不需要安全信道的空间有效秘密分享方案

刘艳红[1),3)] 张福泰[1),2)]

[1)](南京师范大学计算机科学与技术学院 南京 210046)

[2)](江苏省信息安全与保密技术工程研究中心 南京 210097)

[3)](黑龙江省安全生产科学技术研究中心 哈尔滨 150040)

摘 要 高效的秘密分享方案在保护加解密密钥、门限密码系统、多方安全协议等方面发挥着重要作用.文中主要考虑空间有效的秘密分享问题.作者提出一个新的不需要安全信道的空间有效秘密分享方案.方案构造简捷、运行高效,并且在分发者和参与者之间发送信息不需要秘密信道的支持.文中给出了对新方案的安全性和性能的分析,同时给出了方案的工作流程图和一个简单的示例.由于安全性和性能方面的优点,新方案可广泛应用于诸如长期档案安全存储系统、资源受限环境(传感器网络、移动网络等)下机密信息的保护等方面.

关键词 秘密分享;空间有效秘密分享;秘密信道;离散对数

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.01816

A New Space Efficient Secret Sharing Scheme without a Secure Channel

LIU Yan-Hong[1),3)] ZHANG Fu-Tai[1),2)]

[1)](*School of Computer Science and Technology, Nanjing Normal University, Nanjing* 210046)

[2)](*Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, Nanjing* 210097)

[3)](*Heilongjiang Research Center for Labor Safety Science and Technology, Harbin* 150040)

Abstract Efficient secret sharing schemes play significant roles in areas such as safe guarding cryptographic keys, threshold cryptosystems, and secure multi-party protocols, etc. This paper focuses on the problem of space efficient secret sharing. We propose a space efficient secret sharing scheme without using private channels. The new scheme enjoys a simple construction and high efficiency. It does not require secure channels between the dealer and the share holders. The security analysis and performance analysis of the new construction are presented. We also give the execution flow chart and a very simple example to demonstrate how our secret sharing scheme works. Due to its security and performance features, the new scheme can be extensively applied in Long-Term archival storage system, and the safe guarding of very confidential information in resource constrained environments such as sensor networks and mobile networks, etc.

Keywords secret sharing; space efficient secret sharing; private channel; discrete logarithm

1 引 言

随着计算机及计算机网络的飞速发展,信息安全问题日益受到人们的关注.密码学为解决信息安全问题提供了许多实用技术.比如在保密通信中,为了实现信息的安全保密,可以采用加密的手段来保护信息,但是,仅仅通过加密技术还不足以完全保护信息安全.如果解密密钥丢失或者密文在传输和存储过程中遭到了破坏,那么明文将无法恢复.然而秘密分享技术提供了一种在不增加风险的前提下提高可靠性的办法来解决上述问题.

收稿日期:2012-05-16;最终修改稿收到日期:2012-07-12.本课题得到国家自然科学基金(61170298)、江苏省自然科学基金(BK2011101)资助.**刘艳红**,女,1982年生,硕士,主要研究方向为密码学.E-mail: angelpray@126.com. **张福泰**,男,1965年生,博士,教授,主要研究领域为密码学、网络与信息安全.

最早的秘密分享方案是(t,n)门限(threshold)秘密分享方案，是由 Blakley[1] 和 Shamir[2] 于 1979 年各自独立提出的. 其中 Shamir[2] 的方案是信息论安全的. 为了保证信息论安全，(t,n)门限方案要求秘密份额的长度至少不能小于秘密的长度. 即如果被分享的秘密是 b 比特位，在 n 个参与者中分享，那么被分享的秘密将被扩展成至少 $n\times b$ 比特位长度. 此外，我们知道必须有 t 个以上的份额持有者合作才能恢复被分享的秘密，所以，在信息论安全的(t,n)门限秘密分享方案中，信息的有效传输位最多为$\lceil 1/t\rceil$.

如果 $t=n$，就必须所有的参与者合作才能恢复秘密，那么此时信息的有效传输位最多才为$\lceil 1/n\rceil$. 所以在实现信息论安全的方案时，份额的存储和传输开销都比较大，并且随着 n 的增大，这种劣势就显得更加突出. 然而，在一些资源受限的环境，例如：传感器网络、移动网络等，这样高的存储和传输开销却是不适合的.

