

文章编号:1001-9081(2007)08-1913-02

基于特殊差分方程的安全的多重秘密门限共享方案

张艳硕^{1,2}, 刘卓军²

(1. 北京电子科技学院 基础部, 北京 100070; 2. 中国科学院 数学机械化重点实验室, 北京 100080)
(zhangyanshuo@amss.ac.cn)

摘 要:介绍了多重秘密门限秘密共享方案,该方案通过一次秘密共享过程就可实现对任意个秘密的共享,而参与者秘密份额的长度仅为一个秘密的长度。同时,考虑了此类门限方案的安全性,基于特殊差分方程给出安全的多重门限秘密共享方案。分析表明,给出的门限秘密共享方案的信息率为 $1/2$,且对于防欺诈是无条件安全的。

关键词:门限秘密共享; 安全; 差分; 多重秘密

中图分类号: TP309.08 **文献标志码:** A

Secure threshold multi-secret sharing scheme based on special difference equation

ZHANG Yan-shuo^{1,2}, LIU Zhuo-Jun²

(1. Department of Basic Sciences, Beijing Electronic Science and Technology Institute, Beijing 100070, China;
2. Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: A multi-secret threshold secret sharing scheme was introduced. Through one process of secret sharing, any secret sharing could be achieved, and participants share a secret and the length is only a secret length. Meanwhile, considering such programs threshold of safety, a secure threshold multi-secret sharing scheme based on special difference equation was given. Analysis shows that the given threshold secret sharing scheme has the information rate of $1/2$, and for fraud prevention is unconditionally safe.

Key words: threshold secret sharing; secure; difference; multi-secret

0 引言

秘密共享是信息安全和数据保密的重要方法,它在秘密数据的安全保存、传输及合法利用中起着非常重要作用。自从文献[1,2]分别提出了秘密共享体制以来,有关秘密共享体制的研究受到了广泛关注。

文献[3-6]分别提出了多重秘密共享体制,各参与者只需保护一个秘密份额,就可以实现多个秘密的共享。文献[7]基于系统分组码提出另一种 (t, n) 门限多重秘密共享体制。文献[8]给出了一个有效的 (t, n) 门限多重秘密共享体制。

文献[9]基于差分构造出具有特殊权限的秘密共享方案,在此基础上,考虑到门限方案的安全性和门限多重秘密共享体制,本文给出基于特殊差分方程的安全的多重秘密门限秘密共享方案。

1 Shamir 门限秘密共享方案

文献[2]的门限方案是构造一个 $t-1$ 次多项式,即如果已知多项式在 t 个不同点的插值,则可计算出该多项式。具体描述如下:

设共享秘密 $K, p(p > t)$ 是素数,有 n 个参与者。密钥分发者随机选取 z_p 中一个 $t-1$ 次多项式: $s(x) = s_0 + s_1x + \dots + s_{t-1}x^{t-1}, s_i \in Z_p, i = 0, 1, 2, 3, \dots, t-1$, 其中 $s_0 = K$ 。

密钥分发者计算在 n 个不同点 x_i 处的值 $y_i = s(x_i)$, 并将点对 $(x_i, y_i) (i = 1, 2, \dots, n)$ 分别发给这 n 个参与成员,由此可构成一个 (n, t) 门限方案。

2 齐次常系数线性差分方程的解

形如下列的差分方程称为齐次常系数线性差分方程^[8]:

$$a_n + b_1 a_{n-1} + b_2 a_{n-2} + \dots + b_t a_{n-t} = 0 \quad (1)$$

其中 b_1, b_2, \dots, b_t 为常数。当 $b_t \neq 0$ 时,上述差分方程称为 t 阶齐次常系数线性差分方程。对于上述方程的解在文献[9]中已经给出,现简单叙述如下:

齐次常系数线性差分方程(1)的通解具有下列形式:

$$a_n = c_1 f_1(n) + c_2 f_2(n) + \dots + c_t f_t(n) \quad (2)$$

其中 c_1, c_2, \dots, c_t 是可以由初始条件确定的待定常数, $f_i(n) (i = 1, 2, \dots, t)$ 为 n 的函数。

当齐次常系数线性差分方程(1)的特征方程有 t 个不相同的实根 $r_1, r_2, r_3, \dots, r_t$ 时,齐次常系数线性差分方程的通解为:

$$a_n = c_1 r_1^n + c_2 r_2^n + \dots + c_t r_t^n \quad (3)$$

其中 $c_1, c_2, c_3, \dots, c_t$ 为任意常数,由初始条件确定它们的取值^[9]。

3 安全的多重秘密门限方案

门限方案一般都包括参数假设、秘密分发和秘密恢复三

收稿日期:2007-03-05;修回日期:2007-04-26。 基金项目:国家973计划资助项目(2004CB318000)。

作者简介:张艳硕(1979-),男,陕西宝鸡人,讲师,博士研究生,主要研究方向:密码学、信息安全、密码学代数基础; 刘卓军(1958-),男,山东即墨人,研究员,博士生导师,主要研究方向:密码学、编码学和符号计算。

