门限多重秘密共享方案

许春香,肖国镇
(西安电子科技大学计算机网络与信息安全教育部重点实验室,西安 710071)

摘 要: 本文提出了一个门限多重秘密共享方案,其安全性依赖于 RSA 数字签名的安全性,即大数分解的困难性. 该方案具有如下特点:参与者的子秘密可反复使用,可用来共享任意多个秘密;能有效预防管理员欺诈及参与者之间的互相欺骗;此外,在验证是否有欺诈行为存在的过程中,不需要执行交互协议.

关键词: 秘密共享; 门限方案; 多重秘密共享; RSA 数字签名
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2004) 10-1688-02

A Threshold Multiple Secret Sharing Scheme

XU Chun-xiang, XIAO Guo-zhen
(Key Laboratory of Computer Network & Information security, Ministry of Education, Xidian University, Xi'an, 710071, China)

Abstract: A threshold multiple secret sharing scheme is proposed. Its security is based on the security of RSA signature. i. e. the difficulty of factoring large integers. This scheme has the following characteristics: The shares can be repeatedly used for the reconstruction of multiple secrets. The cheating of dealer and the cheating between participants can be detected. In addition, the interactive protocol is not required while detecting the cheaters.

Key words: secret sharing; threshold scheme; multiple secret sharing; RSA signature

1 引言

秘密共享方案是在 N 个参与者中共享秘密 k 的方法. 基于一般访问结构 Γ(访问结构 Γ是由 N 个参与者集合中的一些子集组成,这些子集是能够重构秘密 k 的子集,我们称之为授权子集, Γ为授权子集的集合)的秘密共享方案的原理:首先将秘密 k 分成 N 个子秘密分别给予 N 个参与者,使得(1)访问结构 Γ的授权子集中的参与者联合能够恢复秘密 k;(2)非授权子集中的参与者联合不能得到秘密 k 的任何信息. (t, N)门限秘密共享方案是基于门限访问结构上的秘密共享方案,门限访问结构中的授权子集为 t 个或 t 个以上的参与者集合,即 t 个或 t 个以上的参与者将他们的子秘密放在一起,能够恢复出共享秘密 k,而少于 t 个参与者将他们的子秘密放在一起不能得到有关秘密 k 的任何信息. 门限秘密共享方案自 1979 年由 Shamir[1]提出以后,由于有着广泛的实际应用前景,许多学者投入了很大精力对其本身及相关问题进行深入的研究,并取得了一批研究成果[2~10].

针对 Shamir 门限方案在实际应用中可能存在的管理员 Dealer 欺诈及不良参与者的欺骗问题,文献[2~7]提出了相关的解决方案,即所谓的防欺诈秘密共享方案. 不管是一般的秘密共享方案还是相对安全的防欺诈的秘密共享方案,均存在参与者的子秘密只能使用一次的问题. 对于门限方案,当 N 个参与者中 t 个或 t 个以上参与者出示各自子秘密恢复共享秘密 k 时,所有的秘密信息均已公开,因此 Dealer 只能重新选择新的秘密 k,重新为每个参与者分配新的子秘密. 1992 年 Harn 和 Lin[8]提出了针对一般访问结构的 l-重秘密共享方案,各参与者的子秘密可以重复使用 l 次,分别恢复 l 个共享秘密. l 是由 Dealer 预先设定的固定数,一旦 l 个共享秘密被暴露,Dealer 必须重新分配子秘密. 而 Harn 在 1995 年提出的方案[9]是建立在门限方案的基础之上,克服了上述缺点,参与者可以用同一个子秘密共享任意多个秘密,子秘密可使用任意多次,此方案的安全性是基于离散对数的难解性. 但该方案为防止 Dealer 欺诈,每个参与者需要执行 C_N^t 模指数运算的验证公式,计算量非常大. 同时为了防止参与者之间的相互欺诈,需要执行一个交互式验证协议. Chen 等人提出的方案[10]对上述缺陷作了改进,但在该方案中,对每一个共享秘密,Dealer 除了要计算针对共享秘密的一个模指数外,还需要重新利用各参与者的子秘密计算一个验证向量,向量的每一个分量都是模指数运算,因而 Dealer 计算量很大.

本文提出了一个基于 RSA 数字签名的 (t, N) 多重秘密共享方案,其安全性依赖于 RSA 数字签名的安全性,即大数分解的困难性,参与者的子秘密可反复使用,可用来共享任意多个秘密,同时能有效预防 Dealer 欺诈及参与者之间的互相欺骗,对于每一个共享秘密,Dealer 计算量小,每次只需计算一

收稿日期:2003-01-15;修回日期:2004-06-10
基金项目:国家自然科学基金重大项目(No. 90104005);973 项目(No. G1999035804);陕西省自然科学基金(2003F06)

次模指数运算.此外,在验证是否有欺诈行为存在的过程中,不需要执行交互协议.

