DOI: 10.13718/j.cnki.xdzk.2021.07.014

一个可公开验证的多重秘密共享门限方案

蔡兆政[1,2]，　瞿云云[3]，　包小敏[1]

1. 西南大学 数学与统计学院，重庆 400715；2. 重庆市第十八中学，重庆 400020；
3. 贵州师范大学 数学与计算机科学学院，贵阳 550001

摘要：本文设计了一个安全有效的可公开验证的(t, n)多重秘密共享门限方案. 该方案下的系统需要一个公告牌(bulletin board)，只有秘密分发者(Dealer)可以修改和更新上面的数据，参与者只能下载或浏览. 该方案的特点是，Dealer 分发给参与者加密的秘密份额可以公开被验证，但是只有指定的参与者能够解密得到子秘密，且子秘密可以重复使用；由参与者提供的解密份额也可以公开验证，这两次公开都是非交互的验证，高效便捷，可以有效防止 Dealer 欺骗行为和参与者的欺骗行为. 方案加密采用 ElGamal 公钥密码体制，计算的验证参数可以多次利用，Dealer 要想共享新的秘密，只需要在公告牌上发布新的数据即可，Dealer 的计算量较小，具有广泛的适用性.

关　键　词：秘密共享方案；拉格朗日插值多项式；门限方案；非交互身份认证

中图分类号：O211.4　　**文献标志码**：A　　**文章编号**：1673-9868(2021)07-0105-06

秘密共享的概念最早由文献[1-2]提出. 文献[1]利用拉格朗日插值多项式构造了一个门限秘密共享方案，其主要思想是二维平面内任意 t 个点都可唯一确定一个 $t-1$ 次多项式. 任何 t 个及 t 个以上的参与者联合可以重构多项式，得到的常数项即为分享的秘密. 反之，任何小于 t 个参与者的集合不能重构多项式，从而不能获得秘密. 文献[2]利用线性投影几何原理的性质构造的门限方案，t 个 $t-1$ 维超平面可以确定 t 维空间中一个点，但小于 t 个是无法确定的. 这两个经典的门限秘密共享方案为研究不同访问结构(access structure)上的秘密共享奠定了基础[3]. 文献[4]提出了基于中国剩余定理的门限秘密共享方案，秘密份额是秘密的同余类，满足 t 个同余方程的解在取值范围中是唯一的，少于 t 个方程，解无法确定. 文献[5]利用矩阵乘法构造了一个秘密共享方案，其原理等价于解含有 t 个未知数的线性方程组，每个共享份额相当于一个线性方程，任意大于等于 t 个份额联立可以求得 t 个未知数，而其中的一个未知数恰为分享的秘密，当方程个数小于未知数个数的时候无法确定方程组的解，从而不能恢复共享的秘密. 上述几种构造秘密共享方案的方法是最常用的几种方法，此外，文献[6]中指出，一个 RS 码对应一个秘密共享方案. 文献[7]利用纠错码巧妙构造了一个秘密共享门限方案，该方案是一个$(l, t+l)$门限秘密共享方案，可以共享多个秘密.

任何在实际中应用的密码方案及其算法都应该具有抵抗攻击的能力，Shamir 秘密共享方案[1]和其他秘密共享方案是在秘密分发者和参与者都可信的前提假设下设计的，这样就导致了秘密共享方案在实际应

收稿日期：2019-07-01
基金项目：贵州省教育厅青年科技人才成长项目(黔教合 KY 字[2016]130；贵州省科学技术基金项目(黔科合 J 字[2014]2125 号)；国家自然科学基金项目(61462016).
作者简介：蔡兆政，硕士，主要从事编码理论和密码学的研究.
通信作者：包小敏，博士，教授.

用场景中存在很多安全隐患. 例如内部的参与者为了获得其他参与者的份额而提供假的份额；或者由于受信道中噪音的干扰等导致份额在通信过程中出现错误；又或者外部攻击者冒充授权的参与者进行欺诈；另外，秘密分发者也可能存在欺诈行为. 这些情况都会导致秘密无法重构或者重构的秘密错误. 为了解决这些问题，许多学者提出了可验证的秘密共享方案.