个部分。

1) 参数假设

设参与者集合有 m 个参与成员 $\{P_1, P_2, \dots, P_m\}$, t 为门限值, 设 $p(t < m < p)$ 是大素数, 秘密分发者选取 Z_p 中的一个数列 $\{a_i\}$, 这个数列首先满足齐次常系数线性差分方程:

$$a_n + b_1 a_{n-1} + b_2 a_{n-2} + \dots + b_{2t-1} a_{n-2t+1} = 0 \quad (4)$$

其中: $b_i \in Z_p (i = 1, 2, \dots, 2t-1)$ 且公开, 显然 $n > 2t$ 。构成的差分方程的特征方程必须有 $2t-1$ 个不相同且不为零的实根, 即该特征方程没有重根。这是该差分方程的特殊之处。假设 $s_i (i = 1, 2, \dots, k)$ 表示 k 个要被共享的秘密。

2) 秘密分发

秘密分发者从齐次常系数线性差分方程(1)中计算出 $a_0, a_1, a_2, \dots, a_{m-1}; a_m, a_{m+1}, a_{m+2}, \dots, a_{m+m-1}$ 并保密。

秘密分发者再从齐次常系数线性差分方程(1)中计算出 $a_{2m}, a_{2m+1}, a_{2m+2}, \dots, a_{2m+k}$ 并保密, 然后计算出 $p_i = s_i - a_{2m+i} \bmod p (i = 1, 2, \dots, k)$, 并将 $\{p_1, p_2, \dots, p_k\}$ 公开, 显然 $s_i = p_i + a_{2m+i} \bmod p (i = 1, 2, \dots, k)$ 。

秘密分发者将 $(a_{i-1}, a_{m+i-1}) (i = 1, 2, 3, \dots, m)$ 作为参与者集合 A 中第 $i (i = 1, 2, \dots, m)$ 个参与者的子秘密发给该参与者。秘密分发者将数列 $\{a_i\}$ 保密。虽然 $b_i \in Z_p (i = 1, 2, \dots, 2t-1)$ 是公开的, 但数列 $\{a_i\}$ 满足的方程(1)是保密的。

显然参与者集合中至少 t 个参与者只有协作才能得到 k 个共享的秘密 $s_i (i = 1, 2, \dots, k)$ 。

3) 秘密恢复

恢复秘密的参与者个数达到要求, 即不少于门限值 t , 也就是参与者集合中参与秘密恢复的参与者个数大于等于 t , 不失一般性, 假设参与者集合中恢复秘密的 t 个参与者的子密钥是: $(a_i, a_{i+m}) (i = 0, 1, 2, \dots, t-1)$ 。

参与者集合中恢复秘密的 t 个参与者的子密钥 $(a_i, a_{i+m}) (i = 0, 1, 2, \dots, t-1)$ 和公开的 $b_i \in Z_p (i = 1, 2, \dots, 2t-1)$ 构建差分方程(4), 用特征方程法对齐次常系数线性差分方程求解得:

$$a_n = c_1 f_1(n) + c_2 f_2(n) + \dots + c_{2t-1} f_{2t-1}(n) \quad (5)$$

此差分方程有 $2t-1$ 个不相同的实根, 再取 $r_{2t} \neq 0 \in Z_p, r_{2t} \neq r_i, i = 1, 2, \dots, 2t-1$, 令:

$$a_n = c_1 r^n + c_2 r_2^n + \dots + c_{2t} r_{2t}^n \quad (6)$$

再由参与者集合中恢复秘密的 t 个参与者的子密钥: $(a_i, a_{i+m}) (i = 0, 1, 2, \dots, t-1)$, 代入初值 $a_0, a_1, \dots, a_{t-1}; a_m, a_{m+1}, \dots, a_{m+t-1}$, 可得到 $2t$ 个方程组成的方程组:

