一个有效的(t, n)门限多重秘密共享体制

庞辽军, 柳 毅, 王育民
(西安电子科技大学综合业务网国家重点实验室, 陕西西安 710071)

摘 要: 针对 Chien-Jan-Tseng体制计算量大以及 Yang-Chang-Hwang体制公开信息量大的不足, 利用双变量单向函数提出了一个新的(t, n)门限多重秘密共享体制. 通过一次秘密共享过程就可以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. 在秘密重构过程中, 每个合作的参与者只需提交一个由秘密份额计算的伪份额, 而不会暴露其秘密份额本身. 本文体制结合了现有体制的优点并避免了它们的缺点, 是一个实用、有效的体制.

关键词: 门限体制; 秘密共享; 多重秘密共享
中图分类号: TN918.4 文献标识码: A 文章编号: 0372-2112 (2006) 04-0587-03

An Efficient (*t*, *n*) Threshold Multi-Secret Sharing Scheme

PANG Liao-jun, LIU Yi, WANG Yu-min
(National Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract With the two-variable one-way function, a novel (t, n) threshold multi-secret sharing scheme was presented to overcome Chien-Jan-Tseng scheme's drawback about a large amount of computation and Yang-Chang-Hwang scheme's drawback about lots of public values. Multiple secrets can be shared in one sharing session, and each participant's secret shadow is as long as each of the shared secrets. In the recovery phase, each cooperative participant only needs to submit a pseudo-shadow instead of his secret shadow, and his secret shadow cannot be disclosed. Integrating the advantages of the existing schemes and avoiding their disadvantages, so this scheme is a practical and efficient secret sharing scheme.

Key words threshold scheme; secret sharing; multi-secret sharing

1 引言

秘密共享是信息安全和数据保密中的重要手段, 它在重要信息和秘密数据的安全保存、传输及合法利用中起着非常关键的作用. 秘密共享的概念最早是由 Shamir[1]和 Blakley[2]于 1979年分别独立地提出. 一个秘密被 n个参与者所共享, 只有 t个或更多的参与者联合可以重构该秘密; 而 t-1个或更少的参与者不能得到该秘密的任何信息. 其缺点是一个秘密被重构后, 秘密分发者必须重新分配各参与者的秘密份额. 后来, He和 Dawson[3,4], 以及 Ham[5,6]等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. 在秘密重构过程中, 合作的参与者只需提交一个由秘密份额计算得到的伪份额而并非提交真正的秘密份额, 一个秘密的重构不会披露各参与者所拥有的秘密份额, 也不会影响其它未重构的秘密的安全性.

Chien等人[7]基于系统分组码 (Systematic block codes)提出另一种 (t, n)门限多秘密共享体制, 本文简称为 Chien-Jan-Tseng体制. 与体制 [3~6]所不同的是, 多个秘密可以在一次秘密重构过程中同时得到. 这个方案有非常重要的应用价值. 当需要共享一个大的秘密时, 直接利用 [1~6]等的体制会导致计算空间过大而引起计算复杂度的变大. 例如, 当所共享的秘密为 k×512比特时, 体制 [1]中的模 p应至少为 k×512比特, k越大, 计算越复杂. 一个好的方法就是先将该秘密分成若干子秘密, 再分别实现对其子秘密的共享. 利用 [1~6]等体制, 秘密的重构需要进行多次计算以便重构各子秘密, 尤其体制 [1, 2]还需要多次分配秘密份额. 而利用体制 [7], 则只需进行一次重构计算, 且合作的各参与者只需呈交一个伪份额, 但是在重构秘密时, 需要进行解方程组的运算, 因而效率不高. 最近, Yang等人[8]基于 Shamir的秘密共享体制给出了另一个实现, 本文简称为 Yang-Chang-Hwang体制, 其秘密的重构计算要比体制 [7]简单, 因为构造 Lagrange插值多项式比解方程组容易[8]. 但是当共享的秘密数 m < t时, 体制 [8]要比体制 [7]需要公布的信息多, 这是体制 [8]的不足之处. 因为公共信息量的大小是决定一个体制性能的重要参数, 影响着体制中的存储和通信的复杂度[9].