1985年，文献[8]提出了可验证秘密共享(verifiable secret sharing，VSS)的概念，其方法是在通常的秘密共享方案中添加一个验证算法，这样份额持有者就能验证自己的份额与分发者分发的份额是否一致. 验证方式有交互式和非交互式两种. 随后，其他研究者提出了一系列的可验证的秘密共享方案，文献[9]构造了一个非交互式的VSS方案. 在VSS方案的基础之上，文献[10]提出了可公开验证秘密共享(publicly verifiable secret sharing，PVSS)的思想，不仅仅内部参与者可以验证份额的有效性，非参与者也可以验证. 1999年，文献[11]设计了一个更完善的非交互的PVSS方案，方案中有两次非交互验证. 第一次是验证秘密分发者分发的加密的秘密份额，第二次是验证参与者解密后的秘密份额；前者可以预防秘密分发者的欺骗行为和通信中的错误，后者可以防止参与者之间的欺诈行为. 这样确保了秘密份额的有效性，避免了由于份额错误而产生不必要的计算. 本文也采用两次验证的思想.

在秘密共享中另外一个需要着重考虑的问题就是方案的效率，主要考虑数据传输量和计算量. 若秘密分发者和参与者之间使用一次一密的方式共享秘密，虽然安全性得以保证，但是在效率和成本上都有欠缺. 例如在Shamir门限方案中，参与者重构一次秘密之后，若要共享新的秘密，分发者就必须重新设置参数、给参与者分发秘密份额，因为该方案中参与者持有的秘密份额是一次性的，不能重复使用，方案的效率较低.

为了提高秘密共享方案的效率，文献[12-13]提出了一个多阶段秘密共享方案，方案中的每个份额可以使用l次，但是在重构过程中要求参与者提供相应顺序的秘密份额，这在实际的应用有很大的局限性. 随后，文献[14]构造了克服了上述缺点的一个方案，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，但该方案为防止秘密分发者欺诈，每个参与者需要运行多次模指数运算来验证，计算量非常大. 同时为了防止参与者之间的相互欺诈，方案采用交互式验证方式. 针对上述缺陷，文献[15]提出一个新的方案，但在该方案中，对每一个共享秘密，秘密分发者除了要计算秘密份额外，还需要利用各参与者的子秘密计算一个验证向量，而向量的每一个分量都是模指数运算，因而秘密分发者计算压力很大. 文献[16]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，但是该方案需要将子秘密通过秘密信道发送给参与者，在动态秘密共享情形下，秘密共享者的工作量较大，同时维护秘密信道增加了通信开支. 本文提出了一个安全有效的可公开验证的(t, n)多重秘密共享门限方案. 方案加密采用ElGamal公钥密码体制[17]，不需要维护秘密信道而增加通信成本；计算的验证参数可以多次利用，Dealer要想共享新的秘密，只需要在公告牌上发布新的数据即可，Dealer的计算量较小，具有广泛的适用性.

1 基础知识

定义1(拉格朗日插值多项式) 设(x_0, y_0)，(x_1, y_1)，…，(x_{t-1}, y_{t-1})是二维平面上任意给定的t个点的坐标，则有且仅有一个与这t个点的坐标对应的$t-1$次多项式$p(x)$，满足$p(x_i)=y_i$，$0 \leqslant i < t$.

$p(x)$可以通过下面的公式计算得到：

$$p(x)=\sum_{i=0}^{t} p(x_i) \prod_{\substack{j=0 \\ j\neq i}}^{t} \frac{(x-x_j)}{x_i-x_j} \tag{1}$$

身份识别的目的是使某人的身份被确认. 下面介绍Schnorr身份认证方案，该方案需要一个可信第三方发放证书和选择系统参数.

