[9].针对这些问题提出了动态秘密分享的概念[10].一个高效且实用的动态秘密分享方案应该具有这样的特点:更新要分享的秘密,无需修改和收回任何子秘密.目前,一些动态方案已被提出[9－11],但有些方案不能有效的防止欺诈[10].本文将离散对数、整数分解、求高次方根等数学难题相结合,提出了一个可以检测伪子秘密、防止欺诈的动态秘密分享方案.

1 引 理

引理 设 p 为一素数,Z_p 为一有限域,任意的 $k_1,k_2,x,a,b,m\in Z_p^*$,且$(m,p-1)=1$,若 $k_1a^x=k_2b^x=$与 $k_1a^{x+m}=k_2b^{x+m}$ 同时成立,则 $a=b$.

证明 由 $k_1a^x=k_2b^x$

得 $k_1k_2^{-1}(ab^{-1})^x=1$ ①

由 $k_1a^{x+m}=k_2b^{x+m}$

得 $k_1k_2^{-1}(ab^{-1})^{x+m}=1$ ②

由(1) 和(2) 得

收稿日期:2005－03－19

作者简介:韩金广(1979－),男,河北涉县人,中南大学硕士研究生,从事密码学研究.

$$k_1k_2^{-1}(ab^{-1})^x = k_1k_2^{-1}(ab^{-1})^{x+m}$$

即 $$(ab^{-1})^m = 1$$

若 $a \neq b$，则 $ab^{-1} \neq 1$，$o(ab^{-1}) \neq 1$，

而 $o(ab^{-1}) \mid m$，$o(ab^{-1}) \mid p-1$

所以 $1 \neq 0(ab^{-1}) \mid (m, p-1) = 1$ 矛盾，故 $a = b$.

2 动态秘密分享方案

设 p 为一大的素数，且 $p-1$ 有两个大的素数因子 q_1 和 q_2，令 $q = q_1q_2$. 除特殊说明外所有运算都在 Z_p 中进行. 设现有参与者集合 $P = \{P_1, P_2, \cdots, P_n\}$ 和要分享的秘密集合 $S = \{s_1, s_2, \cdots, s_k\}$.

1) 准备阶段

分发者需要做以下工作：

● 选取 $c_1 = p_1^2, c_2 = p_2^2, \cdots, c_n = p_n^2, p_i \neq p_j (i \neq j)$，$p_i \in Z_p^* (i = 1, 2, \cdots, n)$，并将 p_i 秘密地分发给参与者 p_i，作为参与者 p_i 的密钥.

● 选取 $x_1, x_2, \cdots, x_n \in Z_p$，其中 $x_i \neq x_j (i \neq j)$，$a \in Z_p^*$，并将 $x_1, x_2, \cdots, x_n$，a 公开.

2) 子秘密生成阶段

假设要分享秘密 $s_j \in S$，分发者需要做以下工作：

● 选取多项式

$f_j(x) = s_j + a_{j1}x + a_{j2}x^2 + \cdots + a_{jt-1}x^{t-1}$，$a_{ji} \in Z_P (i = 1, 2, \cdots, t-1)$，且 $f_j(x_i) \neq 0 (i = 1, \cdots, n)$.

● 随机地选取 $w_j, \alpha_i \in Z_p^* (\alpha \neq 1)$，$m_i, k_i \in Z_p$，且满足 $2 \leqslant m_i < k_i < \frac{p}{2}$，$2 \leqslant k_i - m_i < \frac{p}{2}$，$(k_i, m_i) \neq 1$，$(m_i, p-1) = 1$.