笔者基于 Shamir的秘密共享体制[1], 提出一个新的

收稿日期: 2004-04-29; 修回日期: 2006-01-29
基金项目: 国家 973基础研究发展规划重大项目 (No. G 1999035805)

(t, n)门限多重秘密共享体制, 其秘密的重构计算和 Yang-Chang-Hwang体制一样简单, 而所需公布的公共信息量与 Chien-Jan-Tseng体制相同. 本文体制结合了这两种体制的优点, 同时避免了他们的缺点, 因此, 本文体制更为实用和有效.

2 本文提出的新体制

在描述本文方案之前, 首先给出一个双变量单向函数 f(r, s)的定义.

定义 1[7] 双变量单向函数. f(r, s)表示一个有两个变量的单向函数, 能够将任意长的 r 和 s映射为固定长的函数值 f(r, s).

该函数具有一些性质: (1)已知 r 和 s, f(r, s)易于计算; (2)已知 s和 f(r, s), 求 r在计算上是不可行的; (3)在 s未知的情况下, 对于任意的 r, 难以计算 f(r, s); (4)已知 s 的情况下, 找到不同的 r_1 和 r_2 满足 $f(r_1, s) = f(r_2, s)$是不可行的; (5)已知 r和 f(r, s), 求 s在计算上是不可行的; (6)已知任意多的 $(r_i, f(r_i, s))$对, 求 $f(r', s)$是不可行的, 其中 $r' \neq r_i$.

下面给出本文提出的新体制, 包括以下三部分: 系统参数、秘密分发和秘密重构算法.

(1)系统参数: f(r, s)为一个双变量单向函数; q 为一个大素数; 系统工作在有限域 GF(q)上, 系统中所有的参数都是 GF(q)中的元素; 可信的秘密分发者随机选择 n 个整数 $s_1, s_2, \cdots, s_n$ 分别作为 n 个参与者的秘密份额, 并选取 n个不同的随机数 $u_1, u_2, \cdots, u_n$ 分别作为 n 个参与者的公开身份信息.

(2)秘密分发: 假设 $C_1, C_2, \cdots, C_m$ 表示 m 个秘密, 可信的秘密分发者执行以下步骤来完成秘密的分发.

(a)随机选取一个整数 r, 对所有的 s_i (i = 1, 2, …, n) 计算 $f(r, s_i)$;

(b)根据数值对 $(0, C_1)$, $(1, C_2)$, …, $(m-1, C_m)$以及 $(u_i, f(r, s_i))$ (i = 1, 2, …, n)构造 (n + m - 1)次多项式 $h(x) = a_0 + a_1 x + \cdots + a_{n+m-1}x^{n+m-1}$;

(c)从集合 $[m, q-1] - \{u_i \mid i = 1, 2, \cdots, n\}$中取出最小的 n + m - t 个整数 $d_1, d_2, \cdots, d_{n+m-t}$, 并分别计算函数值 $h(d_i)$ (i = 1, 2, …, n + m - t);

(d)以认证的方式[10,11] 公布 $(r, h(d_1), h(d_2), \cdots, h(d_{n+m-t}))$.

(3)秘密重构: 为了重构这 m 个秘密, 至少需要 t 个参与者合作. 不失一般性, 我们选取 t个参与者 $u_1, u_2, \cdots, u_t$ 为例来说明秘密重构过程. 首先, 每个参与者 u_i (i = 1, 2, …, t)需要呈交他的伪份额 $f(r, s_i)$. 有了这 t个伪份额, 可以构成 t 个数值对 $(u_i, f(r, s_i))$ (i = 1, 2, …, t). 这时, 再从集合 $[m, q-1] - \{u_i \mid i = 1, 2, \cdots, n\}$中取出最小的 n + m - t 个整数 $d_1, d_2, \cdots, d_{n+m-t}$, 并利用所公布的信息 $h(d_1)$, $h(d_2)$, …, $h(d_{n+m-t})$, 构成 n + m - t 个数值对 $(d_i, h(d_i))$ (i = 1, 2, …, n + m - t). 如果用 (X_i, Y_i) (i = 1, 2, …, n + m) 分别表示所得到的这 (n + m)个数值对, 就可以将所重构的 (n + m - 1)次 Lagrange插值多项式 h(x)表示如下:

$$h(x) = \sum_{i=1}^{n+m} Y_i \prod_{j=1, j\neq i}^{n+m} \frac{x - X_j}{X_i - X_j} = a_0 + a_1 x + \cdots + a_{n+m-1}x^{n+m-1} \quad (1)$$