定义 2(Schnorr 身份认证方案)　设 p 是一个大素数，α 是 Z_p^* 中的一个元素，阶 $q>2^t$，t 是安全参数，则对任意的 $\beta\in\langle\alpha\rangle$，有 $0\leqslant\log_\alpha\beta\leqslant q-1$，参数 p,q,α,t 是公开的. 系统中的每个用户选择自己的私钥 a，$0\leqslant a\leqslant q-1$，并计算相应的公钥 $\nu=\alpha^{-a}\bmod p$.

(i) Alice 随机选择一个整数 k，$0\leqslant k\leqslant q-1$，计算 $\gamma=\alpha^k\bmod p$. Alice 传送 $Cret_{\text{Alice}}$ 和 γ 给 Bob.

(ii) Bob 利用证书 $Cret_{\text{Alice}}$ 验证 Alice 的公钥 ν. Bob 随机选择一个整数 r，$1\leqslant r\leqslant 2^t$，并传送 r 给 Alice.

(iii) Alice 计算 $y=k+ar\bmod q$，并传送 y 给 Bob.

(iv) Bob 验证 $y\equiv\alpha^y\nu^r\bmod p$. 如果成立，Bob“接受”；否则，Bob“拒绝”.

下面的同余式成立说明 Alice 能够向 Bob 证明自己的身份

$$\alpha^y\nu^r\equiv\alpha^{k+ar}\nu^r\bmod p\equiv$$
$$\alpha^{k+ar}\alpha^{-ar}\bmod p\equiv$$
$$\alpha^k\bmod p\equiv$$
$$\gamma\bmod p$$

在上述的方案中需要证明者和验证者交互才能证实证明者的身份，显然满足不了本文所构造方案中非交互身份认证的需求，因此建立了一个非交互的身份认证方案.

定义 2(非交互身份认证方案)　设 p 是一个大素数，g_1,g_2 是 Z_p 的两个生成元，$hash()$ 是一个安全的密码学 Hash 函数. 假设某证明者拥有私钥 α，记 $h_1=g_1^\alpha$，$h_2=g_2^\alpha$.

(i) 证明者任选 $w\in_R Z_q$，然后计算 $a_1=g_1^w$，$a_2=g_2^w$，$c=hash(h_1,h_2,a_1,a_2)$，$r=w-c\alpha\bmod q$；

(ii) 证明者用(c,r)应答；

(iii) 验证者计算 $a_1=g_1^rh_1^c$ 和 $a_2=g_2^rh_2^c$，$c'=hash(h_1,h_2,a_1,a_2)$. 检查 $c=c'$ 是否成立.

验证通过，则证明者拥有私钥 α，使得 $h_1=g_1^\alpha$，$h_2=g_2^\alpha$ 成立.

2　方案构成

设 $P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参与者的集合，Dealer 是秘密分发者. 该方案在系统中需要一个公告牌，只有 Dealer 可以修改、更新公告牌上的内容，其他人只能阅读和下载. $hash()$ 是一个安全的密码学 Hash 函数.

方案运行前做以下准备工作，设 g 是 q 阶群 G_q 的生成元，q 是一个素数，使得在 Z_q^* 上的离散对数问题是难解的. 参与者 P_i 选择自己的私钥 $x_i\in_R Z_q^*$（x_i 互不相同），并在系统中注册 $y_i=g^{x_i}\bmod q$ 作为自己的公钥，$i=1,2,\cdots,n$.

2.1　秘密分发阶段

1) 秘密份额分发

(i) Dealer 选择一个 $t-1$ 次的多项式

$$p(x)=\sum_{i=0}^{t-1}\alpha_ix^i\bmod q$$

Dealer 保存 $p(x)$，在公告牌上发布相关系数 $C_i=g^{\alpha_i}\bmod q$，$i=0,1,\cdots,t-1$.