● 计算

$f_j(x_i) = z_i$（z_i 称为子秘密）

$$\beta_i = \alpha_i^{p_i^3} \tag{3}$$

$$y_{i1} = \alpha_i^{k_i} \tag{4}$$

$$y_{i2} = (\alpha + wz_i)\beta_i^{(c_i^2 + w_ic_i)^2 k_i} \tag{5}$$

$$t_{i1} = (\alpha + wz_i)^{k_i} \tag{6}$$

$$t_{i2} = (\alpha + wz_i)^{k_i + m_i} \tag{7}$$

其中 $(t_{i1}, t_{i2}, w_i, m_i, k_i)$ 为子秘密 z_i 的验证向量，分发者公布 $(y_{i1}, y_{i2}, t_{i1}, t_{i2}, w_i, m_i, k_i)$.

3) 子秘密获得阶段

参与者 P_i 在公布栏中得到 $(y_{i1}, y_{i2}, t_{i1}, t_{i2}, m_i, k_i)$ 后，利用密钥 p_i 计算 $z_i = (y_{i2}(y_{i1}^{p_i^3(c_i^2 + w_ic_i)^2})^{-1} - a)w_i^{-1}$。实际上

$$\begin{aligned}
&y_{i2}(y_{i1}^{p_i^3(c_i^2+w_ic_i)^2})^{-1} - a)w_i^{-1} \\
&= ((a + wz_i)\beta_i^{(c_i^2+w_ic_i)^2 k_j}(\alpha_i^{p_i^3(c_i^2+w_ic_i)^2 k_i})^{-1} - a)w_i^{-1} \\
&= ((a + wz_i)\alpha_i^{p_i^3(c_i^2+w_ic_i)^2 k_j}(\alpha_i^{p_i^3(c_i^2+w_ic_i)^2 k_i})^{-1} - a)w_i^{-1} \\
&= (a + wz_i - a)w_i^{-1} \\
&= wz_iw_i^{-1} \\
&= z_i
\end{aligned}$$

4) 子秘密收集、验证及秘密 s_j 恢复阶段

假设 t 个参与者要恢复秘密 s_j，需要每个参与者 P_i 交出子秘密 z_i，同时其余的 $t-1$ 个参与者利用验证向量 $(t_{i1}, t_{i2}, w_i, m_i, k_i)$ 对 z_i 进行验证. 事实上，若存在 $z'_i \in Z_P$ 满足验证向量 $(t_{i1}, t_{i2}, w_i, m_i, k)$，即 $t_{i1} = (a + wz'_i)^{k_i}$，$t_{i2} = (a + wz'_i)^{k_i + m_i}$，则有

$$(a + wz_i)^{k_i} = (a + wz'_i)^{k_i},$$

$$(a + wz_i)^{k_i + m_i} = (a + wz'_i)^{k_i + m_i}.$$

由引理知 $a + wz_i = a + wz'_i$，即 $w_i(z_i - z'_i) = 0$，因为 $w_i \neq 0$，所以 $z_i = z'_i$. 因此参与者 P_i 不可能利用伪子秘密 z'_i 进行欺诈. 所有参与者交出 P_i 交出 z_i，并经验证后，利用拉格朗日插值公式可将多项式 $f_j(x)$ 恢复，从而得到秘密 s_j.

这样重复 k 次可将 k 个秘密 $S = \{s_1. s_2, \cdots, s_k\}$ 全部分享.

5) 秘密更新阶段

假设 k 个秘密已经分享完毕，若想再分享一个秘密 s_{k+1}，分发者所做的工作是重新选择多项式 $f_{k+1}(x)(f_{k+1}(x) \neq f_i(x)(i = 1, \cdots, k))$ 和分发给个每个参与者 P_i 的子秘密 z_i 的匹配值 w_i. 最坏的情况是分享秘密 s_{k+1} 时有一个子秘密 z''_i 与前期分享的秘密 $s_j (j = 1, 2, \cdots, k)$ 的一个子秘密 z_l 相同，即 $z''_i \neq z_l$. 这只需选取 $z''z''_i = a + wz_l$ 的匹配值 w_l 与的匹配值不相同，即 $w''_i \neq w_l$，就有 $a + w''z''_i \neq a + wz_l$（若 $a + w''z''_i = a + wz_l$，即 $w''z''_i = wz_l$，则由 $z''_i = z_l$，得 $(w''_i - w_l)z_l = 0$，又由 $z_l \neq 0$ 得 $w''_i - w_l = 0$，即 $w''_i = w_l$，，这与 $w''_i \neq w_1$ 矛盾）. 而在所有公布的信息中真正用到的是 $a + w''z''_i$，所以对已经分发过的子秘密 z_l，可以重复利用而不需要收回、销毁或修改. 该方案秘密可以更新，子秘密可以重复利用，所以是一个动态秘密分享方案. 可见尽管在恢复 $s_1, \cdots, s_k$ 时已经公开了一些子秘密，但这些公开的子秘密不会泄露关于秘密 s_{k+1} 的信息. 也就是说在前 k 个秘密已经分享的情况下，s_{k+1} 的分享仍然是安全的. 所以分发者可以随意扩大秘密集合 S 和参与者集合 P.