2　方案构成

设 $P=\{P_1, P_2, \cdots, P_N\}$ 是 N 个参与者的集合,$[n]=\{1, 2, \cdots, n\}$,其中 n 为正整数.该方案需要一个公告牌(Notice-board),只有 Dealer 可以修改、更新公告牌上的内容,其他人只能阅读或下载.

2.1　Dealer 做如下工作

(1)选取安全大素数 p、q,计算 $n=pq$;

(2)选择 e,使 $\gcd(e, \phi(n))=1$,求 d,使其满足 $ed=1 \bmod \phi(n)$,其中 $\phi(n)$ 为欧拉函数;

(3)选择单向函数 $H(\cdot)$,使其值域 $H(\cdot) \in [n^{\delta_1}]$,其中 $0 \leq \delta_1 \leq 1$ 为安全参数[11];

(4)选择样本消息 $\omega \in Z_n^*$;

(5)随机构造 $t-1$ 次多项式

$$f(x)=d+a_1 x+a_2 x^2+\cdots+a_{t-1} x^{t-1}$$

其中 $a_1, a_2, \cdots, a_{t-1} \in Z_{\phi(n)}$,计算 $d_i=f(i) \bmod \phi(n)$,$W_t=\omega^{d_i} \bmod n$,$i=1,2,\cdots,N$,Dealer 将 d_i 秘密发送给 P_i,并在公告牌上公布 $W_1, W_2, \cdots, W_N, \omega^d, \omega^{a_1}, \omega^{a_2}, \cdots, \omega^{a_{t-1}}$ 及 ω,每个 P_i 通过下式验证 d_i 的正确性.

$$\omega^{d_i}=\omega^d \cdot (\omega^{a_1})^i \cdot (\omega^{a_2})^{i^2} \cdots (\omega^{a_{t-1}})^{i^{t-1}} \bmod n,\ i=1,2,\cdots,N$$

若上式成立,则 P_i 接受 d_i 为子秘密,否则拒绝 d_i.

d, d_i 保密,p、q 不再有用,予以销毁.

2.2　秘密生成

设 $K=\{K_1, K_2, \cdots, K_r\}$ 为 N 个参与者集合 $P=\{P_1, P_2, \cdots, P_N\}$ 共享的秘密集,Dealer 随机选择 $m_1, m_2, \cdots, m_r \in Z_n^*$,其中 m_j 与 K_j 对应.为了使 n 个参与者 $P_1, P_2, \cdots, P_N$ 中任意 t 个能够重构密钥 K_j,Dealer 计算

$$T_j=K_j-m_j^{ld}$$

其中 $l=N!$,并在公告牌上公布 T_j, m_j.

2.3　秘密的恢复

不失一般性,假设参与者集合 $A=\{P_1, P_2, \cdots, P_t\}$ 准备重构共享密钥 K_j.首先 A 中每个参与者 P_i 计算:

$$S_{ij}=m_j^{d_i} \bmod n \quad i=1,2,\cdots,t$$

然后选取 $c_{ij} \in [n^{1+\delta_1+\delta_2}]$,其中 δ_1,δ_2 为安全参数,且 $0 \leq \delta_1$, $\delta_2 \leq 1$[11],计算 $\omega'=\omega^{c_{ij}}$, $m'=m_j^{c_{ij}}$, $b_{ij}=H(\omega, m_j, S_{ij}, W_i, \omega', m')$,在整数环 Z 上计算 $y_{ij}=c_{ij}+b_{ij}d_i$. $P_i(i=1,2,\cdots,t)$ 公布验证值:$\{y_{ij}, b_{ij}\}$,并将 $\{m_j, S_{ij}\}$ 发送给指定生成者 DC(Desig-nated Combiner),DC 可以是 A 中的某一个参与者也可以是其他的某个人.为了验证 P_i 提供的 S_{ij} 的正确性,任何人只需验证下式是否成立.

$$b_{ij}=H(\omega, m_j, S_{ij}, W_i, \omega^{y_{ij}} W_i^{-b_{ij}}, m_j^{y_{ij}} S_{ij}^{-b_{ij}})$$

若上式成立,则 P_i 提供的 $\{m_j, S_{ij}\}$ 是正确的.

