基于圆性质的动态(t,n)门限秘密共享方案

葛丽娜[1,2] 唐韶华[1]

(华南理工大学计算机科学与工程学院 广州 510640)[1] (广西民族大学数学与计算机科学学院 南宁 530006)[2]

摘 要 基于圆的几何特性设计一个动态的门限秘密共享方案,引入双变量杂凑函数与公告牌,参与者的影子由伪影子与公共参数计算而得,而且参与者以相同的伪影子很容易参与下一个秘密共享,使该方案动态变化时参与者所持有的伪影子保持不变。与WU&HE的几何方法秘密共享方案相比,本方案能实现参与者的动态加入与退出,还可以容易地改变门限值t。本方案的计算简单、运算速度快。实验数据表明与Shamir方案相比,本方案有更高的计算效率,它被证明是安全的。

关键词 秘密共享,圆性质,动态的

中图法分类号 TP309 **文献标识码** A

Dynamic (t,n) Threshold Secret Sharing Scheme Based on Circle Properties

GE Li-na[1,2] TANG Shao-hua[1]

(School of Computer Science and Engineering, South China Univ. of Tech., Guangzhou 510640, China)[1]

(School of Math & Computer Science, Guangxi University of Nationalities, Nanning 530006, China)[2]

Abstract A dynamic threshold secret sharing scheme based on circle properties was proposed. A two-variable one-way hash function and a notice board were introduced. A participant computes his shadow information by using both the public information and his pseudo-shadow. The pseudo-shadow of each participant always keeps the same even if a participant leaves/joins, or the value of t changes dynamically. Further more, the participants can share next secret by the same pseudo-shadow. Compared with a geometric approach for sharing secrets proposed by WU & HE, not only the participants can join/leave the system dynamically, but also the value of the threshold of t is easy to change in the proposed scheme. The proposed scheme is simple, and fast. The experimental results show that our scheme is more efficient than the Shamir's scheme. It is proven secure.

Keywords Secret sharing, Circle property, Dynamic

1 引言

秘密共享体制是将一个秘密分解成多个子秘密(影子),分别由多个参与者控制,只有足够多的参与者把子秘密放在一起才能揭示出秘密,而少于那个数量的参与者不能恢复共享秘密。秘密共享在现代密码学中有着非常重要的地位,在现实生活中有着重要的应用,如遗嘱的保存与公布、招投标系统的投标与开标等。

自1979年shamir[1]和Bakley[2]首先分别基于Lagrange多项式插值和射影几何理论提出门限秘密共享方案后,秘密共享得到了大量研究[3-7],文献[3]提出了在线秘密共享机制,引入公告牌发布一些辅助信息;文献[4]等将模运算用于秘密共享,提出了基于中国剩余定理的秘密共享方案;还有一些方案针对多秘密共享、防欺骗等方面进行了研究[5-8]。

WU&HE提出采用多维圆的几何特性进行秘密共享[9],文献[10]主要是针对文献[9]的数学理论背景作改进,认为素数p不需满足限制条件$p=\pm 3 \pmod 8$,同时用概率方法代替[10]的查表法来寻找二次剩余及其相应的模平方根,使p可以取大素数以抵抗穷举攻击;文献[11]在影子生成算法中加入一个偏移运算,使参与者参与秘密恢复时提交的是影子偏移量而非真正的影子,保证影子的机密性。由于文献[9-12]在共享秘密过程所构造圆的圆心由全部的秘密且仅由这些秘密构成,限制了方案的灵活性,使得这些方案不能实现参与者的动态加入与退出;同时,参与者的子秘密是一次性的。本文利用多维圆的几何性质、双变量杂凑函数设计了一个秘密共享方案,能实现参与者的动态加入与退出、门限值t或共享秘密的动态改变,并且在相同的参与者群体中可进行多次秘密共享而无需参与者更改其伪影子。

2 方案描述

定理1[9] 假设$t-1$维空间中的t个点$(x_{i,1},x_{i,2},\cdots,x_{i,t-1})(i=1,2,\cdots,t)$不同在$t-2$维空间中,那么由这些点可

到稿日期:2008-06-24 本文受国家自然科学基金资助项目(No. 60572139),霍英东教育基金资助项目(No. 101069),教育部新世纪优秀人才支持计划(NCET-06-0744)资助。

葛丽娜(1969-),女,博士研究生,主要研究信息安全,E-mail:gelina100@gmail.com;**唐韶华**(1970-),男,博士,教授,博士生导师,主要研究信息安全、计算机网络。