为了改善空间有效性，一些学者提出利用多秘密分享技术来解决. 首先将秘密 S 分割成 p 块，用 $S_i(i=1,2,\cdots,p)$来表示 p 块子秘密，然后用多秘密分享技术同时分享这 p 块子秘密. 目前已经有不少多秘密分享方案. 例如：文献[3]中基于离散对数问题的多秘密分享方案、文献[4]中的基于系统分组码的方案及文献[5-7]中的基于拉格朗日插值法的方案. 上述方案中的绝大多数在用多秘密分享技术减少秘密份额长度的同时，也需要大量的存储空间来存储一些公开信息用以保证方案的安全性. 毋庸置疑，公开参数的数量是衡量一个方案性能的重要指标，因为它影响了一个方案存储和通信的性能. 在文献[8]中，Li 等人列表比较了上面提到的几个多秘密分享方案公开参数的数量(m 表示秘密组的个数，P_i表示第 i 组秘密的个数，t_i表示第 i 组秘密的门限值)，如表 1 所示.

表 1　几种方案的公开参数量[8]

方案	公开参数量
Li 等人的方案[8]	$P_m\le t_1$　　m $P_m>t_1$　　P_m-t_1+m
Chan 等人的方案[9]	$\sum_{i=1}^{m}P_i$
Chien 等人的方案[4]	$m+\sum_{i=1}^{m}(n+p_i-t_i)$
Li 等人的方案[7]	$m+\sum_{i=1}^{m}(n+p_i-t_i)$
Pang 等人的方案[5]	$m+\sum_{i=1}^{m}(n+p_i-t_i)$

表中显示，这些方案都需要大量的公开参数.

另一种改善空间有效性的方法是将加密技术与秘密分享技术结合起来. 在文献[10-14]中，将秘密用对称密钥加密成密文，然后，将对称密钥在 n 个参与者中分享. 这样的解决办法使密钥存储量增长到原来的至少 n 倍，因为每个参与者都需要存储密钥的一个秘密份额. 更重要的是，此种方法将带来新的密文存储的问题. 如果将密文分别在 n 个参与者中存储，那么空间有效性将更低效；如果将密文放在一个公共的空间存储，那么将带来新的单点失败问题和权力过于集中的问题. 所以此种方法也不是理想的解决办法.

还有一种改善空间有效性的办法是隐藏被分享秘密的部分信息. 这种方法可有效减少秘密份额的长度. 文献[15-19]中的方案就是依据此种方法提出的. 它们利用递归的方法隐藏了秘密的部分信息，改善了秘密分享方案的空间有效性. 但是，Sahasranand 等人[20] 指出，此类方案，受到门限值 t 的限制，即它们只能递归隐藏至多 $t-1$ 块秘密. 另外，因为此方法是递归隐藏部分秘密的，在重构被分享的秘密时，就需要递归调用多次插值公式，因此重构的效率比较低.

2009 年 Parakh 和 Kak 在 Shamir 方案的基础上，利用拉格朗日插值法给出了一个空间有效的秘密分享方案[21]. 与 Shamir 方案不同的是，他们的方案是将 k 个子秘密作为分享多项式 $f(x)$的函数值，产生函数曲线上的 k 个点$(i,s_i)(i=0,1,\cdots,k-1)$，然后利用插值法再构造出 $k-1$ 次多项式 $f(x)$，之后再计算 $f(x)$曲线上新的点$(i+k,f(i+k))(i=0,1,\cdots,n-1)$，并将这些新的点秘密地分发给 n 个参与者. 从而完成了整个秘密分发的过程. 然而，Sahasranand 等人[20] 却指出，利用插值方法实现的秘密分享方案存在着一些弊端. 比如：子秘密的个数与门限值 t 一定要满足 $t\le k$；子秘密之间不能存在线性相关性，否则插值出来的多项式将不能满足门限值的要求；对于相同的子秘密，插值出来的多项式可能是一个常量多项式等等. 另外，Sahasranand 等人[20] 对文献[21]中的方案还给出了两个新的攻击方法，这里就不再赘述了.

本文设计了一个新的不需要安全信道的空间有效秘密分享方案. 方案除了在空间有效性的实现上克服了上面提到的不足外，还具有两大优点：一是在分发者与参与者之间不需要维护秘密信道；二是可以用来分享任何类型、任何长度的秘密信息. 方案利用 Diffie-Hellman[22] 密钥协商技术实现了份额在公开信道上的安全分配，采用分组和对称加密来实现对任意长度秘密的分享，同时保持份额只有一个分组的长度.

2 新的不需要安全信道的空间有效(t,n)秘密分享方案

方案由3个阶段构成:初始化阶段、构造阶段和恢复阶段.

先对方案用到的各种符号进行说明,如表2所示.