3　安全性分析

1) 假若攻击者想利用公式(6)和(7)得到 z_1，因为 $2 \leqslant m_i < k_i < \frac{p}{2}$ 直接计算 z_i 需求高次方根，这是困难的. 如果取 $v_{i1}, v_{i2} \in Z_p$，计算

$$t_{i1}^{v_{i1}} t_{i2}^{v_{i2}} = (a + wz_i)^{k_i v_{i1} + (m_i + k_i) v_{i2}} = (a + wz_i)^{(v_{i1} + v_{i2}) k_i + v_{i2} m_i}$$

由 $(m_i, k_i) \neq 1$，得 $(v_{i1} + v_{i2}) k_i + v_{i2} m_i \neq 1$. 又由 $(m_i, p-1) = 1$ 可得，$(v_{i1} + v_{i2}) k_i + v_{i2} m_i \neq p-1$，(否则 $(v_{i1} + v_{i2}) k_i + v_{i2} m_i = p-1$，由 $(m_i, p-1) = 1$，知存在 $e_{i1}, e_{i2} \in Z_p$，使得 $e_{i1} m_i + e_{i2}(p-1) = 1$，有 $e_{i2}(v_{i1} + v_{i2}) k_i + (e_{i2} v_{i2} + e_{i1}) m_i = 1$，与 $(k_i, m_i) \neq 1$ 矛盾). 故由此得到 z_i 至少要求关于 $(a + wz_i)$ 的二次方根，但这是计算不可行的因为没有人知道 q 的两个大的因子 q_1 和 q_2[12]. 如果攻击者试图找到 v'_{i1}, v'_{i2}，使得 $l'_i = (v'_{i1} + v'_{i2}) k_i + v'_{i2} m_i \mid p-1$，即 $l'_i h'_i = p-1$ 然后求 $((a + wz_i)^{l'_i h'_i})^{-1} = a + wz_i$ 得到 z_i，需要将 $p-1$ 整数分解，这是极其困难的.

2) 假若攻击者想利用公式(4)和(5)通过得到 $y_{i2} = (a + wz_i) y_{i1}^{p_i^3 (c_i^2 + w_i c_i)^2}$ 得到 z_i，他需要处理整数分解问题，若想得到 p_i，需要处理离散对数、整数分解及高次方根问题. 子秘密 z_i 公开后，要得到 $p_i^3 (c_i^2 + w_i c_i)^2$ 需要处理离散对数问题，再得到 p_i 需要求高次方根. 以上涉及到的均为难处理的数学问题.

3) 假若攻击者利用公式(4)，(5)，(6)，(7)得到 p_i, z_i，他需要处理离散对数、整数分解及高次方根等数学难题. 尤其是 (α, β_i) 均未公开，计算 p_i^3 比较困难，由 p_i^3 要得到参与者 p_i 的密钥 p_i 还需要求三次方根，这是困难的.

4　结　论

1) 将离散对数、整数分解、求高次方根等数学难题相结合，提出了一个新的防欺诈动态门限秘密分享方案，并给出了检测伪子秘密，防止欺诈的有效方法.