$$\begin{cases} c_1 f_1(0) + c_2 f_2(0) + \dots + c_{2t} f_{2t}(0) = a_0 \\ c_1 f_1(1) + c_2 f_2(1) + \dots + c_{2t} f_{2t}(1) = a_1 \\ c_1 f_1(2) + c_2 f_2(2) + \dots + c_{2t} f_{2t}(2) = a_2 \\ \vdots \\ c_1 f_1(t-1) + c_2 f_2(t-1) + \dots + c_{2t} f_{2t}(t-1) = a_{t-1} \\ c_1 f_1(m) + c_2 f_2(m) + \dots + c_{2t} f_{2t}(m) = a_m \\ c_1 f_1(m+1) + c_2 f_2(m+1) + \dots + c_{2t} f_{2t}(m+1) = a_{m+1} \\ c_1 f_1(m+2) + c_2 f_2(m+2) + \dots + c_{2t} f_{2t}(m+2) = a_{m+2} \\ \vdots \\ c_1 f_1(m+t-1) + c_2 f_2(m+t-1) + \dots + c_{2t} f_{2t}(m+t-1) = a_{m+t-1} \end{cases} \quad (7)$$

也就是方程组:

$$\begin{cases} c_1 r_1^0 + c_2 r_2^0 + \dots + c_{2t} r_{2t}^0 = a_0 \\ c_1 r_1^1 + c_2 r_2^1 + \dots + c_{2t} r_{2t}^1 = a_1 \\ c_1 r_1^2 + c_2 r_2^2 + \dots + c_{2t} r_{2t}^2 = a_2 \\ \vdots \\ c_1 r_1^{t-1} + c_2 r_2^{t-1} + \dots + c_{2t} r_{2t}^{t-1} = a_{t-1} \\ c_1 r_1^m + c_2 r_2^m + \dots + c_{2t} r_{2t}^m = a_m \\ c_1 r_1^{m+1} + c_2 r_2^{m+1} + \dots + c_{2t} r_{2t}^{m+1} = a_{m+1} \\ c_1 r_1^{m+2} + c_2 r_2^{m+2} + \dots + c_{2t} r_{2t}^{m+2} = a_{m+2} \\ \vdots \\ c_1 r_1^{m+t-1} + c_2 r_2^{m+t-1} + \dots + c_{2t} r_{2t}^{m+t-1} = a_{m+t-1} \end{cases} \quad (8)$$

差分方程的特征方程有 $2t-1$ 个不相同且不为零的实根, 可由齐次常系数线性差分方程解的结构得系数行列式:

$$D = \begin{vmatrix} r_1^0 & r_2^0 & \dots & r_{2t}^0 \\ r_1^1 & r_2^1 & \dots & r_{2t}^1 \\ r_1^2 & r_2^2 & \dots & r_{2t}^2 \\ \vdots & \vdots & \dots & \vdots \\ r_1^{t-1} & r_2^{t-1} & \dots & r_{2t}^{t-1} \\ r_1^m & r_2^m & \dots & r_{2t}^m \\ r_1^{m+1} & r_2^{m+1} & \dots & r_{2t}^{m+1} \\ r_1^{m+2} & r_2^{m+2} & \dots & r_{2t}^{m+2} \\ \vdots & \vdots & \dots & \vdots \\ r_1^{m+t-1} & r_2^{m+t-1} & \dots & r_{2t}^{m+t-1} \end{vmatrix} \neq 0 \quad (9)$$

上面的方程组是分别由 $2t$ 个方程组成的含有 $2t$ 个变量的线性方程组, 且系数矩阵都可以看作为特殊的范德蒙矩阵, 因而方程组只有唯一解。此时, 当 $c_{2t} = 0$ 时, 所有参与秘密恢复的参与者中没有欺骗存在, 如果 $c_{2t} \neq 0$, 则说明参与者集合中参与秘密恢复的参与者中有欺诈者。这样可以进行责任追究, 进一步检测参与秘密恢复的参与者中究竟哪个参与者进行了欺诈。

由线性方程组的克莱姆法则, 知方程组只有唯一解, 解出待定系数 $c_1, c_2, \dots, c_{2t} (c_{2t} = 0)$, 从而得到数列 $\{a_n\}$ 形如: $a_n = c_1 f_1(n) + c_2 f_2(n) + \dots + c_{2t-1} f_{2t-1}(n)$, 也就是 $a_n = c_1 r_1^n + c_2 r_2^n + \dots + c_{2t-1} r_{2t-1}^n$, 分别计算出 $a_{2m}, a_{2m+1}, a_{2m+2}, \dots, a_{2m+k}$, 参与秘密恢复的参与者由公开的 $p_i = s_i - a_{2m+i} \bmod p (i = 1, 2, \dots, k)$ 可计算 $s_i = a_{2m+i} + p_i \bmod p (i = 1, 2, \dots, k)$, 于是得到 k 个共享的秘密 $s_i (i = 1, 2, \dots, k)$ 。