这时, m 个秘密 $C_1, C_2, \cdots, C_m$ 就可以得到了, 其中 $C_i = h(i-1)$ (i = 1, 2, …, m).

3 分析和讨论

3.1 骗子的揭发

在秘密共享体制中, 如何发现存在欺骗以及指出骗子非常重要[12]. 在本文方案中, 为了防止内部用户或外部攻击者进行欺骗, 即用假的伪份额来欺骗合法的用户, 秘密分发者可以在秘密分发过程中, 利用一个强的密码杂凑函数[4]对秘密分发算法中的第 a 步得到的每个信息 $f(r, s_i)$ (i = 1, 2, …, n)计算一个杂凑值, 并将其以认证的方式[10,11]进行公布. 如果用 H 表示杂凑函数, $f(r, s_i)$的杂凑值为 $H(f(r, s_i))$. 这样, 在秘密重构过程中, 任何人都可以验证每个合作的参与者是否正确的给出其伪份额. 由杂凑函数的性质可知, 要找到一个 $f'(r, s) \neq f(r, s)$, 使得 $H(f'(r, s)) = H(f(r, s))$是计算上不可行的. 这样就可以防止欺骗并指出骗子.

3.2 安全性分析

本文体制的安全性可以从以下方面分析:

(1)尽管公布了 h(x)的 n + m - t个函数值 $h(d_i)$ (i = 1, 2, …, n + m - t), 但是攻击者不会得到 h(x), 因此就得不到秘密的任何信息. 这是因为 h(x)的构造至少需要 n + m 个不同的数值对.

(2)如果少于 t个参与者进行秘密的重构计算, 他们仍然不能构造出多项式 h(x), 原因同 (1). 而当 t个或 t个以上的参与者合作, 它们能够确定唯一的多项式 h(x). 因此, 本文所提出的体制是一个(t, n)门限秘密共享体制.

(3)秘密的重构过程不会披露各参与者的秘密份额. 即使 n 个伪份额 $f(r, s_i)$被披露, 由双变量单向函数 f(r, s)的性质可知, 任何参与者的秘密份额 s_i 都不会被披露. 而且每一次秘密重构过程都不会影响下一次秘密共享所对应的伪份额的安全性. 因此, 在下一次共享过程中, 秘密分发者不需要重新分配秘密份额 s_i, 只需重新选取一个随机整数 r.

通过以上分析, 本文体制具有和 Chien-Jan-Tseng体制以及 Yang-Chang-Hwang体制相同的优点: (1)允许并行的恢复多个秘密, 可以一次性共享 m ($m \geqslant 1$)个秘密; (2)秘密的分发者可以动态的决定本次所要共享的秘密的数量; (3)可以多次用来进行秘密共享而不必重新分配各参与者的秘密份额.

3.3 三种体制的比较分析

下面, 我们分别从秘密重构的计算复杂度和需要公布

的公共信息量来对 Chien-Jan-Tseng 体制、Yang-Chang-Hwang体制以及本文所提出的体制作以比较.

从秘密重构的计算复杂度来看, 本文体制和 Yang-Chang-Hwang体制具有同样的复杂度, 都是通过构造 Lagrange插值多项式完成的. 而在 Chien-Jan-Tseng体制中, 秘密的重构是通过解 n + m - t 元方程组来完成的. 因此, 本文体制和 Yang-Chang-Hwang体制的秘密重构计算的复杂度比 Chien-Jan-Tseng体制的小, 这是因为构造 Lagrange 插值多项式要比解方程组容易得多[8].

从需要公布的公共信息量来看, 本文体制和 Chien-Jan-Tseng体制比 Yang-Chang-Hwang体制更优越. 下面的表 1给出了三种体制所需的公共信息量.