以唯一地确定一个圆方程：$\sum_{i=1}^{t-1}(x_i-c_i)^2=R(\bmod p)$。

本文所有运算都在有限域 $GF(p)$ 上进行。当 $p\equiv 3 \pmod 4$ 时可以通过公式求得一个二次剩余元素的方根[10]：$a\in QR_p$，$x=a^{(p+1)/4}(\bmod p)$，x 就是 a 模 p 的一个平方根。故 p 选取一个形如 $p\equiv 3 \pmod 4$ 的大素数。

2.1 初始化

系统的对象包括：秘密分发者 D；n 个参与者 $P=\{P_1,P_2,\cdots,P_n\}$；秘密恢复者；需要共享的秘密 s；一个公告牌，用于存放公开信息，系统各方均可读取公告牌上的内容，但只有秘密分发者才能写或更新公告牌上的内容。

D 作如下初始化操作：

(1) 选取一个形如 $p\equiv 3 \pmod 4$ 的大素数 p；

(2) 定义两个杂凑函数 f 与 g，$f:[0,p),[0,p)\to[0,p)$，$g:[0,p)\to[0,p)$；基于函数 g，定义一个嵌套函数：$g^n(x)=\underbrace{g(g(\cdots(g}_{n}(x))\cdots))$；

(3) 在公告牌上公布信息：p,f,g,t。

f 是一个双变量的杂凑函数，以下给出它的一个定义：

定义 1[8] 双变量杂凑函数 $f(r,s)$，该函数具有以下性质：

① 已知 r 和 s，$f(r,s)$ 易于计算；

② 已知 s 和 $f(r,s)$，计算 r 在计算上是不可行的；

③ 在 s 未知的情况下，对于任意的 r，难于计算 $f(r,s)$；

④ 已知 s 的情况下，找到 $r_1\neq r_2$ 且满足 $f(r_1,s)=f(r_2,s)$ 在计算上是不可行的；

⑤ 已知 r 和 $f(r,s)$，计算 s 在计算上是不可行的；

⑥ 已知任意多的 $(r_i,f(r_i,s))$ 对，计算 $f(r',s)$ 在计算上是不可行的，其中 $r'\neq r_i$。

2.2 秘密分配

秘密分发者在确定了参与者集合后，为每个参与者 P_i 选取秘密数 $s_i\in(0,p)$，s_i 称为 P_i 的伪影子，并通过安全信道将 s_i 发送给参与者 P_i，P_i 秘密保存 s_i。然后，秘密分发者首先生成一个含共享秘密信息的 $t-1$ 维空间圆，即：

(1)随机生成 $t-1$ 个数：$c_1,c_2,\cdots,c_{t-1}\in(0,p)$；

(2)以 $O(c_1,c_2,\cdots,c_{t-1})$ 为圆心、s 为半径平方确定圆 Ω，其圆方程为：$\sum_{i=1}^{t-1}(x_i-c_i)^2=s(\bmod p)$；

(3)选取一个随机数：$r((0,p)$；

(4)将 r 公布于公告牌上。

接着，秘密分发者分别将圆 Ω 上的不同点作为影子分配给 n 个参与者，以 P_i 为例说明影子的分配过程：

(1) 根据参与者 P_i 的伪影子 s_i 与公开参数 r，找到 $t-3$ 个数 $(x_{i,1},x_{i,2},\cdots,x_{i,t-3})$：$y_i=f(r,s_i)$，$x_{i,1}=g(y_i)$，$x_{i,2}=g^2(y_i)$，$x_{i,3}=g^3(y_i)$，$\cdots$，$x_{i,t-3}=g^{t-3}(y_i)$。

(2)计算：

$$\begin{cases} d_{i,1}=x_{i,1}-c_1(\bmod p)\\ d_{i,2}=x_{i,2}-c_2(\bmod p)\\ \cdots\cdots\\ d_{i,t-3}=x_{i,t-3}-c_{t-3}(\bmod p)\end{cases}$$

(3)计算：

$e_{i,1}=d_{i,1}^2(\bmod p)$，$e_{i,2}=d_{i,2}^2(\bmod p)$，$\cdots$，$e_{i,t-3}=d_{i,t-3}^2(\bmod p)$。

(4) 重复计算：

随机生成 $d_{i,t-2}\in[0,p)$，

计算 $e_{i,t-2}=d_{i,t-2}^2(\bmod p)$；

计算 $e'_{i,t-1}=s-\sum_{j=1}^{t-2}e_{i,j}(\bmod p)$，则 $d_{i,t-1}=e'^{(p+1)/4}_{i,t-1}(\bmod p)$；

计算 $e_{i,t-1}=d_{i,t-1}^2(\bmod p)$.