表2 方案中的符号说明

符号	符号说明
t	门限值
n	参与者的个数
$\mathcal{M}=\{M_1,M_2,\cdots,M_n\}$	n个参与者的集合
D	分发者,$(D\notin\mathcal{M})$
K	安全参数
S	被分享的秘密,并且$S\in\Omega$
Ω	秘密空间
$\mathcal{C}$	份额空间
$P_i(i=1,2,\cdots,n)$	参与者获得的份额
a_i	参与者$M_i(i=1,2,\cdots,n)$的私钥
Y_i	参与者$M_i(i=1,2,\cdots,n)$的公钥
b	分发者D的秘密值
Y_D	分发者D的公开值
$\mathbb{F}_q$	q阶有限域
g	$\mathbb{F}_q^*$上的生成元
d	秘密被分割的块数
L	多项式需要选择随机系数的个数
Z	多项式需要公开的函数点的个数
$S_i(i=1,2,\cdots,d)$	分割后的子秘密块
R	对称密钥
S_i'	每块子秘密加密后的密文块
E	对称加密算法
D	对称解密算法
$f(x)$	构造出来的秘密分享多项式
$R_i(i=1,2,\cdots,L)$	为构造多项式而选择的辅助随机数
$\eta_i(i=1,2,\cdots,Z)$	需要公开的函数点的自变量取值

方案由n个参与者$\mathcal{M}=\{M_1,M_2,\cdots,M_n\}$和一个分发者$D(D\notin\mathcal{M})$组成.并且在整个方案中,假设分发者和参与者都是诚实、可信的.这里暂不考虑分发者和参与者的欺骗行为.K是基于离散对数的安全参数,用来保证方案的计算安全性.原始秘密分割后的比特位长度不得小于此安全参数的值.在目前的实际应用中,一般$K=1024$就可以满足广泛的安全要求了.但我们的方案并不将安全参数固定.用户可以根据实际情况,在系统初始化阶段自己灵活地设置安全参数的值.

下面将给出方案详细的介绍.

(1)初始化阶段

分发者D首先创建一个公开的公告牌(notice board),此公告牌用来存储一些必要的公开信息,这里要求只有秘密分发者D可以修改、更新公告牌上的内容,而其他人只能阅读或下载.

分发者D执行下面的初始化操作:

① 设置安全参数K的值.

② 设置门限t的值.

③ 选择一个素数q满足$q>\max(2^K,n)$,$\mathbb{F}_q$为包含q个元素的有限域,在$\mathbb{F}_q^*$中随机选择一个整数g,满足离散对数问题在此基础上是计算不可行的.

④ 秘密空间为$\Omega=\{0,1\}^*$,份额空间为$\mathcal{C}=\mathbb{F}_q$.

⑤ D将公开信息$params=\langle K,t,n,\mathcal{M},\mathbb{F}_q,g,\Omega,\mathcal{C}\rangle$公布到公告牌上.

参与者$M_i(i=1,2,\cdots,n)$的初始化操作:随机选择一个整数$a_i\in_U\mathbb{Z}_{q-1}$作为自己的私钥,计算公钥$Y_i=g^{a_i}\bmod q$,并将公钥Y_i公开发送给分发者D.

D将所有参与者的公钥信息$params=\langle Y_i\rangle(i=1,2,\cdots,n)$公布到公告牌上.

(2)构造阶段

分发者D执行下面的步骤进行秘密分发:

① 计算秘密S分割的块数$d=\left\lceil\frac{|S|}{K}\right\rceil$.

② 判断不等式$t\leq(d+2)$是否成立,

如果成立,$L=0$,$Z=(d+2)-t$;

如果不成立,$L=t-(d+2)$,$Z=0$.

③ 对秘密S按照二进制从低位到高位进行分割,每K个比特位作为一个子秘密块.即$S=S_1\|S_2\|S_3\|\cdots\|S_{d-1}\|S_d$分割成$d$块子秘密,然后安全销毁秘密$S$.

④ 随机选择对称密钥$R\in\mathbb{F}_q$和对称加密算法E,加密每一个子秘密块,并将加密的密文作为二进制整数再进行模运算.即$S_i'=E_R(S_i)\bmod q(i=1,2,\cdots,d)$将对称加密算法$E$公布到公告牌.之后安全销毁所有的子秘密块$S_i(i=1,2,\cdots,d)$.

⑤ 选择L个随机数.$R_L,R_{L-1},\cdots,R_1\in\mathbb{F}_q$,如果$L=0$,则不需要进行此步操作,然后安全销毁$L$.

⑥ 将随机数$R_i(i=L,L-1,\cdots,2,1)$、密文块$S_i'(i=d,d-1,\cdots,2,1)$、变量d和对称密钥R作为系数,来构造多项式$f(x)$:

$$f(x)=(R_Lx^{L+1+d}+\cdots+R_1x^{2+d}+Rx^{1+d}+S_d'x^d+\cdots+S_2'x^2+S_1'x+d)\bmod q.$$

⑦ 随机选择$b\in\mathbb{F}_q$.计算相应的公开值$Y_D=g^b\bmod q$,并将公开值Y_D公布到公告牌上,对b严格保密.