表 1　三种体制所需的信息量比较

体制 / 信息量 / 条件	Chien-Jan-Tseng 体制	Yang-Chang-Hwang 体制	本文体制
m ⩾ t	n + m - t + 1	n + m - t + 1	n + m - t + 1
m < t	n + m - t + 1	n + 1	n + m - t + 1

由表 1可知, 当 m < t时, 本文体制和 Chien-Jan-Tseng 体制需要公布的信息量小于 Yang-Chang-Hwang体制需要公布的信息量. 尤其当 m = 1和 t = n 时, 本文体制和 Chien-Jan-Tseng体制只需要公布 2个公共信息, 而 Yang-Chang-Hwang体制仍需要公布 n + 1个信息.

通过以上分析发现: Chien-Jan-Tseng体制的优点是需要公布的信息量小, 而缺点是秘密重构的计算复杂度大; Yang-Chang-Hwang体制的优点是秘密重构的计算复杂度小, 而缺点是需要公布的信息量大, 而且需要区分两种不同的情况并给以不同的实现. 本文体制正好综合了这两个体制的优点, 避免了它们的缺点, 因而是一种非常有效的秘密共享体制.

4　结论

基于 Shamir的秘密共享体制, 提出了一种 (t, n)门限多重秘密共享体制, m (m ⩾1)个秘密被 n 个参与者所共享, 至少 t个参与者联合可一次性的重构这m 个秘密, 而少于 t个参与者合作得不到秘密的任何信息. 参与者的秘密份额长度等于共享的任一个秘密的长度, 而且不必更新参与者的秘密份额就可以实现多次的秘密共享过程. 分析发现, 本文体制结合了现有体制的优点, 并避免了它们的缺点, 是一个安全、有效的 (t, n)门限多重秘密共享体制.

参考文献:

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

[2] G Blakley. Safeguarding cryptographic keys[A]. In Proc AFIPS 1979 National Computer Conference[C]. New York: AFIPS Press, 1979. 313-317.

[3] J He, E Dawson. Multistage secret sharing based on one-way function[J]. Electronics Letters, 1994, 30(19): 1591-1592.

[4] J He, E Dawson. Multisecret-sharing scheme based on one-way function[J]. Electronics Letters, 1995, 31(2): 93-95.

[5] L Harn. Comment multistage secret sharing based on one-way function[J]. Electronics Letters, 1995, 31(4): 262.

[6] L Harn. Efficient sharing (broadcasting) of multiple secrets[J]. IEE Proceedings Computers and Digital Techniques, 1995, 142(3): 237-240.

[7] H Y Chien, J K Jan, Y M Tseng. A practical (t, n) multisecret sharing scheme[J]. IEICE Transactions on Fundamentals, 2000, E83-A (12): 2762-2765.

[8] Yang ChouChen, Chang TingYi, Hwang MinShiang. A (t, n) multisecret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490.

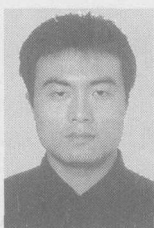
[9] Giovanni Di Crescenzo. Sharing one secret vs sharing many secrets: Tight Bounds on the average improvement ratio[J]. Theoretical Computer Science, 2003, 295(1-3): 123-140.

[10] T ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[11] R L Rivest, A Shamir, L Adleman. A method for obtaining digital signatures and public key cryptosystems[J]. Communication of the ACM, 1978, 21(2): 120-126.

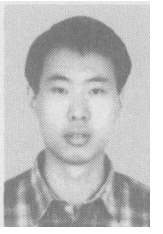
[12] K J Tan, H W Zhu, S J Gu. Cheater identification in (t, n) threshold scheme[J]. Computer Communications, 1999, 22(8): 762-765.

作者简介:



庞辽军　男, 1978年 7月出生于陕西省渭南市, 博士生, 主要研究方向为密码学、电子商务中的安全理论与技术.

E-mail: pangliaojun_ x@ etang. com



柳　毅　男, 1976年 11月生于河北省邯郸市, 博士生, 主要研究方向是信息安全、移动代理.