直到 $e_{i,t-2}+e_{i,t-1}=s-\sum_{j=1}^{t-3}e_{i,j}(\bmod p)$

(5)令 $\begin{cases}x_{i,t-2}=d_{i,t-2}+c_{t-2}(\bmod p)\\ x_{i,t-1}=d_{i,t-1}+c_{t-1}(\bmod p)\end{cases}$

(6) 令 $B_i=(x_{i,1},x_{i,2},\cdots,x_{i,t-1})$，$B_i$ 就是圆 Ω 上的一点，将 B_i 作为 P_i 的影子。

以上过程要保证 $\{B_i\mid i=1,2,\cdots,n\}$ 中任意 t 个点不同在 $t-2$ 维空间中。为 P_i 计算出圆上一点 B_i 之后，再计算 $h_i=g(\sum_{j=1}^{t-1}x_{i,j}(\bmod p))$，$h_i$ 用于保证数据的完整性，B_i 是 P_i 的影子，秘密分发者不需要将 B_i 传送给 P_i，而只需将 h_i 与 $(x_{i,t-2},x_{i,t-1})$ 公布于公告牌上。

通过以上方法为所有的参与者 $P_i\in P$ 选取影子 B_i，$i=1,2,\cdots,n$，但各参与者只需要保存其伪影子 s_i。此时，公告牌上的信息有：$p,f,g,t,r,\{h_i,(x_{i,t-2},x_{i,t-1})\mid i=1,2,\cdots,n)\}$。

2.3 秘密的恢复

秘密恢复时，需要至少 t 个参与者提交影子，参与者利用自己的伪影子与公共参数计算其影子的有关信息。秘密恢复者需要收集足够多的影子：

(1)必须有不少于 t 个参与者参与秘密恢复，这些参与者作如下操作，以 P_i 为例：

a)从公告牌上下载 p,f,g,t,r，

b)取出自己的伪影子 s_i，利用 s_i 与 r 计算：

$y_i=f(r,s_i)$，$x_{i,1}=g(y_i)$，$x_{i,2}=g^2(y_i)$，$x_{i,3}=g^3(y_i)$，$\cdots$，$x_{i,t-3}=g^{t-3}(y_i)$；

c)将 $(x_{i,1},x_{i,2},\cdots,x_{i,t-3})$ 发送给秘密恢复者；

(2)秘密恢复者获取 P_i 的 $(x_{i,1},x_{i,2},\cdots,x_{i,t-3})$，从公告牌上下载 $(x_{i,t-2},x_{i,t-1})$，生成一点：$B_i(x_{i,1},x_{i,2},\cdots,x_{i,t-1})$，该点便是 P_i 的影子。计算 $g(\sum_{j=1}^{t-1}x_{i,j}(\bmod p))$，如果与公告牌上的 h_i 相同，表示 P_i 提交了正确的信息。

然后，秘密恢复者得到了不少于 t 个点，任取其中的 t 个点，设为 $B_1(x_{1,1},x_{1,2},\cdots,x_{1,t-1})$，$B_2(x_{2,1},x_{2,2},\cdots,x_{2,t-1})$，$\cdots$，$B_t(x_{t,1},x_{t,2},\cdots,x_{t,t-1})$，通过以下步骤将共享秘密恢复出来：

(1)设 $t-1$ 维空间圆的圆心为 $O(c_1,c_2,\cdots,c_{t-1})$，半径平方为 R，则圆方程为：

$$\sum_{i=1}^{t-1}(x_i-c_i)^2=R(\bmod p) \tag{1}$$

(2)将 $B_1,B_2,\cdots,B_t$ 的坐标代入以上的圆方程(1)，得到 t 个方程组成的方程组：

$$\left.\begin{array}{l}\sum_{i=1}^{t-1}(x_{1,i}-c_i)^2=R(\bmod p)\\ \sum_{i=1}^{t-1}(x_{2,i}-c_i)^2=R(\bmod p)\\ \cdots\cdots\\ \sum_{i=1}^{t-1}(x_{t-1,i}-c_i)^2=R(\bmod p)\\ \sum_{i=1}^{t-1}(x_{t,i}-c_i)^2=R(\bmod p)\end{array}\right\} \tag{2}$$

(3)对以上的式(2)进行化简，可得到式(3)。

$$\left.\begin{array}{l}2\sum_{i=1}^{t-1}(x_{2,i}-x_{1,i})c_i=\sum_{i=1}^{t-1}x_{2,i}^2-\sum_{i=1}^{t-1}x_{1,i}^2(\bmod p)\\ \cdots\cdots\\ 2\sum_{i=1}^{t-1}(x_{t,i}-x_{t-1,i})c_i=\sum_{i=1}^{t-1}x_{t,i}^2-\sum_{i=1}^{t-1}x_{t-1,i}^2(\bmod p)\end{array}\right\} \tag{3}$$