(ii) Dealer 计算份额 $Y_i=y_i^{p(i)}\bmod q$，设 $X_i=\prod_{j=1}^{t-1}C_j^{i^j}\bmod q$. Dealer 要为每一个 $p(i)$ 产生一个承诺，满足 $X_i=g^{p(i)}\bmod q$，$Y_i=y_i^{p(i)}\bmod q$，$i=1,2,\cdots,n$. 承诺中包含挑战 c_i 和应答 r_i 以及子秘密密文 d_i，具体步骤如下：Dealer 选取 $w_i\in_R Z_q$，计算 $a_{1i}=g^{w_i}\bmod q$，$a_{2i}=y_i^{w_i}\bmod q$，$c_i=hash(X_i,Y_i,a_{1i},a_{2i})$，$r_i=(w_i-c_ip(i))\bmod q$，$d_i=p(i)a_{2i}\bmod q$. Dealer 在公告牌上发布 Y_i 及其对应的承诺(c_i,r_i,d_i)，$i=1,2,\cdots,n$.

2) 秘密份额的验证

验证者运行非交互式认证协议. 验证者首先计算 $X_i=\prod_{j=1}^{t-1}C_j^{i^j} \bmod q$, 然后以 $g, X_i, y_i, Y_i, c_i, r_i$ 为输入, 计算 $a_{1i}=g^{r_i}X_i^{c_i} \bmod q$, $a_{2i}=y_i^{r_i}Y_i^{c_i} \bmod q$, 接下来检验 $c_i'=hash(X_i, Y_i, a_{1i}, a_{2i})$ 是否与承诺 c_i 相等. 若相等, 接收; 否则, 拒绝.

2.2 秘密生成阶段

设 $K=\{K_1, K_2, \cdots, K_r\}$ 是共享的秘密集, Dealer随机选取 $m_j \in_R Z_q^*$, $j=1,2,\cdots,r$, 其中 m_j 和 K_j 对应. 为了使 n 个参与者中任意 t 个及 t 个以上的参与者能够重构 K_j, Dealer计算 $T_j=(K_j-m_j^{la_0}) \bmod q$, 其中 $l=n!$. Dealer在公告牌上公布 (T_j, m_j).

2.3 秘密重构阶段

1) 秘密份额解密

不失一般性, 假设一个最小授权子集 $A=\{P_1, P_2, \cdots, P_t\}$. P_i 验证 Y_i 对应的承诺通过之后, 计算 a_{1i} 与 d_i 的乘积即可得到 $p(i)$. 因为 $a_{1i}=g^{w_i} \bmod q$, $d_i=p(i)a_{2i} \bmod q$, $a_{2i}=y_i^{w_i} \bmod q$, $y_i=g^{x_i} \bmod q$, 所以

$$p(i)=a_{1i}^{-x_i}d_i=g^{-w_ix_i}p(i)y_i^{w_i}=p(i)g^{-w_ix_i}g^{w_ix_i} \bmod q$$

然后计算 $S_{ij}=m_j^{p(i)} \bmod q$. 此时有 $g^{p(i)}=X_i \bmod q$, $m_j^{p(i)}=S_{ij} \bmod q$, P_i 对解密得到的 S_{ij} 产生一个承诺, 具体步骤如下: P_i 随机选取 $v_i \in_R Z_q$, 计算 $b_{1i}=g^{v_i} \bmod q$, $a_{2i}=m_j^{v_i} \bmod q$, $e_i=hash(y_i, S_{ij}, b_{1i}, b_{2i})$, $\mu_i=(v_i-e_ip(i)) \bmod q$. P_i 把 (m_j, S_{ij}) 及其对应的承诺 (e_i, μ_i), $i=1,2,\cdots,t$, 发送给指定解密者 B, 解密者可以是系统中的某个参与者, 也可以是其他人.