⑧ 计算每个参与者的份额$P_i=(Y_i)^b\bmod q(i=1,2,\cdots,n)$.并计算份额的函数值$f(P_i)\bmod q(i=1,2,\cdots,n)$.将这些信息$f(P_i)$公布到公告牌上.

⑨ 从集合$\mathbb{Z}_{q-1}^*-\{g^b,Y_i,(Y_i)^b\mid i=1,2,\cdots,n\}$中选取$Z$个最小整数$\eta_1,\eta_2,\cdots,\eta_Z$,并且计算函数值$f(\eta_i)(i=1,2,\cdots,Z)$.之后将这些信息

$(\eta_i, f(\eta_i))(i=1,2,\cdots,Z)$公布到公告牌上. 如果$Z=0$,则不需要进行此步操作,然后安全销毁 Z.

⑩ 最后安全销毁$f(x)$,R,d 和 $S_i'(i=1,2,\cdots,d)$,$R_i(i=1,2,\cdots,L)$.

为了能够清楚地说明此阶段的工作过程,我们给出了一个流程图用来进行直观的描述,如图 1 所示.

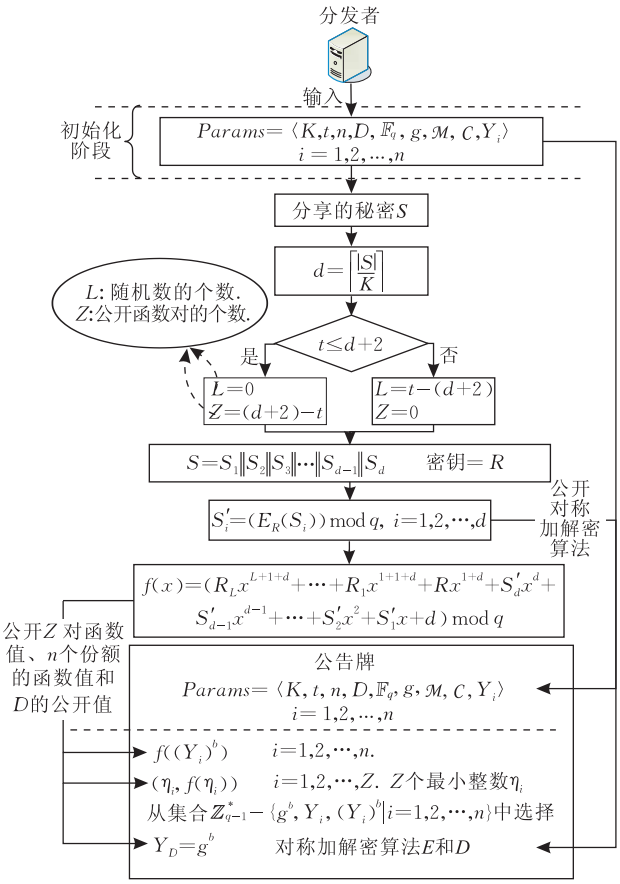

图 1　方案的构造阶段

(3) 恢复阶段

假设任意 t 个或更多的参与者$\{M_i\}_{i\in I}$($I\subseteq\{1,2,\cdots,n\}$)合作重构被分享的秘密. 不失一般性,这里我们就假设$\{M_1,M_2,\cdots,M_t\}$ t 个参与者合作重构秘密. 他们将执行下面的步骤:

① 计算份额 $P_i=(Y_D)^{a_i}$,之后提交自己的份额 P_i来重构被分享的秘密.

② 通过 Lagrange 插值方法得到 $f(x)$多项式:

$$\begin{aligned} f(x)&=\Big(\sum_{i=1}^{Z}f(\eta_i)\prod_{j=1,j\neq i}^{Z}\frac{x-\eta_j}{\eta_i-\eta_j}+\\ &\quad\sum_{i=1}^{t}f(P_i)\prod_{j=1,j\neq i}^{t}\frac{x-P_j}{P_i-P_j}\Big)\bmod q\\ &=(\alpha_{L+d+1}x^{L+d+1}+\cdots+\alpha_{d+1}x^{d+1}+\\ &\quad\alpha_d x^d+\cdots+\alpha_2 x^2+\alpha_1 x+\alpha_0)\bmod q. \end{aligned}$$

③ 由 $f(0)=\alpha_0$,得到原始秘密被分割的块数 $d=\alpha_0$,得到对称密钥 $R=\alpha_{d+1}$.