以上是构造的基于特殊差分方程的安全的多重秘密门限秘密共享方案, 该方案对于这样安全秘密共享问题是可行的, 且具有实际意义。对于这类方法性能的分析结果: 信息率为 $1/2$, 在预防欺诈方面无条件安全。

攻击者如果得不到数列 $\{a_i\}$, 就得不到秘密的任何信息; 如果参与秘密恢复的参与者个数之和少于 t 进行秘密恢复计算, 他们仍然不能构造出数列 $\{a_i\}$, 也不能得到任何秘密信息。

4 结语

基于特殊差分方程, 提出了一种安全的多重秘密门限秘密共享方案, k 个秘密被 m 个参与者所共享, 至少参与秘密恢复的参与者个数之和大于等于 t 的才可一次性的重构这 k 个秘密, 而参与者个数之和少于 t 的参与者集合得不到秘密的任何信息。

(下转第 1918 页)

2) 攻击 2 的攻击场景:

- 1.1 $I(A) \rightarrow B:A$
- 1.2 $B \rightarrow I(A):N_b$
 - 2.1 $C \rightarrow I(B):C$
 - 2.2 $I(B) \rightarrow C:N_b$
 - 2.3 $C \rightarrow I(B):\{N_b\}k_{cs}$
 - 3.1 $A \rightarrow I(C):A$
 - 3.2 $I(C) \rightarrow A:C, \{N_b\}k_{cs}$
 - 3.3 $A \rightarrow I(C):\{C, \{N_b\}k_{cs}\}k_{as}$
 - 4.1 $I(A) \rightarrow S:\{C, \{N_b\}k_{cs}\}k_{as}$
 - 4.2 $S \rightarrow I(A):\{N_b\}k_{as}$
- 1.3 $I(A) \rightarrow B:A, \{N_b\}k_{as}$
- 1.4 $B \rightarrow S:\{A, \{N_b\}k_{as}\}k_{bs}$
- 1.5 $S \rightarrow B:\{N_b\}k_{bs}$

3) 攻击 3 的攻击场景:

- 1.1 $I(A) \rightarrow B:A$
- 1.2 $B \rightarrow I(A):N_b$
 - 2.1 $E \rightarrow I(B):E$
 - 2.2 $I(B) \rightarrow E:N_b$
 - 2.3 $E \rightarrow I(B):\{N_b\}k_{es}$
 - 3.1 $D \rightarrow I(E):D$
 - 3.2 $I(E) \rightarrow D:E, \{N_b\}k_{es}$
 - 3.3 $D \rightarrow I(E):\{E, \{N_b\}k_{es}\}k_{ds}$
 - 4.1 $I(D) \rightarrow S:\{E, \{N_b\}k_{es}\}k_{ds}$
 - 4.2 $S \rightarrow I(D):\{N_b\}k_{ds}$
 - 5.1 $C \rightarrow I(D):C$
 - 5.2 $I(D) \rightarrow C:D, \{N_b\}k_{ds}$
 - 5.3 $C \rightarrow I(D):\{D, \{N_b\}k_{ds}\}k_{cs}$
 - 5.4 $I(C) \rightarrow S:\{D, \{N_b\}k_{ds}\}k_{cs}$
 - 5.5 $S \rightarrow I(C):\{N_b\}k_{cs}$
 - 6.1 $A \rightarrow I(B):A$
 - 6.2 $I(B) \rightarrow A:C, \{N_b\}k_{cs}$
 - 6.3 $A \rightarrow I(B):\{C, \{N_b\}k_{cs}\}k_{as}$
 - 7.1 $I(C) \rightarrow S:\{C, \{N_b\}k_{cs}\}k_{as}$
 - 7.2 $S \rightarrow I(A):\{N_b\}k_{as}$
 - 1.3 $I(A) \rightarrow B:A, \{N_b\}k_{as}$
 - 1.4 $B \rightarrow S:\{A, \{N_b\}k_{as}\}k_{bs}$
 - 1.5 $S \rightarrow B:\{N_b\}k_{bs}$

4) 攻击 4 的攻击场景:

- 1.1 $I(A) \rightarrow B:A$
- 1.2 $B \rightarrow I(A):N_b$
- 1.3 $I(A) \rightarrow B:A, X$
- 1.4 $B \rightarrow S:\{A, X\}k_{bs}$
 - 2.1 $C \rightarrow I(D):C$
 - 2.2 $I(D) \rightarrow C:N_b$
 - 2.3 $C \rightarrow I(D):\{N_b\}k_{cs}$
 - 3.1 $C \rightarrow I(B):C$
 - 3.2 $I(B) \rightarrow C:C, \{N_b\}k_{cs}$
 - 3.3 $C \rightarrow I(B):\{C, \{N_b\}k_{cs}\}k_{cs}$

