基于LUC密码体制防欺诈的秘密共享方案

庞辽军[1]，李慧贤[2]，王育民[1]

(1. 西安电子科技大学综合业务网国家重点实验室 西安 710071; 2. 西北工业大学计算机学院 西安 710072)

【摘要】基于LUC密码体制，提出一种防欺诈的(t，n)门限秘密共享方案。在秘密恢复过程中，任何参与者能够对其他参与者所出示的子秘密进行验证，不仅能有效地阻止敌手窃取秘密，也能有效地防止内部成员之间的相互欺骗；各参与者的子秘密长度与秘密长度相同，方案的信息率为1，是一个理想的方案。该方案的安全性是基于LUC密码体制和Shamir的(t，n)门限秘密共享方案的安全性。

关 键 词 密码学; 信息安全; 秘密共享; 门限方案
中图分类号 TP309 文献标识码 A

A Secret Sharing Scheme with Ability to Identify Cheaters Based on LUC Cryptosystem

PANG Liao-jun[1]，LI Hui-xian[2]，WANG Yu-min[1]

(1. National Key Lab. of Integrated Service Networks, Xidian Univ. Xi'an 710071;
2. School of Comput. Sci., Northwestern Polytechnical Univ. Xi'an 710072)

Abstract Secret sharing plays an important role in information security and data privacy. Based on LUC cryptosystem, a (t, n) threshold secret sharing scheme is proposed in this paper, which has the capability to identify cheater. In the secret recovery phase, each participant is allowed to check whether another participant provides the true share or not, which can prevent adversaries from getting the secret and the participants cheating each other efficiently. Each participant's share is as short as the shared secret. Therefore, this scheme is an ideal one with the information rate 1. The security of this scheme is based on that of the LUC cryptosystem and Shamir's (t, n) threshold secret sharing scheme.

Key words cryptography; information security; secret sharing; threshold scheme

秘密共享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。文献[1]和[2]分别独立地提出了最初的秘密共享门限方案。自从秘密共享概念被提出后，许多研究人员对秘密共享进行了研究，并取得大量的成果[3]。目前，秘密共享方案已被广泛应用于通信密钥的管理、数据安全、银行网络管理、导弹控制发射等方面。

秘密共享方案在实际使用时，一方面必须防止外部欺诈，即防止敌手获得秘密s；另一方面要防止内部欺诈，即防止子秘密合法拥有者出示伪子秘密和非法窃取秘密s。有各种可防止欺诈的(t, n)门限秘密共享方案[4-7]。信息率是秘密共享方案的一个重要的性能指标。经过分析发现，在文献[4]的方案中，尽管能以一定的概率发现欺骗者，但其信息率较低，仅为$1/(3n-2)$；在文献[5-6]的方案中，信息率较文献[4]的方案有了很大的提高，前者为$1/(t+2n-2)$，后者为$\log_2 q/(\log_2 q + \log_2 n)$。尽管文献[6]的方案的信息率相对较高，但是易受公共模攻击而泄漏部分秘密[7]；文献[8]的方案主要是通过定期更新各参与者的子秘密预防欺诈，计算量大且同样易受到公共模攻击[7]。

本文基于文献[9]提出的LUC密码体制，提出了可以防止欺诈的(t, n)门限秘密共享方案。该方案的主要特点是安全性强，具有很强的防止欺诈的能力，且各参与者的子秘密长度与秘密长度相同。

1 LUC密码体制简介

LUC是双钥密码体制，该密码体制是采用Lucas数列来实现消息的加密和解密，本文拟对其作一简单的介绍。

1.1 Lucas数列

Lucas数列可以定义为，选两个非负整数P和Q，构成二次式$x^2-Px+Q=0$，其根为α、β，且：

收稿日期：2005 - 03 - 28
基金项目：国家973计划资助项目(G1999035804)；军事通信技术预研项目
作者简介：庞辽军(1978 –)，男，博士，主要从事电子商务安全理论与技术方面的研究.

$$\alpha,\beta=\frac{P\pm\sqrt{D}}{2} \tag{1}$$

式中 D是方程的判别式，即$D=P^2-4Q$。如果选P和Q，使$D\neq0$，则Lucas数列可定义为：

$$U_n(P,Q)=\frac{\alpha^n-\beta^n}{\alpha-\beta}\quad n\geq0 \tag{2}$$

$$V_n(P,Q)=\alpha^n+\beta^n\qquad n\geq0 \tag{3}$$

LUC公钥体制仅对$V_n(P,Q)$序列感兴趣。有关$V_n(P,Q)$的性质及证明可以参见文献[8-9]，这里仅给出本文所用到的性质。

性质 1　$V_n(P \bmod N, Q \bmod N)=V_n(P, Q) \bmod N$。

性质 2　设a，b为任意正整数，则有$V_{ab}(P,1)=V_a(V_b(P, 1), 1)$。

性质1和性质2的证明可参见文献[8-9]。

性质 3　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2可以得到$V_b(V_a(P,1),1)=V_{ba}(P,1)=V_{ab}(P,1)=V_a(V_b(P,1),1)$。证毕。