④ 用对称密钥 R 解密密文块,如下所示:

$$S_i=D_R(\alpha_i)\bmod q\ (i=1,2,\cdots,d),$$

从而得到子秘密块 $S_i(i=1,2,\cdots,d)$.

⑤ 合并所有子秘密块得到被分享的原始秘密 $S=S_1\|S_2\|S_3\|\cdots\|S_{d-1}\|S_d$.

为了能够清楚地说明此阶段的工作过程,我们给出了一个流程图用来进行直观的描述,如图 2 所示.

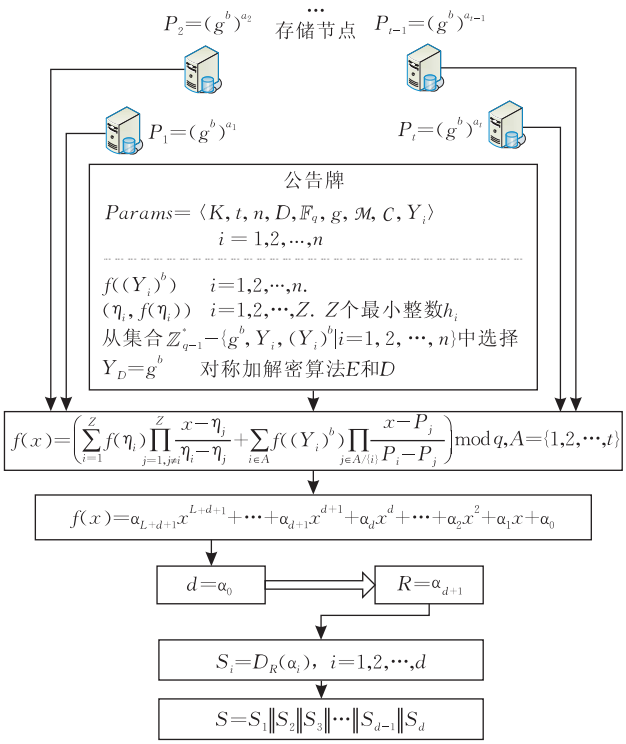

图 2　方案的恢复阶段

3　举　例

本节给出了一个简单实例来说明方案的可行性. 为使所举实例具有说服性和可比性,这里采用了与 Parakh 等人[19]方案中相同的参数,即相同的参与者人数 $n=7$($\mathcal{M}=\{M_1,M_2,\cdots,M_7\}$),相同的门限值 $t=5$,以及相同的原始秘密 $S=17280512$. 此实例的安全参数设置的比较小,即 $K=6$. 当然,在实际应用中,这样的安全参数可能达不到安全的要求. 在方案分发和重构过程中,暂不考虑分发者和参与者的欺骗行为,也不考虑信息在传输途中可能出现的各种差错.

整个方案的运行过程如下:

(1) 初始化阶段

分发者 D 首先创建一个公开的公告牌(notice board),此公告牌用来存储一些必要的公开信息,这里要求只有秘密分发者 D 可以修改、更新公告牌上

的内容，而其他人只能阅读或下载.

D 执行下面的初始化操作：

① 设置安全参数 $K=6$，门限值 $t=5$，参与者人数 $n=7$.

② 选择一个素数 $q=67$ 满足 $67>\max(2^6,7)$，$\mathbb{F}_{67}$ 为包含 67 个元素的有限域，取 $\mathbb{F}_{67}^*$ 一个生成元 $g=8$.

③ 秘密空间为 $\Omega=\{0,1\}^*$，要分享的秘密 $S=17280512\in\Omega$. 份额空间为 $\mathcal{C}=\mathbb{F}_{67}$.

④ D 将公开信息 $params=\langle 6,5,7,\mathcal{M},\mathbb{F}_{67},8,\Omega,\mathcal{C}\rangle$ 公布到公告牌上.

参与者的初始化操作：$M_1,M_2,\cdots,M_7$ 依次选取整数 $\mathbb{Z}_{67}^*$ 中的元素 $a_1=5,a_2=3,a_3=6,a_4=4,a_5=7,a_6=9,a_7=8$ 作为自己的私钥，计算出各自的公钥依次为 $Y_1=g^{a_1}=5$，$Y_2=g^{a_2}=43$，$Y_3=g^{a_3}=40$，$Y_4=g^{a_4}=9$，$Y_5=g^{a_5}=52$，$Y_6=g^{a_6}=45$，$Y_7=g^{a_7}=14$，并将各自的公钥公开发送给分发者 D.

D 将所有参与者的公钥信息 $params=\langle 5,43,40,9,52,45,14\rangle$ 公布到公告牌上.