由方程组(2)中任何两个方程相减后产生 C_t^2 个线性方程，式(3)是其中的一个极大线性无关组，由于 $B_1,\cdots,B_t$ 不在同 $t-2$ 维空间中，由定理1知这 t 个点必定能确定一个 $t-1$ 维圆。方程组(3)是含 $t-1$ 个方程的 $t-1$ 元线性方程组，c_1，$c_2,\cdots,c_{t-1}$ 为未知数，该方程组有唯一解，获得该圆的圆心 $(c_1,c_2,\cdots,c_{t-1})$。将圆心的值代入式(2)中的任意一个式子，可求出 R。即：

$$D=\det\begin{bmatrix} x_{2,1}-x_{1,1} & x_{2,2}-x_{1,2} & \cdots & x_{2,t-1}-x_{1,t-1} \\ x_{3,1}-x_{2,1} & x_{3,2}-x_{2,2} & \cdots & x_{3,t-1}-x_{2,t-1} \\ & \cdots & \cdots & \\ x_{t,1}-x_{t-1,1} & x_{t,2}-x_{t-1,2} & \cdots & x_{t,t-1}-x_{t-1,t-1} \end{bmatrix} (\mathrm{mod}\ p) \tag{4}$$

$$c_1=\det\begin{bmatrix} \sum_{i=1}^{t-1}x_{2,i}^2-\sum_{i=1}^{t-1}x_{1,i}^2 & x_{2,2}-x_{1,2} & \cdots & x_{2,t-1}-x_{1,t-1} \\ \sum_{i=1}^{t-1}x_{3,i}^2-\sum_{i=1}^{t-1}x_{2,i}^2 & x_{3,2}-x_{2,2} & \cdots & x_{3,t-1}-x_{2,t-1} \\ & \cdots & \cdots & \\ \sum_{i=1}^{t-1}x_{t,i}^2-\sum_{i=1}^{t-1}x_{t-1,i}^2 & x_{t,2}-x_{t-1,2} & \cdots & x_{t,t-1}-x_{t-1,t-1} \end{bmatrix} \times \frac{(-1)^{(1+1)}}{2D}(\mathrm{mod}\ p) \tag{5}$$

当 $1<i<t-1$ 时，c_i 通过式(6)求得：

$$c_i=\det\begin{bmatrix} \sum_{j=1}^{t-1}x_{2,j}^2-\sum_{j=1}^{t-1}x_{1,j}^2 & x_{2,1}-x_{1,1} & \cdots & x_{2,i-1}-x_{1,i-1} & x_{2,i+1}-x_{1,i+1} & \cdots & x_{2,t-1}-x_{1,t-1} \\ \sum_{j=1}^{t-1}x_{3,j}^2-\sum_{j=1}^{t-1}x_{2,j}^2 & x_{3,1}-x_{2,1} & \cdots & x_{3,i-1}-x_{2,i-1} & x_{3,i+1}-x_{2,i+1} & \cdots & x_{3,t-1}-x_{2,t-1} \\ & & \cdots & \cdots & & & \\ \sum_{j=1}^{t-1}x_{t,j}^2-\sum_{j=1}^{t-1}x_{t-1,j}^2 & x_{t,1}-x_{t-1,1} & \cdots & x_{t,i-1}-x_{t-1,i-1} & x_{t,i+1}-x_{t-1,i+1} & \cdots & x_{t,t-1}-x_{t-1,t-1} \end{bmatrix} \times \frac{(-1)^{(i+1)}}{2D}(\mathrm{mod}\ p) \tag{6}$$

$$c_{t-1}=\det\begin{bmatrix} \sum_{i=1}^{t-1}x_{2,i}^2-\sum_{i=1}^{t-1}x_{1,i}^2 & x_{2,1}-x_{1,1} & \cdots & x_{2,t-2}-x_{1,t-2} \\ \sum_{i=1}^{t-1}x_{3,i}^2-\sum_{i=1}^{t-1}x_{2,i}^2 & x_{3,1}-x_{2,1} & \cdots & x_{3,t-2}-x_{2,t-2} \\ & \cdots & \cdots & \\ \sum_{i=1}^{t-1}x_{t,i}^2-\sum_{i=1}^{t-1}x_{t-1,i}^2 & x_{t,1}-x_{t-1,1} & \cdots & x_{t,t-2}-x_{t-1,t-2} \end{bmatrix} \times \frac{(-1)^{(t-1+1)}}{2D}(\mathrm{mod}\ p) \tag{7}$$

$$R=\sum_{i=1}^{t-1}(x_{1,i}-c_i)^2(\mathrm{mod}\ p) \tag{8}$$

(4) $s=R$ 就是共享的秘密。

2.4 参与者的加入

当有新参与者 P_{n+1} 加入时，秘密分发者为 P_{n+1} 分配伪影子和影子：

(1)为 P_{n+1} 选取一个伪影子 $s_{n+1}\in(0,p)$，通过安全信道交给 P_{n+1}；

(2)利用与为 P_i 取 B_i 点相同的方法，为 P_{n+1} 在圆 Ω 上取点 $B_{n+1}(x_{n+1,1},x_{n+1,2},\cdots,x_{n+1,t-1})$ 作为 P_{n+1} 的影子；计算 $h_{n+1}=g(\sum_{j=1}^{t-1}x_{n+1,j}(\mathrm{mod}\ p))$；