2) 联合解密

解密者 B 要对收到可行集合 A 中参与者发送的秘密份额进行验证. 首先, 以 $g, X_i, m_j, S_{ij}, e_i, \mu_i$ 为输入, 计算 $b_{1i}=g^{\mu_i}X_i^{e_i} \bmod q$, $b_{2i}=m_j^{\mu_i}S_{ij}^{e_i} \bmod q$, 然后检验 $e_i'=hash(g, S_{ij}, b_{1i}, b_{2i})$ 是否与承诺中的 e_i 相等, $i=1,2,\cdots,t$. 若相等, 接收; 否则, 拒绝并停止解密. 若验证都通过, B 利用收到的解密份额恢复秘密: 取 $l=n!$, 在整数环 Z 上计算拉格朗日系数

$$\lambda_i=\prod_{j\neq i}\frac{j}{j-i}$$

B 可以计算

$$m_j^{la_0}=\prod_{i=1}^{t}S_{ij}^{l\lambda_i}=\prod_{i=1}^{t}m_j^{p(i)l\lambda_i}=m_j^{\sum_{i=1}^{t}p(i)l\lambda_i}=m_j^{l\sum_{i=1}^{t}p(i)\lambda_i}=m_j^{la_0} \bmod q$$

从而 $K_j=(T_j-m_j^{la_0}) \bmod q$, $j=1,2,\cdots,r$. 若Dealer想在参与者集 P 中共享新的秘密 K_{r+1}, 则只需要重新选择 $m_{r+1} \in_R Z_q^*$, 计算 $T_{r+1}=K_{r+1}-m_{r+1}^{la_0}$, 在公告牌上发布 (T_{r+1}, m_{r+1}) 即可.

3 安全性分析

Shamir门限方案共享一次秘密之后就会暴露插值多项式的系数, 因此不能继续使用该多项式共享新的秘密. 若Dealer要共享新的秘密, 则只能重新构造多项式. 一个直观的思想就是隐藏插值多项式的系数, 本方案采用的思想是找一个计算离散对数困难的群 Z_q^*, 计算参数 $C_i=g^{\alpha_i}$, 而攻击者在知道 g 和 C_i 的情况下是无法计算插值系数 α_i 的. 下面通过两个定理来证明本方案是安全的.

定理1 攻击者无法从 Y_i 或 S_{ij} 中计算得到 $p(i)$.

证 在本方案中, $p(i)$ 非常重要, 需要每个参与者秘密保存. $Y_i=g^{p(i)} \bmod q$, $S_{ij}=m_j^{p(i)} \bmod q$, 而在 Z_q^* 中计算离散对数是困难的, 所以攻击者无法从 Y_i 或 S_{ij} 中计算得到 $p(i)$.

定理 2　若参与者数量少于门限值 t 则不能从 T_j, m_j 得到共享秘密 K_j.

证　根据计算公式 $T_j = K_j - m_j^{la_0}$ 可知，若要计算 K_j，则先要计算 $m_j^{la_0}$. 不失一般性，设 $1 \leqslant j \leqslant t-1$

$$\prod_{i=1}^{t-1} S_{ij}^{l\lambda_i} = \prod_{i=1}^{t-1} m_j^{p(i)l\lambda_i} = m_j^{\sum_{i=1}^{t-1} p(i)l\lambda_i} = m_j^{l\sum_{i=1}^{t-1} p(i)\lambda_i}$$

而 $p(i)$ 是一个 $t-1$ 次多项式，需要 t 个点才能确定 $p(i)$，所以若参与者数量少于 t 则无法从 T_j，m_j 得到共享秘密 K_j.

在解密的过程中，没有直接用到 $p(i)$，也无法从解密参数中获取 $p(i)$，可以保证 $p(x)$ 安全，所以可以用设定的参数安全共享多个秘密.

4　结束语

本文构造了一个可公开验证的门限多重秘密共享方案.

该方案基于拉格朗日插值多项式，且采用两次非交互的验证协议，第一次验证是为了防止 Dealer 作弊或信息在传递过程中受到信道中噪音的干扰而出现错误；第二次验证是检测参与解密的参与者提供的秘密份额是否为 Dealer 发送. 只有通过两次验证的秘密份额才能作为重构秘密的份额.

共享多个秘密的思想是将秘密和一个随机参数作二进制加法隐藏起来，只有达到或超过门限值个数的参与者联合才能计算得到这个随机参数. 共享新的秘密只需选择新的参数，因此可以共享任意多个秘密.