- 4.1 $B \rightarrow I(C):B$
- 4.2 $I(C) \rightarrow B:C, \{C, \{N_b\}k_{cs}\}k_{cs}$
- 4.3 $B \rightarrow I(C):\{C, \{C, \{N_b\}k_{cs}\}k_{cs}\}k_{bs}$
- 4.4 $I(B) \rightarrow S:\{C, \{C, \{N_b\}k_{cs}\}k_{cs}\}k_{bs}$
- 4.5 $S \rightarrow I(B):\{C, \{N_b\}k_{cs}\}k_{bs}$
 - 5.4 $I(B) \rightarrow S:\{C, \{N_b\}k_{cs}\}k_{bs}$
 - 5.5 $S \rightarrow I(B):\{N_b\}k_{bs}$
- 1.5 $I(S) \rightarrow B:\{N_b\}k_{bs}$

其中攻击 1、2、4 与文献[6] 中是一致的,而攻击 3 是一个新的攻击路径。

3 结语

通过对 Woo-Lam 协议的具体分析,基于关联规则能够很好地分析基于重放攻击的攻击行为,在检验过程中,能通过使用关联规则统一推导出现有的已知攻击,并能发现新的攻击(如攻击 3)。从以上推导过程中可以看出,存在许多向外扩张的推导步骤,这反映了协议的攻击路径具有无穷性。该协议中规则 5 可使推导更为复杂,而规则 3 和 4 则使推导向更为简单的方向发展,规则 1 和 2 则是攻击者成功攻击必须使用的规则,即是攻击者成功攻击的终点位置。很容易看出,只要用规则 5 往更深方向推导,参与协议的主体无限,则复杂的攻击场景将有无穷多个,其攻击行为的个数也是无限的。

协议的关联性是安全协议的基本特征,开展对协议的关联特性的研究和创新,完善安全协议的关联性理论和基于关联规则的协议验证方法,对提高安全协议的分析能力有重要的作用。

参考文献:

- [1] WOO T, LAM S. A semantic model for authentication protocols [C]// Proceedings of the IEEE CS Symposium on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1993: 178-194.
- [2] HORE C A R. Communicating sequential processes [M]. New Jersey: Prentice-Hall, 1985.
- [3] 丁一强. 基于 CCS 的加密协议分析[J]. 软件学报, 1999, 10(10): 1103-1107.
- [4] 梁坚. 密码协议验证与设计若干关键技术研究[D]. 上海: 上海交通大学电子信息学院, 2001.
- [5] 周宏斌, 黄连生, 桑田. 基于串空间的安全协议形式化验证模型及算法[J]. 计算机研究与发展, 2003, 40(2): 251-256.
- [6] DEBBABI M, MEJRI M, TAWBI N, et al. A new algorithm for the automatic verification of authentication protocols: from specifications to flaws and attack scenarios[EB/OL]. [2007-01-03]. <http://dimacs.rutgers.edu/Workshops/Security/program2/debbabi/index.html>
- [7] HAM L. Comment: multi stage secret sharing based on one-way function[J]. Electronics Letters, 1995, 31(4): 262-263.
- [8] HAM L. Efficient sharing (broadcasting) of multiple secrets[J]. IEE Proceedings of Computers and Digital Techniques, 1995, 142(3): 237-240.
- [9] CHIEN H Y, JAN J K, TSENG Y M. A practical (t, n) multi secret sharing scheme[J]. IEICE Transactions on Fundamentals, 2000, E83-A(12): 2762-2765.
- [10] 庞辽军, 柳毅, 王育民. 一个有效的(t, n) 门限多重秘密共享体制[J]. 电子学报, 2006, 34(4): 587-589.
- [11] 李滨. 基于特殊访问权限的差分秘密共享方案[J]. 四川大学学报: 自然科学版, 2006, 43(1): 78-83.

(上接第 1914 页)

参考文献:

- [1] BLAKEY G R. Safeguarding cryptographic keys[C]// Proceedings of NCC. Montvale: AFIPS Press, 1979, 48: 313-317.
- [2] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 24(11): 612-613.
- [3] HE J, DAWSON E. Multi stage secret sharing based on one way function[J]. Electronics Letters, 1994, 30(19): 1591-1592.
- [4] HE J, DAWSON E. Multi secret sharing scheme based on one way function[J]. Electronics Letters, 1995, 31(2): 93-95.
- [5] HAM L. Comment: multi stage secret sharing based on one-way func-