(2) 构造阶段

D 执行下面的步骤：

① 计算秘密 $S=17280512$ 分割的块数

$$d=\left\lceil\frac{|S|}{K}\right\rceil=\left\lceil\frac{|100000111101011100000000|}{6}\right\rceil=5.$$

② $5\leq(5+2)$ 成立，所以 $L=0$，$Z=2$.

③ 将秘密 S 进行分割

$$\begin{aligned}S&=S_1\|S_2\|S_3\|S_4\|S_5\\&=1\|000001\|111010\|111000\|000000\\&=1\|1\|58\|56\|0,\end{aligned}$$

然后安全销毁秘密 $S=17280512$.

④ 随机选择对称密钥 $R=47\in\mathbb{F}_{67}$，并加密每一个子秘密块 $S_i'=E_{47}(S_i)\bmod 67(i=1,2,\cdots,5)$ 为了方案的直观性，这里我们选择简单的移位加密操作，如下所示：

$$S_i'=(R+S_i)\bmod q=\{48,48,38,36,47\}.$$

之后安全销毁所有的子秘密块 S_i.

⑤ 因为 $L=0$，不需要进行其它操作，只需将 L 安全销毁即可.

⑥ 将密文块 $S_i'(i=5,4,3,2,1)$、变量 $d=5$ 和对称密钥 $R=47$ 作为多项式的系数，构造多项式 $f(x)$：

$$\begin{aligned}f(x)&=(Rx^{1+5}+S_5'x^5+S_4'x^4+S_3'x^3+\\&\quad S_2'x^2+S_1'x+d)\bmod 67\\&=(47x^6+47x^5+36x^4+38x^3+\\&\quad 48x^2+48x+5)\bmod 67.\end{aligned}$$

⑦ 随机选择 $b=2\in\mathbb{F}_{67}$. 计算公开值

$Y_D=g^b\bmod q=8^2\bmod 67=64$. 并将公开值 $Y_D=64$ 公布到公告牌上.

⑧ 计算出每个参与者份额 $P_i=(Y_i)^b\bmod q$ 依次为 25，40，59，14，24，15，62 以及份额的函数值 $f(P_i)\bmod q$ 依次为 20，37，13，6，63，1，66. 并将函数值的信息 $\langle 20,37,13,6,63,1,66\rangle$ 公布到公告牌上.

⑨ 从集合 $\mathbb{Z}_{66}^*-\{64,5,43,40,9,52,45,14,25,59,24,15,62\}$ 中选取 $Z=2$ 个最小整数 $\eta_1=1,\eta_2=2$，计算出它们的函数值 $f(\eta_i)\bmod q$ 分别为 1，57. 将这些信息 $\langle(1,1),(2,57)\rangle$ 公布到公告牌上. 之后安全销毁 R,d 和 $S_i'(i=1,2,\cdots,5)$.

(3) 恢复阶段

假设任意 $t=5$ 个或更多的参与者 $\{M_i\}_{i\in I}(I\subseteq\{1,2,\cdots,7\})$ 合作重构被分享的秘密. 不失一般性，这里我们假设参与者 $\{M_1,M_2,M_3,M_4,M_5\}$ 合作重构秘密. 他们将执行下面的步骤：

① 每个参与者计算自己的份额 $P_i=(Y_D)^{a_i}\bmod q$. $\{M_1,M_2,M_3,M_4,M_5\}$ 计算并提交自己的份额 25，40，59，14，24.

② 通过 Lagrange 插值方法重构多项式 $f(x)=47x^6+47x^5+36x^4+38x^3+48x^2+48x+5$.

③ 由 $f(0)=5$，得知秘密被分割成的块数 $d=f(0)=5$ 及对称密钥 $R=47$.

④ 用对称密钥 $R=47$ 解密密文块，与构造阶段的加密算法对应，这里进行简单的移位解密操作. 得到的子秘密块 S_i 依次为 1，1，58，56，0.

⑤ 合并所有子秘密块，得到

$$\begin{aligned}S&=S_1\|S_2\|S_3\|S_4\|S_5\\&=1\|1\|58\|56\|0\\&=000001\|000001\|111010\|111000\|000000\\&=00000100000111101011000000000\\&=17280512,\end{aligned}$$

即恢复出了被分享的秘密 $S=17280512$.

4 分析与讨论

4.1 安全性分析

这节对我们的方案进行安全性分析，分析结论如下：

(1) 在离散对数问题和 CDH 问题是困难的前提下，敌手通过公告牌上的信息 $Y_D=g^b,Y_i=g^{a_i}(i=1,2,\cdots,n)$，获得分发者或者参与者的秘密信息 b,a_i 是计算不可行的. 同样敌手获得任何参与者 M_i 的份额 $P_i=(g^{a_i})^b$ 的概率也是可以忽略的.