取 $l=N!$,在整数环 Z 上计算

$$\beta_i=\frac{1}{\prod_{\substack{j=1 \\ j\neq i}}^{t}(i-j)} \cdot \prod_{\substack{j=1 \\ j\neq i}}^{t}(-j)$$

$$\alpha_i=\beta_i$$

由于 $\prod_{\substack{j=1 \\ j\neq i}}^{t}(i-j) \mid l$,所以 α_i 在整数环 Z 上是可计算的.

DC 通过下列计算可重构 K_j.

$$m_j^{ld}=S_j=\prod_{i=1}^{t} S_{ij}^{\alpha_i} \bmod n \qquad (1)$$

从而 $K_j=T_j-m_j^{ld} \bmod n$, $j=1,2,\cdots,r$.如果 D 想让 N 个参与者 $P_1, P_2, \cdots, P_N$ 共享新的秘密 K_{r+1},只需在公告牌上公布随机选取的 m_{r+1} 及 $T_{r+1}=k_{r+1}-m_{r+1}^{ld}$ 之值即可达到目的.

下面证明式(1)成立.

证明:$S_j=\prod_{i=1}^{t} S_{ij}^{\alpha_i}=\prod_{i=1}^{t} m_j^{\alpha_i d_i}=m_j^{\sum_{i=1}^{t}\alpha_i d_i}=m_j^{\sum_{i=1}^{t}\beta_i d_i}=m_j^{ld} \bmod n$.

3　安全性分析

本文提出的门限多重秘密共享方案的安全性是基于 RSA 数字签名和门限方案的安全性.

(1)从 ω^d, $\omega^{d_i}(i=1,2,\cdots,N)$, $\omega^{a_j}(j=1,2,\cdots,t-1)$ 不能求出 d, $d_i(i=1,2,\cdots,N)$, $a_j(j=1,2,\cdots,t-1)$.实际上,值 ω^d, ω^{d_i}, ω^{a_j} 相当于对样本消息 ω 的 RSA 数字签名.

(2)少于 t 个参与者不能从 T_j, m_j 之值得到 K_j.为了计算 K_j,根据 $T_j=K_j-m_j^{ld}$,必须先求出 m_j^{ld},而由门限秘密共享方案可知,只有 t 个或 t 个以上的参与者联合才能计算出 m_j^{ld},因而当且仅当 t 个或 t 个以上的参与者联合才能重构秘密 K_j.

(3)任何人不能从公布的 $\{y_{ij}, b_{ij}\}$ 得到 d_i 值.因为方程 $y_{ij}=c_{ij}+b_{ij}d_i$ 中含有两个未知数 c_{ij} 和 d_i,所以不可能求得 d_i.如果还有另外一对 $\{y'_{ij}, b'_{ij}\}$ 值满足 $y'_{ij}=c'_{ij}+b'_{ij}d_i$,虽然增加了一个方程,但又增加了一个未知数 c'_{ij},总之未知数的个数总比方程的个数多一个,因此 d_i 是安全的.

4　结束语

本文在门限秘密共享和 RSA 数字签名的基础之上,提出了门限多重秘密共享方案.在该方案中,参与者的子秘密可反复使用,能预防各种可能出现的欺诈,管理者计算开销小.该方案克服了已有方案的缺陷,具有更广泛的适用性.

作者简介:

许春香　女,1965 年 1 月生于湖南宁乡,博士,教授,现任教于电子科技大学计算机学院,主要研究方向为信息安全和密码学. E-mail:chxxu@mail.xidian.edu.cn

肖国镇　男,教授,博士生导师,主要研究方向为密码学和编码学.

(下转第 1687 页)

沌系统的量化函数.

5 结论

采用 KMM 序列对分段线性混沌系统实施扰动得到改进型分段线性混沌序列.这类序列能够克服因有限精度效应引起的短周期行为,在适当的初值条件下具有周期长、平衡性好、自相关函数较尖锐、互相关较小以及线性复杂度理想等直扩码特性.量化函数对这类序列的平衡性几乎无影响;由二进制取值法映射所得序列的自相关和互相关特性略优于不可逆映射法;两种量化函数对序列的线性复杂度影响相同.然而,不可逆映射法的算法较复杂,硬件实现复杂度较大.由于数字混沌序列发生器电路本身就是直接对二进制数进行处理,所以二进制取值法十分易于硬件实现.二进制取值法是一种比不可逆映射法更适合应用于改进型分段线性混沌系统的量化函数.改进型分段线性混沌序列是一类有潜力的、适合用作 DS-CDMA 系统直扩码的 PN 序列.