本文所构造的方案是将可公开验证和可共享多个秘密这两个优点相结合，是对秘密共享作了进一步研究.

参考文献：

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

[2] BLAKLEYG R. Safeguarding Cryptographic Keys [C] //1979 International Workshop on Managing Requirements Knowledge. New York: IEEE Press, 1979: 313-318.

[3] STINSON D R. Cryptography Theory and Practice [J]. Clinical Nurse Specialist CNS, 1995, 7(3): 177-186.

[4] ASMUTH C, BLOOM J. A Modular Approach to Key Safeguarding [J]. IEEE Transactions on Information Theory, 1983, 29(2): 208-210.

[5] KARNINE, GREENE J, HELLMANM. On Secret Sharing Systems [J]. IEEE Transactions on In formation Theory, 1983, 29(1): 35-41.

[6] MCELIECE R J, SARWATE D V. On Sharing Secrets and Reed-Solomon Codes [J]. Communications of the ACM, 1981, 24(9): 583-584.

[7] OZBEK I, SIAP I. A New Secret Sharing Scheme [J]. Electronic Notes in Discrete Mathematics, 2016, 56: 43-48.

[8] CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults [C] //26th Annual Symposium on Foundations of Computer Science. New York: IEEE Press, 1985: 383-395.

[9] FELDMAN P. A Practical Scheme for Non-Interactive Verifiable Secret Sharing [C] //28th Annual Symposium on Foundations of Computer Science. New York: IEEE Press, 1987: 427-438.

[10] STADLER M. Publicly Verifiable Secret Sharing [M] //Advancesin Cryptology-EUROCRYPT'96. Berlin: Springer, 1996: 190-199.

[11] SCHOENMAKERS B. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting [J]. Lecture Notes in Computer Science, 1999, 1666: 784-784.

[12] HARN L, LIN H Y. An L-Span Generalized Secret Sharing Scheme [M] //Advancesin Cryptology-CRYPTO'92. Berlin: Springer, 1992: 558-565.

[13] HARN L. Comment: Multistage Secret Sharing Based on One-Way Function [J]. Electronics Letters, 1995, 31(4):

262.

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

[15] CHEN L Q, GOLLMANN D, MITCHELL C J, et al. Secret Sharing with Reusable Polynomials [M] //Information Security and Privacy. Berlin: Springer, 1997: 183-193.

[16] 许春香，肖国镇. 门限多重秘密共享方案 [J]. 电子学报，2004，32(10)：1687-1689.

[17] ELGAMAL T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms [C] //Advances in Cryptology. Berlin: Springer, 1985.

A Publicly Verifiable Multiple Secret Sharing Threshold Scheme

CAI Zhao-zheng[1,2], QU Yun-yun[3], BAO Xiao-min[1]

1. *School of Mathematics and Statistics, Southwest University, Chongqing 400715, China;*
2. *Chongqing No. 18 Middle School, Chongqing 400020, China;*
3. *School of Mathematical Science, Guizhou Normal University, Guiyang 550001, China*

Abstract: A secure and effective (t, n) multiple secret sharing threshold scheme is designed in this paper. The system of this scheme requires a bulletin board. Only the Dealer can modify and update the data on it, and the participants can only download or browse it. What is unique for this scheme is that the encrypted secret share distributed by the Dealer to the participants can be verified publicly, but only the designated participant(s) can decrypt the sub-secret and the sub-secret can be re-used. The declassified share provided by the participants can also be verified publicly. Both disclosures are non-interactive verification, which are efficient and convenient and can effectively prevent the Dealer's cheating behavior and the participants' cheating behavior. The encryption scheme adopts ElGamal public key cryptography, and the calculated verification parameters can be used many times. If the Dealer wants to share the new secret, he needs onlyto publish the new data on the bulletin board. The Dealer has a small amount of computation and a wide range of applicability.

Key words: secret sharing scheme; the Lagrange interpolation polynomial; threshold scheme; non-interactive authentication

责任编辑 张 枸