2) 本方案以多个数学难题为基础，安全性较强，对数据的利用率高，解决了秘密的更新和复用问题.

参考文献：

[1] A·Shamir· How to share a secret[J]· Comm· Acm, 1979, 22 (11): 612—613.

[2] G·R·Blakley· Safeguading cryptographic key[A], Proceeding of National Computer Conference of AFIPS[C]· New York: AFIPS, Press, 1979, 48: 313—317.

[3] liu· Hung—Yu, Harn ·Lein· Fair reconstruction of a secret [J]· Information Processing Letters, 1995, 55: 45—47.

[4] B·Schneier· Applied Cryptography (2 nd Edition)[M]· New York: John wiley & Sons, Inc, 1994.

[5] R·G·E·Pinch· Online multiple secret sharing[J]· Electronics Letters, 1996, 32(1): 1087—1088.

[6] ·P·Morillo, C·Padro, G·Saez, et al· Weighted threshold secret sharing schemes[J]· Information Processing Letters, 1999, 70: 211—216.

[7] D·R·Stinson· Decomposition constructions for secret sharing schemes[J]· IEEE Trans on Inform Theory, 1994, 40: 118—125.

[8] Carles Padro· Robust Vector space secret sharing schemes[J]· Information Processing Letters, 1998, 68: 107—111.

[9] 张建中，肖国镇. 可防止欺诈的动态秘密分享方案[J]. 通信学报, 2000, 2:81—83.
ZHANG Jan-zhong· A dynamic secret sharing scheme to identify cheaters[J]· Journal of China Institute of Communications, 2000, 2: 81—83.

[10] C·S·Laih, L·Hurn, J·Y·Lee, et al· Dyna mic threshold scheme based on the definition of cross-product in an N-dimensional linear space[J]· Information Science and Engineering, 1991, 7: 13—23.

[11] H·M·Sun, S·P·Shich· Construction of dynamic threshold shemes[J]· Electronics letters, 1994, 30(24): 2023—2025.

[12] J·He, T·Kiesler· Enhancing the security of EI Gamal's signature sheme[J]· IEEE pro-comput, Digital·Tech, 1994, 141: 249—252.

(下转第 164 页)

The Limit Behavior of a NLAR Model under the Random Environment

YU Zheng, XIAO Xin-ling

(School of Math. Sciences & Computing Technology, Changsha 410075, China)

Abstract: We study the problem of a variety of nonlinear threshold autoregressive model $X_{n+1}=\Phi(X_n)+\varepsilon_{n+1}(Z_{n+1})$ in which $\{Z_n\}$ is a Markov chain with finite state space, and for every state of the Markov chain, $\{\varepsilon_n(i)\}$ is a sequence of independent and identically distributed random variables, and $\varepsilon_n(Z_n)=:\sum_i \varepsilon_n I_{\{i\}}(Z_n)$. Also, in this paper, the limit behavior of the sequence $\{X_n\}$ defined by the above model is investigated and a sufficient condition for the convergence of sequence $\{X_n\}$ with a geometric convergence rate is provided.

Key words: ergodic; nonlinear time series; random environment.

(上接第 157 页)

A New Dynamic Threshold Secret Sharing Scheme to Identify Cheaters

HAN Jin-guang, KANG Bao-yuan, WANG Qing-ju

(College of Mathematics Science and Computing Technology, Central South University, Changsha, Hunan 410075, China)

Abstract: A threshold sheme is a method whereby pieces of the secret , called shares are distributed to participants so that : the secret can be reconstructed from the knowledge of any or more shares, and the secret cannot be reconstructed from the knowledge of any or less shares. A dynamic secret sharing sheme is an especial threshold sheme. Its character is that the secret can be renewed without modifying and rebaking any share. This paper proposes a new dynamic threshold secrete sharing sheme to identify cheaters by integrating the discrete logarithm problem and the integer factorization problem with higher roots problem. This paper also discusses the security of the sheme.

Key words: crptography; secret sharing; dynamic threshold scheme