基于 LUC 密码体制的(t,n)门限秘密共享方案

庞辽军, 王育民
(西安电子科技大学 综合业务网理论与关键技术国家重点实验室,陕西 西安 710071)

摘要:基于 LUC 密码体制提出了一个(t,n)门限秘密共享方案,使用参与者的私钥作为他们的秘密份额,秘密分发者不需要进行秘密份额的分配. 秘密份额的长度小于或等于秘密的长度. 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,且任何人都能够立即检验每个合作的参与者是否进行了欺骗. 该方案可用来共享任意多个秘密,而不必修改各参与者的秘密份额. 方案的安全性是基于 LUC 密码体制和 Shamir 的(t,n)门限方案的安全性.

关键词:秘密共享;门限方案;LUC 密码体制
中图分类号:TP918 **文献标识码**:A **文章编号**:1001-2400(2005)06-0927-04

A (t,n) secret sharing scheme based on the LUC cryptosystem

PANG Liao-jun, *WANG Yu-min*
(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: A (t,n) threshold secret sharing scheme based on the LUC cryptosystem was proposed. In the new scheme, each participant's private-key is used as his secret share and the secret dealer does not have to distribute each participant's secret share. All these shares are shorter than or as short as the shared secret. In the recovery phase, each cooperative participant only needs to submit a pseudo-share instead of his secret share and anyone is allowed to check whether a cooperative participant provides the true information or not immediately. The secret shares do not need to be changed when sharing multiple secrets. The security of this scheme is the same as that of the LUC cryptosystem and Shamir's (t,n) threshold secret sharing scheme.

Key Words: secret sharing; threshold scheme; LUC cryptosystem

第一个秘密共享方案是(t,n)门限共享方案,由 Shamir[1] 和 Blakley[2] 在 1979 年分别基于 Lagrange 插值法和多维空间点的性质提出的. 现有大多数秘密共享方案,如文[1~5]等,具有一些共同点:一是各参与者的秘密份额都是由秘密分发者产生,秘密分发者掌握着所有参与者的秘密份额. 这使得秘密分发者需要保存大量的秘密信息,而且会成为攻击者所攻击的目标;二是在秘密分发者和各参与者之间需要一条安全信道,利用该信道进行秘密份额的分发,但是维护一条安全信道会提高系统的代价和复杂度. 而且在许多秘密共享方案中,为了能够检验在秘密重构过程中合作的参与者是否进行欺骗,秘密分发者需要专门构造一个验证算法和一些验证信息[6]. 这必然会增加系统的复杂度,并影响秘密分发的效率. 这些特点或多或少会影响秘密共享方案的实际应用,比如,当参与者和秘密分发者之间不可能存在安全信道时,这些方案也将不再有用.

笔者基于 LUC 密码体制[7] 提出了一个(t,n)门限秘密共享方案,它使用参与者的私钥作为他们的秘密份额,秘密分发者和各参与者之间可以以明文形式相互通信,不需要维护安全信道. 秘密份额的长度小于或等于秘密的长度. 在秘密重构过程中,每个合作的参考者只需提交一个由秘密份额计算的伪份额,而且不需要设计专门的验证算法就可立即判断每个合作的参与者是否进行了欺骗. 由于在秘密重构过程中,每个参与者只需提交一个由秘密份额计算的伪份额,而不必暴露他的秘密份额,因此,该方案可用来共享任意多个秘

收稿日期:2004-11-25
基金项目:973 国家重大项目资助(G1999035804);"十五"国家部委预研资助项目(Y1010122)
作者简介:庞辽军(1978-),男,西安电子科技大学博士研究生.

密,而不必修改参与者的秘密份额. 方案的安全性是基于所使用的 LUC 密码体制和 Shamir 的 (t,n) 门限方案的安全性.

1 LUC 秘密体制简介

LUC 是新西兰学者 P. Smith 等[7]提出的双钥密码体制,它采用 Lucas 数列来实现消息的加密和解密.

1.1 Lucas 数列

Lucas 数列可定义为:

定义 1 选两个非负整数 P 和 Q,构成二次式 $x^2 - Px + Q = 0$,其根为

$$\alpha,\beta = (P \pm D^{1/2})/2 \quad , \tag{1}$$

其中 D 是方程的判别式,即 $D = P^2 - 4Q$. 如果选 P 和 Q,使 $D \neq 0$,则 Lucas 数列可定义为

$$U_n(P,Q) = (\alpha^n - \beta^n)/(\alpha - \beta) \quad , \quad n \geqslant 0 \quad , \tag{2}$$

$$V_n(P,Q) = \alpha^n + \beta^n \quad , \quad n \geqslant 0 \quad . \tag{3}$$

LUC 公钥体制仅对 $V_n(P,Q)$ 序列感兴趣[7],这里仅给出本文中所用到的性质:

性质 1 设 a,b 为任意正整数,则有 $V_{ab}(P,1) = V_a(V_b(P,1),1)$.