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$(e, \phi(N))=1$，其中$\phi(N)$是欧拉函数；并由$ed\equiv1 \bmod \phi(N)$确定出另一整数d。构造LUC体制可以简单地表示如下：

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；密文$C=V_e(P, 1) \bmod N$；解密$P=V_d(C, 1) \bmod N$。

有关LUC密码体制的正确性、安全性的证明，以及密钥的选取，可参见文献[9]，本文不再赘述。

2 本文提出的新方案

基于LUC密码体制防欺诈的秘密共享方案需要一个公告牌(Noticeboard)，只有秘密分发者可以修改、更新公告牌上的内容，其他人只能阅读或下载。

2.1 系统参数的建立

设$P=\{P_1, P_2,\cdots, P_n\}$是$n$个参与者的集合；$Q$为一个随机选取的大素数，其取值应大于所要共享的秘密。秘密分发者随机从$GF(Q)$中选取n个不同的整数$u_1, u_2,\cdots, u_n$分别标识这n个参与者的公开身份。此外，秘密分发者还需要计算两套LUC公私钥$\{N, e_1\}$和d_1，$\{N, e_2\}$和d_2，将私钥d_1和d_2保密并将公钥$\{N, e_1\}$和$\{N, e_2\}$向系统中所有成员公开。

最后，秘密分发者应该将所有的公开信息在公告牌上进行公布，如N，Q, $u_1, u_2, \cdots, u_n$, $\{N, e_1\}$和$\{N, e_2\}$等。由于素数p和q不再有用，予以销毁。

2.2 秘密的分发

为了在n个参与者$P_1, P_2, \cdots, P_n$中共享秘密$s\in G_F(Q)$，秘密分发者可以执行如下算法。

1) 构造一个$(t-1)$次多项式，即：

$$f(x)=s+a_1x+\cdots+a_{t-1}x^{t-1} \bmod Q \tag{4}$$

式中 $a_1, a_2, \cdots, a_{t-1}$均随机从$GF(Q)$选取，且满足$a_{t-1}\neq0$。

2) 对于$I_i=1, 2, \cdots, n$，重复以下步骤，即：

(1) 计算用于秘密重构的子秘密$S_i=f(u_i)$；

(2) 计算$W_i=V_{e_2}(V_{d_1}(S_i,1),1) \bmod N$。

3) 子秘密S_i被安全地送给参与者P_i，并且由参与者P_i安全保存，将信息W_i在公告牌上公布。S_i和W_i分别为用于秘密重构的子秘密和用于防止欺诈的验证信息。

2.3 秘密的重构过程

为了重构秘密s，需要至少t个参与者合作。为不失一般性，假设t个参与者$P_1, P_2, \cdots, P_t$准备重构秘密s。下面，给出参与者$P_1, P_2, \cdots, P_t$如何重构秘密s的步骤。

(1) 合作的参与者P_i将其子秘密S_i提交给指定的秘密计算者DC(Designated Combiner)。秘密计算者可以通过验证$V_{e_1}(W_i,1)=V_{e_2}(S_i,1) \bmod N$是否成立来验证参与者$P_i$所提交的子秘密是否真实。$W_i$可以从公告牌上获得，如果$V_{e_1}(W_i,1)=V_{e_2}(S_i,1) \bmod N$成立，则$P_i$所提交的子秘密$S_i$是正确的，可执行步骤(2)；如果$P_i$没有诚实地给出自己的份额，或者消息在传送过程中出错，秘密计算者可以向P_i发送一个抱怨信息，并要求其重发，直到验证通过，或者进行其他相应的出错处理。

(2) 利用所得到的t个子秘密可以构成t个插值点$(u_1, S_1), (u_2, S_2), \cdots, (u_t, S_t)$，进而使用Lagrange插值算法重构$(t-1)$次多项式：

$$f(x)=\sum_{i=1}^{t}S_i\prod_{j=1,j\neq i}^{t}\frac{x-u_j}{u_i-u_j} \bmod Q \tag{5}$$

(3) 恢复所共享的秘密$s=f(0)$。

3 分析和讨论

3.1 验证欺诈行为

在秘密共享方案中，如何发现存在欺骗以及指出骗子非常重要。基于LUC密码体制防欺诈的秘密共享方案中，秘密重构过程的步骤(1)止给出了能有效地检测出内部欺诈和外部欺诈的方法。下面给出一个定理来说明该方法的有效性。