参考文献:

[1] M B Pursley, H F A Roefs. Numerical evaluation of correlation parameters for optimal phases of binary shift-register sequences [J]. IEEE Trans on COM, 1979, 27(10): 1597 - 1604.

[2] R A Scholtz, L R Welch. GMW sequences [J]. IEEE Trans On IT, 1984, 30(3): 548 - 553.

[3] Xu Duan Lin, Kyung Hi Chang. Optimal PN sequence design for quasisynchronous CDMA communication systems [J]. IEEE Trans on COM, 1997, 45(2): 221 - 226.

[4] D Sandoval-Morantes, D Munoz-Rodriguez. Chaotic sequences for multiple access [J]. Electronics Letters, 1998, 34(3): 235 - 237.

[5] Tohur Kohda, Akio Tsuneda. Pseudonoise sequences by chaotic nonlinear maps and their correlation properties [A]. IEICE Trans Commun [C]. 1993, E97～B(8): 855 - 862.

[6] Gianluca Mazzini, Gianluca Setti, Riccardo Rovatti. Chaotic complex spreading sequences for asynchronous DS-CDMA [J]. IEEE Trans On-CAS, 1997, 44(10): 937 - 947.

[7] Ghobad Heidari-Bateni, Clare D McGillem. A chaotic direct-sequence-spread-spectrum communication system [J]. IEEE Trans on COM., 1994, 42(2/3/4): 1524 - 1527.

[8] 胡健栋,郑朝辉,龙必起,李兴明. 码分多址与个人通信[M]. 北京:人民邮电出版社, 1996: 90 - 155.

[9] 周红等. 有限精度混沌系统的 m 序列扰动实现[J]. 电子学报. 1997, 25(7): 95 - 97.

[10] 桑涛,王汝笠. 一类新型混沌反馈序列的理论设计[J]. 电子学报, 1999, 27(7): 47 - 50.

[11] 饶妮妮,龚耀寰. KMM 序列伪随机特性分析[J]. 电子科技大学学报, 1994, 23(4): 363 - 369.

作者简介:

饶妮妮　女,1963 年生于四川宜宾,籍贯重庆,教授、博士生导师,1997 年 9 月至 1998 年 9 月和 2003 年 11 月至 2004 年 2 月在英国作学术访问,在国内外核心刊物、国际国内学术会议上发表涉及生物信息学、生物医学工程、移动通信和教学研究的论文 30 多篇,现在的研究兴趣包括:移动通信、信号/图像处理、生物医学信息学.

(上接第 1689 页)

参考文献:

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

[2] H.-Y. Lin, Harn L. A generalized secret sharing scheme with cheater detection [A]. Advances in Cryptology-ASIACRYPT '91 Proceedings [C], Berlin: Springer-Verlag, 1993. 149 - 158.

[3] M Carpentieri. A perfect threshold secret sharing scheme to identify cheaters [J]. Designs, Codes and Cryptography, 1995, 5(3): 183 - 197.

[4] J Rifa-Coma. How to avoid the cheaters succeeding in the key sharing scheme [J]. Designs, Codes and cryptography, 1993, 3(3): 221 - 228.

[5] C Padró, G Sáez. Detection of cheaters in vector space secret sharing schemes [J]. Designs, Codes and Cryptography, 1999, 16(1): 75 - 85.

[6] 张建中,肖国镇. 可防止欺诈的秘密共享方案. 通信学报, 2000, 21(5): 81 - 83.

[7] E F Brickell, D R Stinson. The detection of cheaters in threshold scheme [A]. Advances in Cryptology-CRYPTO '88 [C], Berlin: Springer-Verlag, 1988. 564 - 577.

[8] L Harn, H Lin. An l-span generalized secret sharing scheme [A]. Advances in Cryptology-CRYPTO '92 [C]. Berlin: Springer-Verlag, 1992. 558 - 565.

[9] L Harn. Efficient sharing (Broadcasting) of multiple secrets, IEE Proc.-Comput. Digit. Tech. 1995, 142(3): 237 - 240.

[10] L Chen, D Gollmann, C J Mitchell, P Wild. Secret sharing with reusable polynomials [A]. The Second Australasian Conference on Information Security and Privacy-ACISP '97 [C]. Berlin: Springer-Verlag, 1997. 183 - 192.

[11] GENNARO R., JARECKI S., KRAWCZYK H. et al. Robust and efficient sharing of RSA functions [A]. Advanced in Cryptology-- CRYPTO '96 Proceedings [C]. Berlin: Springer Verlag, 1996. 157 - 172.