性质 2 设 a,b 为任意正整数,则有 $V_b(V_a(P,1),1) = V_a(V_b(P,1),1)$.

证明 由性质 1 可得到, $V_b(V_a(P,1),1) = V_{ba}(P,1) = V_{ab}(P,1) = V_a(V_b(P,1),1)$.

1.2 LUC 密码体制

令 $N = pq$,为两个奇素数之积;选一个整数 e,使 $(e,\phi(N)) = 1$,这里 $\phi(N)$ 是欧拉函数;并由式 $ed \equiv 1 \bmod \phi(N)$ 确定出另一整数 d. 构造 LUC 体制表示如下:

公钥:N,e;私钥:d(陷门信息 p,q);明文:P 为小于 N 的某个整数;加密:$C = V_e(P,1) \bmod N$;解密:$P = V_d(C,1) \bmod N$.

2 本文中提出的新方案

2.1 系统成员及主要参数

系统成员:包括可信的秘密分发者 d(dealer)和 n 个参与者(participant)$P_1,P_2,\cdots,P_n$.

系统参数:令 $N = pq$,为两个足够大的奇素数之积;系统中每个参与者的 LUC 公钥和私钥分别为 $\{N,e_i\}$ 和 d_i;秘密分发者的 LUC 公钥和私钥分别为 $\{N,e_d\}$ 和 d_d;令 Q 是一个随机选取的且大于 N 的素数;一个公告牌(Noticeboard),只有秘密分发者可修改、更新公告牌上的内容,其他人只能阅读或下载;秘密分发者随机地从 $[n-t+2,Q-1]$ 中选取 n 个不同的整数 $x_1,x_2,\cdots,x_n$ 分别作为参与者 $P_1,P_2,\cdots,P_n$ 的公开身份标识,并以每个参与者的私钥作为其秘密份额.

2.2 秘密分发算法

为了在 n 个参与者 $P_1,P_2,\cdots,P_n$ 中共享秘密 $s \in Z_Q$,使得至少 t 个参与者合作才可重构该秘密,秘密分发者可执行如下算法:

D.1 从 $[N^{1/2},N-1]$ 中随机选取一个整数 r.

D.2 对于每一个参与者 $P_i(i = 1,2,\cdots,n)$,秘密分发者与其进行以下交互过程:

D.2.1 将 r 送给参与者 P_i;

D.2.2 参与者 P_i 利用自己的私钥对 r 进行解密(或签名),即计算 $V_{d_i}(r,1) \bmod N$,并将结果送给秘密分发者;

D.2.3 秘密分发者可利用 P_i 的公钥来验证 $V_{d_i}(r,1) \bmod N$ 的正确性,即验证 $r = V_{e_i}(V_{d_i}(r,1),1) \bmod N$ 是否成立. 如果不成立,说明参与者 P_i 没有诚实地给出自己计算的 $V_{d_i}(r,1) \bmod N$,或者可能消息在传送过程中出错. 这时,秘密分发者可向 P_i 发送一个抱怨信息,并要求其进行重发,直到验证通过,或者进行

其他相应的出错处理. 如果$r = V_{e_i}(V_{d_i}(r,1),1) \bmod N$成立,秘密分发者利用自己的私钥对$V_{d_i}(r,1) \bmod N$进行解密,得到$V_{d_d}(V_{d_i}(r,1),1) \bmod N$.

D.3　利用$(n+1)$个点$(0,s),(x_1, V_{d_d}(V_{d_1}(r,1),1) \bmod N),(x_2, V_{d_d}(V_{d_2}(r,1),1) \bmod N),\cdots,(x_n, V_{d_d}(V_{d_n}(r,1),1) \bmod N)$和 Lagrange 插值方法[1]构造$n$阶多项式$f(x)$:

$$f(x) = s \times \prod_{k=1}^{n} (x - x_k)/(-x_k) + \sum_{l=1}^{n} \left[(V_{d_d}(V_{d_l}(r,1),1) \bmod N) \times \right.$$

$$\left. (x/x_l) \times \prod_{k=1,k\neq l}^{n} (x - x_k)/(x_l - x_k) \right] \bmod Q \quad . \tag{4}$$

D.4　分别计算$f(1),f(2),\cdots,f(n-t+1)$.