(2) 假设敌手已经掌握了 $t-1$ 个参与者的份额

信息，即 $P_i(i=1,2,\cdots,t-1)$. 但根据求解线性方程组理论，敌手不能确定多项式 $f(x)$ 的系数. 所以敌手得不到关于秘密 S 的信息.

(3) 假设敌手获得部分子秘密块，即使敌手获得了 $d-1$ 块子秘密，也无法获得另外一块子秘密. 这是因为构造多项式 $f(x)$ 的时候，各子秘密是用随机对称密钥加密过的，只要所用对称加密算法具有足够的安全性(如选择密文安全)，敌手已经知道部分子秘密块，无益于他获取其它子秘密块.

(4) 与 Parakh 和 Kak 的方案比，新方案在构造阶段没有使用插值的方法构造多项式，可以保证多项式能够满足门限值的要求. 所以克服了 Sahasranand 等人[20]指出的用在构造阶段使用插值法所带来的弊端，避免了他们提到的两种攻击.

(5) 方案甚至不会泄露秘密的长度信息. 因为将秘密进行分块后，块数的秘密隐藏在多项式中. 所以对于原始秘密的长度信息，敌手是没有办法知道的.

(6) 方案即使多次分享相同的秘密 S，每次得到多项式相同的概率是可以忽略的. 因为每次分发者选择的对称密钥是随机的，所以每次多项式的系数也就不同. 那么公告牌上发布的信息也必然不同. 这样就可以很有效地抵抗重放攻击.

上面的分析说明，我们的方案是安全的空间有效秘密分享方案.

4.2　运行性能

本节对新方案的运行性能进行分析.

(1) 方案在计算性能上较 Parakh 等人[21]的方案要强. 在 Parakh 的方案中，采用了递归隐藏数据的方法来实现空间有效性. 所以在构造阶段，需要递归操作多个多项式. 在恢复阶段，需要递归调用多次 Lagrange 插值法才能恢复被分享的秘密. 而我们的方案在构造和恢复阶段，都只需操作一个多项式. 所以在计算性能上，新方案要高于 Parakh 等人的方案.

(2) 新方案中参与者的份额是可以自己计算的. 方案利用 Diffie-Hellman 密钥协商技术，参与者通过公告牌信息得到分发者的临时公钥 Y_D，就可以计算自己的份额 $P_i=(Y_D)^{a_i}$. 分发者可以得到相同的 $P_i=(Y_i)^b$. 在方案的运行过程中，秘密份额不需要进行传输. 所以新方案的通信性能是非常高的.

(3) 新方案利用 Diffie-Hellman 技术解决了秘密信道的问题. 所以，方案可以运行在价格非常低廉、普及范围非常广、通信性能非常高的万维网上. 秘密信道是需要付出一定运行成本才能实现的，甚至在有些情况下是不可能得到满足的. 因此，新方案的运行成本低，非常适合推广及应用.

(4) 新方案对被分享的秘密 S 没有任何限制，可以是任何类型、任何长度的信息. 然而，在文献[19]中，只可以实现 $t-1$ 个秘密块的分享. 另外，在文献[21]中，子秘密块不能存在线性相关性，否则将达不到门限值的要求. 当所有子秘密块相同时，方案甚至不能正常工作，因为插值出来的多项式将是一个常函数. 所以，同上述方案相比，新方案的适用范围更广.

通过上面的分析我们得出，新方案无论从计算性能、通信性能以及适用范围等方面都具有一定的优势. 而且还特别适合一些特定场合的应用. 例如长期归档文件的存储、在资源受限环境下对机密文件的安全保存与备份等.

5　结　语

不需要安全信道的空间有效秘密分享方案不仅具有理论意义，而且具有重要的实际应用价值. 本文给出了一个新的不需要安全信道的空间有效秘密分享方案. 在新方案的构造中，借鉴了多秘密分享的思想，使用了 Diffie-Hellman 密钥协商技术，及对称加密技术. 新方案可以分享任何类型、任何长度的秘密，分发者与参与者之间不需要通过秘密信道进行保密通信，而且参与者需要保存秘密信息的长度是固定的. 我们给出了方案的运行流程图和一个简单的运行实例，以说明方案的工作流程. 分析显示新方案在安全性和运行性能方面与已有的几个同类方案相比，有明显的优势. 这些特点使新方案可以在现实的很多场合得到推广和应用，例如在长期归档文件的安全存储，在一些资源受限的环境下保存和备份机密文件等等.