(3)将 h_{n+1}，$(x_{n+1,t-2},x_{n+1,t-1})$ 公布于公告牌上。

2.5 参与者的退出

假设参与者 P_j 退出，必须更新圆 Ω，使 B_j 不在其上，从而使得 P_j 不再能够参与秘密恢复。圆的参数含圆心与半径，由于圆半径平方是秘密 s，故不变，只能改变圆 Ω 的圆心坐标。然后，秘密分发者为所有未退出的参与者重新计算影子并更新其公布于公告牌上的信息：$\{h_i,(x_{i,t-2},x_{i,t-1})\mid i=1,2,\cdots,j-1,j+1,\cdots,n)\}$。过程如下：

(1)随机生成 $t-1$ 个数：$c_1',c_2',\cdots,c_{t-1}'\in(0,p)$，以 $O'(c_1',c_2',\cdots,c_{t-1}')$ 为圆心、s 为半径平方确定圆 Ω'：$\sum_{i=1}^{t-1}(x_i-c_i')^2=s(\mathrm{mod}\ p)$；

(2)秘密分发者为除了 P_j 以外的所有参与者更新影子，以 P_i 为例：利用与秘密分配阶段为 P_i 取 B_i 点相同的方法，为 P_i 在圆 Ω' 上取点 $B_i'(x_{i,1},x_{i,2},\cdots x_{i,t-3},x_{i,t-2}',x_{i,t-1}')$；计算 $h_i'=g((\sum_{k=1}^{t-3}x_{i,k})+x_{i,t-2}'+x_{i,t-1}'(\mathrm{mod}\ p))$；

(3)公告牌上的相应信息更新为：$\{h_i',(x_{i,t-2}',x_{i,t-1}')\mid i=1,2,\cdots,j-1,j+1,\cdots,n)\}$，并删除退出者 P_j 的相关信息。

显然，参与者退出时，只需秘密分发者计算并更新公告牌上的信息，各参与者保留自己原有的秘密(伪影子)，不必要作任何的更新。

2.6 改变门限值 t

假设将(t,n)改变为(t',n)，由于 t 的改变导致了以共享秘密为半径平方的圆所处的空间维数发生了变化。所有的参与者仍然不需对自己的伪影子作任何改变，只需要秘密分发者做如下操作即可：

(1)随机生成 $t'-1$ 个数：$c_1'',c_2'',\cdots,c_{t'-1}''\in(1,p)$，以 $O'(c_1'',c_2'',\cdots,c_{t'-1}'')$ 为圆心、s 为半径平方确定圆 Ω''：$\sum_{i=1}^{t'-1}(x_i-c_i'')^2=s(\mathrm{mod}\ p)$；

(2)为所有参与者计算影子，以 P_i 为例：利用与秘密分配阶段为 P_i 在圆 Ω 上取 B_i 点相同的方法，根据 s_i，r 与 Ω'' 的值，为 P_i 在圆 Ω'' 上取点 $B_i''(x_{i,1},x_{i,2},\cdots,x_{i,t'-3},x_{i,t'-2},x_{i,t'-1})$，计算 $h_i''=g(\sum_{j=1}^{t'-1}x_{i,j}(\mathrm{mod}\ p))$；

(3)更新公告牌上相应的信息为：$\{h_i'',(x_{i,t'-2},x_{i,t'-1})\mid i=1,2,\cdots,n)\}$，同时更新 t 为 t'。

2.7 共享秘密 s 的改变

当共享秘密改变为 s' 时，首先秘密圆的方程变为：$\sum_{i=1}^{t-1}(x_i-c_i)^2=s'(\mathrm{mod}\ p)$，然而秘密分发者为所有参与者更新影子，最后更新公告牌上各个参与者影子公开的部分以及影子的杂凑值即可。具体方法与秘密分配阶段秘密分发者为各个参与者分配影子的方法相同。