D.5　在公告牌上公开关于秘密s的信息:$\mathrm{Msg}(s) = (r, V_{d_d}(r,1) \bmod N, f(1), f(2),\cdots, f(n-t+1))$.

2.3　秘密重构算法

为了重构秘密s,需要至少t个参与者合作. 不失一般性,假设t个参与者$P_1,P_2,\cdots,P_t$准备重构秘密s. 注意每一个参与者不需要提供他的秘密份额,即他的私钥,而仅仅需要提供一个由秘密份额计算的伪份额. 而且,在这个过程中,任何人都可立即检验各参与秘密重构的合作者是否诚实地提供自己正确的份额. 下面,给出参与者$P_1,P_2,\cdots,P_t$如何重构秘密s:

R.1　每个合作的参与者P_i从公告牌上读取关于共享秘密s的公开信息$\mathrm{Msg}(s)$.

R.2　每个合作的参与者P_i利用自己的私钥计算关于秘密s的伪份额$V_{d_i}(V_{d_d}(r,1),1) \bmod N$,并将其提交给指定的秘密计算者. 秘密计算者可通过验证$V_{d_d}(r,1) = V_{e_i}(V_{d_i}(V_{d_d}(r,1),1),1) \bmod N$是否成立来验证参与者$P_i$所提交的伪份额. 如果成立,那么,$P_i$所提交的伪份额是正确的,接着执行下面的第(R.3)步;否则,P_i没有诚实地给出自己的伪份额,或者可能消息在传送过程中出错,这时,秘密计算者可向P_i发送一个抱怨信息,并要求其进行重发,直到验证通过,或者进行其他相应的出错处理.

R.3　由性质 2 可知,$V_{d_i}(V_{d_d}(r,1),1) = V_{d_d}(V_{d_i}(r,1),1)$. 这样就可得到$t$个点$(x_1, V_{d_d}(V_{d_1}(r,1),1) \bmod N),(x_2, V_{d_d}(V_{d_2}(r,1),1) \bmod N),\cdots,(x_t, V_{d_d}(V_{d_t}(r,1),1) \bmod N)$,再利用公开的信息$\mathrm{Msg}(s)$可得到另外的$(n-t+1)$个点$(1,f(1)),(2,f(2)),\cdots,(n-t+1,f(n-t+1))$. 通过汇集这$(n+1)$个秘密点,采用 Lagrange 内插多项式[1]即可重构多项式$f(x)$. 为简单起见,如果用$(X_i,Y_i)\ i = 1,2,\cdots,n+1$来表示所得到的$(n+1)$个数值对,就可以如下方法重构$n$次 Lagrange 插值多项式$f(x)$:

$$f(x) = \sum_{i=1}^{n+1} Y_i \prod_{j=1,j\neq i}^{n+1} ((x - X_j)/(X_i - X_j)) \bmod Q \quad . \tag{5}$$

R.4　恢复所共享的秘密$s = f(0)$.

3　安全性分析与讨论

本文中提出的(t,n)门限秘密共享方案的安全性是基于 LUC 公钥系统和 Shamir 的门限方案的安全性.

(1) 所提出的方案利用了 LUC 密码体制的性质,以参与者的私钥作为秘密份额,这样秘密分发者不需与各参与者进行秘密通信即可使一群参与者共享任意的秘密s. 秘密分发者和各参与者之间的所有通信可以以明文形式进行,因此,该方案对于秘密分发者与参与者之间不存在安全通信信道的场合尤为有用.

(2) 如果某个参与者P_i想进行欺骗,他可在秘密分发过程的第(D.2.2)步计算$V_{d_i}(r,1) \bmod N$时,或在秘密重构过程的第(R.2)步计算伪份额$V_{d_i}(V_{d_d}(r,1),1) \bmod N$时进行欺骗. 但是,由于$r$和$V_{d_d}(r,1)$都是已知的信息,任何人都可利用$P_i$的公钥进行验证,发现这种欺骗.

(3) 系统外的攻击者可通过设法推导出各参与者的私钥来对本方案进行攻击. 他可在秘密分发过程的第(D.2.2)步中,或在秘密重构过程的第(R.2)步中,根据各参与者P_i提交的信息$V_{d_i}(r) \bmod N$或$V_{d_i}(V_{d_d}(r,1),1) \bmod N$来推导出参与者$P_i$的私钥,即参与者$P_i$的秘密份额. 由于 LUC 密码体制的安全性,攻击者的这种攻击无法奏效. 同样道理,攻击者通过推导秘密分发者的私钥以进行模仿秘密分发者的攻击也是不可能的.