定理 1　假设在秘密重构过程的步骤(1)中，某

合作的参与者P_i提供了子份额S_i。如果$V_{e_1}(W_i,1)=V_{e_2}(S_i,1) \bmod N$，则$S_i$是正确的；否则，$S_i$是错误的，$P_i$可能是骗子。

证明 由性质1和3可知，$V_{e_1}(W_i,1)=V_{e_1}(V_{e_2}(V_{d_1}(S_i,1),1),1)=V_{e_1}(V_{d_1}(V_{d_2}(S_i,1),1),1) \bmod N$。再由LUC公钥体制的加解密性质可知，$V_{e_1}(W_i,1)=V_{e_2}(S_i,1) \bmod N$。因此，如果$P_i$不是骗子，则$V_{e_1}(W_i,1)=V_{e_2}(S_i,1) \bmod N$应该成立。而且，由LUC密码体制的安全性可知，在不知道秘密分发者私钥的情况下，要找到一个$S_i' \neq S_i$并满足验证方程在计算上是不可行的。

3.2 安全性分析

基于LUC密码体制防欺诈的秘密共享方案的安全性是基于Shamir门限方案和LUC密码系统的安全性的。首先，在该方案中，秘密份额的计算和秘密的重构采用了基于Lagrange插值的Shamir秘密共享方案[1]。从Shamir方案的原理可知，本文方案中的秘密分发和秘密重构算法也是正确的。对于一个(t, n)门限秘密共享方案来说，一个最基本的要求就是$(t-1)$个或更少的参与者的合作不能重构共享的秘密。由于重构$(t-1)$阶多项式$f(x)$需要知道t个满足$Y_i=f(X_i)$的点(X_i, Y_i)，而$(t-1)$个或更少的参与者的合作最多只能得到$(t-1)$个这样的点，利用$(t-1)$个或更少个点重构n阶多项式$f(x)$等价于成功地攻破Shamir的(t, n)门限方案。因此，$(t-1)$个或更少的参与者的合作不能正确地重构n阶多项式$f(x)$，换句话说，就是不能恢复共享的秘密s。可见，本文所提出方案是完善的，符合(t, n)门限方案的规则和要求。其次，在秘密重构的过程中，任何参与者能够对其他参与者出示的子秘密进行验证，可以防止外部非合法参与者欺骗合法参与者，并防止内部合法参与者提供虚假信息欺骗其他合法参与者。

下面给出一个定理来说明在基于LUC密码体制防欺诈的秘密共享方案中，除非攻破LUC密码体制，否则，欺诈者的攻击不可能成功。

定理 2 在基于LUC密码体制防欺诈的秘密共享方案中，欺诈者成功欺诈的难度等价于成功地攻破LUC密码体制的难度。

证明 一个欺诈者可以是内部欺诈者，也可以是外部欺诈者。对于外部欺诈者来说，该欺诈者可以在秘密重构过程中提供伪造的信息S_i'来进行欺骗；对于内部欺诈者，该欺诈者可以将其要提供的信息S_i改为任意的S_i'来欺骗其他参与者。从本文的方案可知，为了不被检验出来，欺诈者提供的信息S_i'必须满足$V_{e_1}(W_i,1)=V_{e_2}(S_i',1) \bmod N$。$W_i$可以从公告牌上获得，但是，由于欺诈者不知道秘密分发者的私钥，所以在已知W_i的条件下来计算满足$V_{e_1}(W_i,1)=V_{e_2}(S_i',1) \bmod N$的$S_i'$同样等价于攻破LUC密码体制。除非攻破LUC密码体制，否则，这种攻击无法奏效。证毕。

3.3 方案的信息率

信息率定义为共享的秘密长度与最小子秘密长度之比。在基于LUC密码体制防欺诈的秘密共享方案中，秘密的空间与子秘密的空间相同，记为Q。考虑均匀分布和等长编码情况，信息熵$H(Q)=\log_2 q$。因此，本文方案的信息率为$\log_2 q/\log_2 q=1$。很明显，基于LUC密码体制防欺诈的秘密共享方案是一个理想的方案，比起本文中所提到的其他方案，其信息率更高。

3.4 安全性说明

值得注意的是，尽管LUC和RSA[10]通常是可替换的[9]，但是在本文的方案中不可以使用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，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[9]；而LUC不具有这样的乘积性质，因而不受这些攻击[9]。这也从另一个侧面显示了本文方案的安全性。

4 结 论

在基于LUC密码体制防欺诈的秘密共享方案的秘密恢复过程中，任何参与者都能够对其他参与者所出示的子秘密进行验证，不仅能有效地阻止敌手窃取秘密，也能有效地防止内部成员之间的相互欺骗。此外，各参与者的子秘密长度与秘密长度相同，因而基于LUC密码体制防欺诈的秘密共享方案是一个理想的方案，比本文所提到的其他方案具有更高的信息率。方案的安全性是基于LUC密码体制和Shamir的(t, n)门限秘密共享方案的安全性，只要LUC密码体制和Shamir的(t, n)门限秘密共享方案具有足够强的安全性，基于LUC密码体制防欺诈的秘密共享方案就具有很强的防欺诈和防攻击能力。

参 考 文 献

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

[2] BLAKLEY G. Safeguarding cryptographic keys[C]// In: Proc. AFIPS 1979 Natl. Conf., New York, 1979: 313-317.