3 安全性与性能分析

在本文的方案中，公告牌上公布每个参与者影子的点坐标的最后两个值，则至少还有一个坐标是由参与者的伪影子

所决定的，否则参与者的影子就全部暴露，因此秘密圆所在空间的维数至少是3维，所以上面所提出的方案适用于$t\geqslant 4$的情况。为了使以上的方案适用于$t=2,3$的情况，需要在公布牌上添加一些点的信息。当$t=2$时，秘密分配阶段构造3维的圆Ω，则需要在公告牌公布圆上任意两个点，由两个参与者处得到两个点、公告牌上的两点共计4个点，则可以重构3维空间中的圆，恢复秘密；而$t=3$时，只需在公告牌公布圆上任意一个点即可。这样，本文的方案可适用于任意$t>1$情况下的(t,n)门限秘密共享。

3.1 安全性分析

3.1.1 提供安全(t,n)门限秘密共享

从定理1知方案中任意t个或多于t个参与者能合作恢复秘密s。以下命题1证明任意少于t个的参与者不能恢复秘密。

命题1 $t-1$维空间中少于t个点不能唯一确定一个圆，从而少于t个参与者不能恢复秘密。

证明：由于不足t个参与者提交影子时，最多只能产生$t-1$维空间中的$t-1$个点。采用反证法，假设少于t个点也能唯一确定一个$t-1$维空间圆，不妨设$t-1$个点$B_1,B_2,\cdots,B_{t-1}$唯一确定一个圆，记为Ω_1，选取不在Ω_1上的空间一个点W，并且$B_1,B_2,\cdots,B_{t-1},W$不同在$t-2$维空间。由定理1知$B_1,B_2,\cdots,B_{t-1},W$唯一确定一个圆，记为Ω_2。由于W不在Ω_1上，故$\Omega_1\neq\Omega_2$，但$B_1,B_2,\cdots,B_{t-1}$既在Ω_1上又在Ω_2上，与$B_1,B_2,\cdots,B_{t-1}$唯一确定一个$t-1$维空间圆矛盾。所以，少于t个点不能唯一确定一个$t-1$维空间圆。

由于少于t个参与者所能提供的点个数少于t个，故不能恢复秘密。证毕。

命题2 由公告牌上的信息$\{(x_{i,t-2},x_{i,t-1})\mid i=1,2,\cdots,n)\}$不能推出共享秘密。

证明：公告牌上的$\{(x_{i,t-2},x_{i,t-1})\mid i=1,2,\cdots,n)\}$是$n$个参与者的影子的最后个坐标值，它由圆$\Omega$方程与影子的前$t-3$个坐标值推算出来。现在要反推导，将无法推导出影子的前$t-3$个坐标值，则参与者的影子不会泄露，故无法由公告牌上的公开信息推出共享秘密。证毕。

3.1.2 防止欺骗

命题3 本文方案防参与者欺骗。

证明：由于在公告牌上有每个参与者影子的单向杂凑函数值，如果某参与者所提交的影子的前$(t-3)$个坐标值有错误时，秘密恢复者对该参与者所提交影子的前$(t-3)$个坐标值与公告牌上公布的最后两个坐标值求和之后再求其单向杂凑函数值，结果将不等于公告牌相应的值，则可检查出该参与者提交了错误的数据。证毕。

3.2 计算性能与存储需求分析

当有参与者加入与退出、或门限值t变化时，其它参与者的伪影子无需任何变化、无任何运算要求。

当需要在相同的参与者集合中共享下一个秘密时，只需要秘密分发者修改随机数r，为所有的参与者计算相对这个新秘密的影子$\{(x_{i,t-2},x_{i,t-1})\mid i=1,2,\cdots,n)\}$，参与者仍只需持有原来的伪影子，当其参与秘密恢复时，通过新的r与伪影子来产生参与恢复新秘密的新影子，该新影子已随着公开参数r的变化而变化。所以，系统可以在参与者持有的伪影子不变的情况下不断地共享新的秘密。

本文方案中有一个发布公共信息的公告牌，故需要一定的存储空间（如表1所列），$|p|$表示p的二进制位数。

表1 公告牌的存储需求

公告牌上的对象	存储空间（单位：bit）
r	$\|p\|$bit
n个参与者的公开信息	$3n\times\|p\|$bit

公告牌上还有对函数g与f的描述，未列入表1中。

除了公告牌的信息之外，秘密分发者还应该秘密保存每个参与者的伪影子，即需要$n\times|p|$bit。而每个参与者需要保存的仅仅是自己的伪影子，故需$|p|$bit的存储空间。

3.3 实验数据与分析

3.3.1 实验环境

通过JAVA语言实现了上面所述方案与Shamir方案，所有的运算定义于有限域$GF(p)$上。硬件环境是CPU频率为2.5GHz，内存为512MB，操作系统为Window XP的7台机器，开发工具是JDK版本是1.5，采用Eclipes-SKD-3.0.1的集成工具。一台机器运行秘密分发者应用程序，另一台机器运行秘密恢复者应用程序，其余的机器运行参与者应用程序。网络环境为支持TCP/IP协议的校园网。