(4) 由 Lagrange 内插多项式的性质[1]可知,只有t个或t个以上的参与者合作才可重构多项式$f(x)$,从而

恢复秘密 s ;而不超过 $(t-1)$ 个参与者的合作无法重构多项式 $f(x)$,从而无法获得秘密 s 的任何信息. 因此,本文中所提的方案体现了 (t,n) 门限秘密共享方案的原则. 攻击者即使与 $(t-1)$ 个参与者串通,由他们所计算的关于秘密 s 的 $(t-1)$ 个伪份额及公开信息也无法得到其他任何一个参与者的份额. 由 $(t-1)$ 个份额恢复秘密 s 相当于在 Z_Q 中随机猜测 s 获得成功,其概率仅为 $1/Q$. 因为方案中 Q 是足够大的数,因此,这种攻击成功的概率几乎为 0.

(5) 该方案也是一个多秘密共享方案[8] ,可使一群参与者利用他们各自的私钥共享任意多个秘密而不必更新他们的私钥. 为了共享多个秘密 $s_1,s_2,\cdots,s_k \in Z_Q$,秘密分发者在进行秘密分发时,只需在秘密分发过程的第(D. 1) 步为每个秘密 $s_i(i=1,2,\cdots,k)$ 随机选取一个惟一的整数 r_i. 由 LUC 密码体制的安全性可知,在秘密的分发和重构过程中,每个参与者 P_i 的私钥不会被其他参与者或系统外的任何人计算出来. 而且,即使知道某个参与者 P_i 关于若干个秘密的伪份额,也不可能计算出他的关于其他秘密的伪份额. 这也是本文方案的一个优点,即秘密分发者可动态地在 n 个参与者中共享任意秘密.

(6) 值得注意的是,尽管 LUC 和 RSA[9] 通常是可替换的[7] ,但在本文的方案中不可使用 RSA 来替换 LUC,这种替换会导致方案安全性的降低. 这是因为在 RSA 体制中,数字签字的乘积是相应消息之积的数字签字,这使得 RSA 会受到公共模以及称之为自适应选择消息伪造的密码攻击[7] ;而 LUC 不具有这样的乘积性质,因而不受这些攻击[7] . 这也从另一个侧面显示了本文方案的安全性.

4 结 束 语

基于 LUC 密码体制提出了一个 (t,n) 门限秘密共享方案,其中参与者的秘密份额不是由秘密分发者决定,而是使用他们的私钥作为秘密份额,即使秘密分发者也不能获得每个参与者的秘密份额 ;秘密分发者和各参与者间所有的消息都可以以明文形式发送,不需要在他们之间维护一条安全信道,这对于秘密分发者与参与者之间不存在安全通信信道的场合尤为有用 ;秘密重构过程中,任何人可立即检验每个合作的参与者是否进行了欺骗. 利用该方案可共享任意多个秘密,而不必修改参与者的秘密份额. 方案的安全性是基于 LUC 密码体制和 Shamir 的 (t,n) 门限方案的安全性.

参考文献:

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

[2] Blakley G. Safeguarding Cryptographic Keys[A]. Proc AFIPS 1979 Natl Conf[C]. New York:AFIPS Press, 1979. 313-317.

[3] Chien H Y, Jan J K, Tseng Y M. A Practical (t,n) Multi-secret Sharing Scheme[J]. IEICE Trans on Fundametals, 2000, E83-A(12):2762-2765.

[4] Xu Chunxiang, Fu xiaotong, Xiao Guozhen. A Vector Space Secret Sharing Scheme Against Cheating[J]. Journal of Xidian University, 2002, 29(4):527-529.

[5] Yang C C, Chang T Y, Hwang M S. A (t,n) Multi-secret Sharing Scheme[J]. Applied Mathematics and Computation, 2004, 151(2):483-490.

[6] Tan K J, Zhu H W, Gu S J. Cheater Identification in (t,n) Threshold Scheme[J]. Computer Communications, 1999, 22(8):762-765.

[7] Smith P. LUC Public-key Encryption:a Secure Alternative to RSA[J]. Dr Dobb's Journal, 1993, 18(1):44-49.

[8] Harn L. Efficient Sharing(Broadcasting) of Multiple Secrets[J]. IEE Proceedings—Computers and Digital Techniques, 1995, 142(3):237-240.

[9] Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public Key Cryptosystem[J]. Communication of ACM, 1978, 21(2):120-126.

(编辑:李维东)