[3] YANG C C, CHNAG T Y, HWANG M S. A (t, n) multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490.

[4] RABIN T, BEN-Or M. Verifiable secrets sharing and multiparty protocols with honest majority[C]// In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing, New York, 1989: 73-85.
[5] 张建中, 肖国镇. 一个可防止欺诈的秘密分享方案[J]. 电子科学学刊, 1999, 21(4): 516-521.
[6] 费如纯, 王丽娜. 基于RSA和单向函数防欺诈的秘密共享体制[J]. 软件学报, 2003, 14(1): 146-150.
[7] 王育民, 刘建伟. 通信网的安全—理论与技术[M]. 西安: 西安电子科技大学出版社, 1999.
[8] 许春香, 魏仕民, 肖国镇. 定期更新防欺诈的秘密共享方案[J]. 计算机学报, 2002, 25(6): 657-660.
[9] SMITH P. LUC public-key encryption: A secure alternative to RSA[J]. Dr. Dobb's Journal, 1993, 18(1): 44-49.
[10] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public key cryptosystem[J]. Communication of the ACM, 1978, 21(2): 120–126.

编　辑　熊思亮

(上接第71页)

测量玻璃培养皿的厚度时，发现培养皿底表面有很多同心圆纹路且整个面不平整。有机材料的细胞培养皿没有相应的情况而且培养皿底面材料厚度的一致性较好。

表**2**　有机材料培养皿介电常数测试结果

f_0/GHz	t /mm	f_s /GHz	空载 Q 值 ($\times10^{-3}$)	载样 Q 值 ($\times10^{-3}$)	ε_r	$\tan\delta$
34.412	0.98	34.211	11.36	8.105	3.07	0.001 8
34.412	1.00	34.210	11.28	8.362	3.09	0.001 6
34.412	1.00	34.210	11.47	8.553	3.11	0.001 6
36.399	0.98	36.159	12.05	9.051	3.01	0.001 5
36.399	1.00	36.160	12.13	9.040	2.99	0.001 5
36.399	1.00	36.160	11.94	8.760	2.97	0.001 6

4　结　论

本文建立的单层平面材料介电常数扫频测试系统为毫米波生物效应相关实验的电磁剂量学研究奠定了基础。通过对有机材料和玻璃制作的两类培养皿在8 mm波段的两个频率点上进行介电常数测试后，结果表明有机材料制作的细胞培养皿具有底部表面平整、光洁度好、材料对毫米波的损耗小的特点。因此，在做细胞层次上的毫米波生物效应研究时，有机材料的细胞培养皿比玻璃的细胞培养皿更适合被用于对细胞进行毫米波辐照。

参　考　文　献

[1] PAKHOMOV A G, AKYEL Y, PAKHOMOVA O N, et al. Current state and implications of research on biological effects of millimeter waves:a review of the literature[J]. Bioelectromagnetics, 1998, 19(7): 393-413.
[2] 廖小丽. 毫米波生物效应的水分子谐振机理[J]. 电子科技大学学报. 2002, 31(1): 80-83.
[3] ZHAO J X, LI J X. Algorithm analysis of electromagnetic wave power density measurement for millimeter-wave irradiators in bioelectromagnetic experiments[J]. Int.J. IR & MMW, 2003, 24(6): 909-928.
[4] 赵建勋, 牛中奇, 鲁德强. 辐照到培皿中细胞单层上的毫米波功率密度分析[J]. 生物医学工程学杂志, 2004, 21(1): 97-101.
[5] HIRVONEN T M, VAINIKAINNN P, LOZOWSKI A, R, et al. Measurement of dielectrics at 100 GHz with an open resonator connected to a network analyzer[J]. IEEE Trans.Instrum. Meas, 1996, 45(8): 780-786.
[6] 高源慈, 余国芬, 孙嘉鸿. 准光腔品质因数的标网测量与研究[J]. 强激光与粒子束, 2004, 16(4): 517-520.
[7] AFSSR, DING Han-yi. A novel open-resonator system for precise measurement of permittivity and loss-tangent[J]. IEEE Trans. Instrum. Meas., 2001, 50(2): 402-405.

编　辑　孙晓丹