3.3.2 实验数据

表2、表3与表4的数据是通过100次实验取平均值。表4中时间消耗指秘密分配和重构的时间总和。

表2 分配单个影子的时间消耗（单位：毫秒）

$\|p\|=64$	$\|p\|=128$	$\|p\|=256$	$\|p\|=512$	$\|p\|=1024$
2	3	6	19	113

表3 秘密恢复时间消耗（单位：毫秒）

t的值	p的二进制位数				
	64	128	256	512	1024
t=3	1.7	2	2	3	7
t=6	3	4	6	10	26
t=12	7	11	20	46	128
t=18	17	27	52	120	340
t=24	31	54	105	245	737
t=30	53	91	183	434	1305

表4 本文方案与Shamir方案实现(3,5)门限秘密共享时间消耗之比较（单位：毫秒）

方案	p的二进制位数			
	128	256	512	1024
本文方案	17	32	98	572
Shamir方案	125	217	785	16017

3.3.3 分析

表2与表3分别描述了本文方案的秘密分配、秘密恢复的时间消耗。表2表示分配一个影子在$|p|$取不同值时所需的时间，例如$|p|=1024$bit时，分配一个影子所需的时间需0.113秒。表3显示(t,n)门限的秘密恢复时间消耗，在秘密恢复阶段构造的方程组(3)是含$t-1$个方程的$t-1$元线性方程组，显然解方程组(3)时t越大则需要越多的时间，当$t=30,|p|=1024$时，时间消耗1.305秒。表4显示了本文方案与Shamir方案在实现(3,5)门限秘密共享的时间消耗比较（包括秘密的分配与重构），显然与本文方案相比shamir方案的时间消耗更多、随$|p|$的增大有更快的时间消耗增长速度，在$|p|=1024$bit时，Shamir方案的时间消耗大约是本文方案的28倍。

结束语 本文利用圆的几何特性、双变量杂凑函数提出了一个(t,n)门限秘密共享方案，与文献[9-12]的方案相比，

本文方案的秘密分发简单、参与者需要保存的伪影子仅是一个$(0,p)$上的数而非一个多维空间点，该伪影子秘密可以长期使用，参与者利用其伪影子与公共参数r计算其影子；当秘密分发者想更改参与者的影子时，只需更新公告牌上的公开信息即可，可见其秘密分发效率高。

本文方案还具有如下特点：1)它是一个动态的方案，可动态实现参与者的加入与退出，步骤简单，还可以动态改变门限值t；2)运算高效，在$|p|=1024$bit、实现(3,5)门限共享时，Shamir方案的时间消耗约是本文方案的28倍；3)在系统参数变化时，例如参与者的加入/退出、t的改变、甚至是共享秘密的修改等，用户所持有的伪影子一直保持不变；4)在同一个参与者集合中，参与者可以使用同一个伪影子多次共享秘密；5)方案是一个安全的(t,n)门限秘密共享方案；6)方案动态变化时，秘密分发者与参与者之间无通信量的需求。

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 R. Safeguarding cryp tograph ic keys [C]// Proceedings of National Computer Conference. Montvale, NJ: AFIPS Press, 1979, 48: 313-317

[3] Stadler M. Publicly verifiable secret sharing [C]// Proc. of Advances in Cryptology —Eurocrypt'96. Berlin: Springer-Verlag, 1996: 190-199

[4] Asmuth C, Bloom J. A modular approach to key safeguarding [J]. IEEE Trans on Information Theory, 1983, 29 (2): 208-210

[5] Chang T Y, Hwang M S, et al. An improvement on the Lin-Wu (t,n) threshold verifiable multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2005, 163(1): 169-178

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

[7] 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

[8] Chien H Y, Jan J K, Tseng Y M. A practical (t, n) multi-secret sharing scheme [J]. IEICE Trans on Fundamentals, 2000, E83-A (12): 2762-2765

[9] Wu T C, He W H. A geometric approach for sharing secrets [J]. Computer & Security, 1995, 14(2): 135-145

[10] Chor L P, Jing H W, Chong T P. A geometric approach for shared secrets, a refinement [J]. Computers & Security, 1998, 17 (10): 725-732

[11] 庞辽军，王育民. 一个基于几何性质的(t,n)多重秘密共享方案[J]. 西安交通大学学报，2005，39(4)：425-428

[12] 庞辽军，李慧贤，王育民. 基于几何性质一般访问结构上的多重秘密共享方案[J]. 计算机科学，2006，33(10)：90-93

(上接第91页)