参　考　文　献

[1] Blakley G R. Safeguarding cryptographic keys//Proceedings of the AFIPS 1979 National Computer Conference. New York, 1979: 313-317

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

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

[4] Chien H Y, Jan J K, Tseng Y M. A practical (t,n) multi-secret sharing scheme. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2000, E83-A(12): 2762- 2765

[5] Pang L J, Wang Y M. A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing. Applied Mathematics and Computation, 2005, 167(2): 840-848

[6] Yang C C, Chang T Y, Hwang M S. A (t,n) multi-secret

sharing scheme. Applied Mathematics and Computation, 2004, 151(2): 483-490

[7] Li Huixian, Cheng Chentian, Pang Liaojun. A new (t,n)-threshold multi-secret sharing scheme//Lecture Notes in Artificial Intelligence. Berlin: Springer-Verlag, 2005: 421-426

[8] Li Huixian, Pang Liaojun, Cai Wandong. An efficient threshold multi-group-secret sharing scheme//Proceedings of the 2nd International Conference on Fuzzy Information and Engineering. Heidelberg, 2007: 911-918

[9] Chan Chao-Wen, Chang Chin-Chen. A scheme for threshold multi-secret sharing. Applied Mathematics and Computation, 2005, 166(1): 1-14

[10] Schneier Bruce. Schneier's Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography. USA: Wiley, 2007

[11] Rogaway P, Bellare M. Robust computational secret sharing and a unified account of classical secret-sharing goals//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, 2007: 172-184

[12] Vinod V, Narayanan A, Srinathan K, Rangan C, Kim K. On the power of computational secret sharing//Proceedings of the Progress in Cryptology INDOCRYPT 2003. Lecture Notes in Computer Science 2904. 2003: 265-293

[13] Beguin P, Cresti A. General short computational secret sharings chemes//Proceedings of the EUROCRYPT 95. Lecture Notes in Computer Science 921. Springer, 1995: 194-208

[14] Krawczyk H. Secret sharing made short//Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California. USA: Lecture Notes in Computer Science. Springer, 1994: 136-146

[15] Gnanaguruparan M, Kak S. Recursive hiding of secrets in visual cryptography. Cryptologia, 2002, 26(1): 68-76

[16] Parakh A, Kak S. A tree based recursive scheme for space efficient secret sharing. Cryptology ePrint Archive, Report, 2009: 409

[17] Parakh A, Kak S. A recursive threshold visual cryptography scheme. Cryptology ePrint Archive, Report, 2008: 535

[18] Parakh A, Kak S. Space efficient secret sharing: A recursive approach, arXiv: 0901. 4814v1 [cs. CR] Jan 2009; Cryptology ePrint Archive, Report, 2009: 365

[19] Parakh A, Kak S. Space efficient secret sharing for implicit data security. Information Sciences, 2011, 181(2): 335-341

[20] Sahasranand K R, Nagaraj N, Rajan S. How not to share a set of secrets. International Journal of Computer Science and Information Security, 2010, 8(1): 234-237

[21] Parakh A, Kak S. Space efficient secret sharing, arXiv: 0901. 4798v2 [cs. CR] Feb 2009//Proceedings of the 4th Annual Computer Science Research Conference. University of Oklahoma, 2009

[22] Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

LIU Yan-Hong, born in 1982, M. S. candidate. Her research interests focus on cryptography and network security.

ZHANG Fu-Tai, born in 1965, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography, network and information security.

Background

Secret sharing is a fundamental tool in group oriented cryptography, secure multi-party computation, and secure storage, etc. In 1979, the first (t,n) threshold secret sharing schemes were introduced by Blakley and Shamir independently. Shamir's scheme is a perfect threshold scheme where knowing only $t-1$ or fewer secret shadows provides no more information about the secret to an opponent than knowing no pieces. While from the view point of space efficiency, perfect or information theoretically secure secret sharing schemes are space inefficient. This is because a (t,n) threshold information theoretically secure secret sharing scheme expands a secret of b bits into n shares each of at least b bits in size. Furthermore, since only t of these shares are needed to recreate the secret, each bit of any share in a (t,n) threshold information theoretically secure secret sharing scheme, effectively conveys at most $1/t$ bits of the shared secret. Such an expansion will inevitably induce the increase in bandwidth and transmission costs. This problem was firstly addressed by Hugo Krawczyk, and consequently studied by Parakh et al.. However, almost all previous solutions either have security weaknesses, or computationally inefficient, or rely on private channels between the dealer and the shareholders. This paper focuses on the design of practical space efficient secret sharing schemes.

Our work is supported by the National Natural Science Foundation of China under Grant No. 61170298 and the Natural Science Foundation of Jiangsu Province under Grant No. BK2011101.