RENO流的价格映射函数：$m_l^2(p_l)=(p_l c_l-\underline{b}_l)/(K_l(\bar{b}_l-\underline{b}_l))$

所以价格映射函数矩阵$\dot{m}^1$为单位阵，$\dot{m}_l^2=c_l/(K_l(\bar{b}_l-\underline{b}_l))$。

由式(15)和式(23)知：要保证图1网络平衡点唯一性，价格映射函数(RED参数设置)应满足：

$\dot{m}_1^2\dot{m}_2^1\dot{m}_3^1+\dot{m}_1^1\dot{m}_2^1\dot{m}_3^2>\dot{m}_1^1\dot{m}_2^2\dot{m}_3^1$，将上式代入得：

$$\frac{c_1}{k_1(\bar{b}_1-\underline{b}_1)}+\frac{c_3}{k_3(\bar{b}_3-\underline{b}_3)}>\frac{c_2}{k_2(\bar{b}_2-\underline{b}_2)} \tag{24}$$

结束语 虽然标准的效用函数最大化方法已无法解决具有多协议多瓶颈链路的网络拥塞控制问题。但在引入价格映射函数及满足适当设计条件后重新找到解决网络平衡点存在性、延迟相关和全局唯一性的问题的方法。在得到网络全局唯一平衡点后进一步研究工作应该包括两个方面：(1) 多协议多瓶颈链路的网络拥塞控制在平衡点附近的全局稳定性问题。(2)平衡点唯一性表示多协议数据流带宽分配的唯一性，所以瓶颈链路带宽的公平性分配问题也值得研究。

参 考 文 献

[1] Misra V, Gong W B, Towsley D. Fluid-based Analysis of a Network of AQM Routers Supporting TCP Flows with an Application to RED [C]// Proceedings of ACM/SIGCOMM. 2000: 151-160

[2] Hollot C V, Misra V, Towsley D, et al. A control theoretic analysis of RED[C] // Proceedings of IEEE INFOCOM. 2003, 5: 1510-1519

[3] Kim K B. Design of Feedback Control Supporting TCP Based on the State-Space Approach [J]. IEEE TRANS on Automatic Control, 2006, 51(7): 1086-1098

[4] Tan Liansheng, Zhang Wei, Peng Gang, et al. Stability of TCP/RED systems in AQM Routers [J]. IEEE TRANS Automatic Control, 2006, 51(8): 814-871

[5] Kelly F, Maoulloo A, Tan D. Rate control for communcation networks: shadow prices, proport -ional fairness and stability [J]. Oper. Res. Soc., 1998, 49: 237-252

[6] Low S H. A duality model of TCP and queue management algorithms[J]. IEEE/ACM Trans. Networking, 2003, 11(4): 525 -536

[7] Lei Ying, Dullerud G E, Srikant R. Global stability of internet congestion controllers with heterogeneous delays [J]. IEEE/ACM Trans. Networking, 2006, 14(3): 579-592

[8] Zhang Yueping, Kang S-R, Loguinov D. Delay-Independent Stability and Performance of Distributed Congestion Control [J]. IEEE/ACM Trans. Networking, 2007, 15(5): 838-852

[9] Wang Zhikui, Paganini F. Boundedness and Global Stability of a Nonlinear Congestion Control With Delays[J]. IEEE Automatic Control, 2006, 51(9): 1514-1517

[10] Tang A, Wang J, Low S H, et al. Network equilibrium of heterogeneous congestion control protocols[C] // Proc. IEEE INFOCOM. 2005: 1338-1349

[11] Tang A, Wang J, Low S H, et al. Equilibrium of heterogeneous congestion control protocols. Dept. Comput. Sci., California Inst. Technol., Pasadena, CSTR: 2005. 005, 2005

[12] Tang A, Wang J, Hedge S, et al. Equilibrium and fairness of networks shared by TCP Reno and Vegas/FAST [J]. Telecomm. Syst., 2005, 30(4): 417-439

[13] Tang A, Wei D, Low S H, et al. Heterogeneous congestion control: Efficiency, fairness and design [C] // Proc. IEEE ICNP. 2006: 127-136

[14] Wei D, Jin C, Low S H, et al. FAST TCP: Motivation, architecture, algorithms, performance [J]. IEEE/ACM Trans. Netw., 2007, 15(6): 1246-1259

[15] Dutta D, goel A. Oblivious AQM and Nash Equilibria [J]. IEEE INFOCOM, 2003, 3: 1311-1318

[16] Aranson S, Belisky G. Introduction to the Qualitative Theory of Dynamical System on Surfaces [J]. Translation of Mathematical Monograhs, 1996, 153(6): 123-128