一种无可信中心动态秘密共享方案*

何二庆，侯整风，朱晓玲
（合肥工业大学 计算机与信息学院，合肥 230009）

摘　要：现有的无可信中心动态秘密共享方案，尚未对新增成员秘密份额的动态更新问题作相关研究，在很大程度上降低了秘密共享系统的安全性。针对这一缺陷进行研究，提出了一种新的无可信中心动态秘密共享方案，在不暴露原秘密的情况下，成员可以协同交互，动态地更新各自的秘密份额，增加新成员，且新增成员也可以与其他成员协同参加下一轮秘密份额的动态更新。

关键词：可信中心；秘密份额；动态更新；新增成员
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2013)02-0491-03
doi:10.3969/j.issn.1001-3695.2013.02.047

Proactive secret sharing scheme without trusted party

HE Er-qing, HOU Zheng-feng, ZHU Xiao-ling
(*School of Computer & Information*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: Some existing secret sharing schemes have not researched the proactive refreshment of new members' secret shares, which greatly reduced the security of the secret sharing system. Against this defect researched, this paper put forward a new proactive secret sharing scheme without trusted part, without exposing the original secret, all members can interact collaboratively, refresh their secret shares proactively, and add new members. What's more, new members could also proactively refresh their secret shares with other members at next time period.

Key words: trusted party; secret sharing; proactive refreshment; new members

随着计算机和网络技术的迅速发展及普及，网络安全日益引起人们的关注。应用需求的多样化、复杂化使得密码学理论和网络安全技术也从最初意义上的单人模式扩展到更为广泛的领域。门限秘密共享改变了传统的单人加密、签名和认证模式，能够分散责任，提高系统的安全性、可靠性和健壮性，成为保障信息安全的重要手段之一。

1979 年，Shamir[1] 提出了基于 Lagrange 插值公式的 (t,n) 门限秘密共享方案，同年，Blakley[2] 提出了基于射影定理的门限秘密共享方案，1985 年 Asmuth 等人[3] 提出了基于中国剩余定理的秘密共享方案。传统秘密共享方案的基本思想是将共享秘密分割成 n 个秘密份额分发给 n 个成员，t 个或 t 个以上成员协同合作能够恢复秘密，而少于 t 个则无法恢复。1987 年 Feldman[4] 提出了一种基于 Lagrange 插值多项式的非交互式可验证秘密共享方案，也是第一个非交互式可验证秘密共享方案。1991 年 Pedersen[5] 对 Feldman 的方案进行改进，结合同态承诺提出了一个更高效的、可靠的非交互式可验证秘密共享方案，但这些方案都无法解决分发者的权威欺骗问题。

1991 年，Ingemarsson 等人[6] 提出了一种无可信中心的秘密共享方案，方案无须可信中心，t 个或者 t 个以上参与者相互合作即可恢复秘密，有效地解决了可信中心的权威欺骗行为。1994 年 Harn[7] 提出了一种无可信中心的门限群签名方案，方案的群签名和群公钥由参与者协同完成。无可信中心秘密共享解决了权威欺骗问题，提高了系统的安全性，因此得到广泛的研究[8~10]。1991 年 Ostrovsky 等人[11] 提出了移动敌手和动态秘密共享的概念，参与者周期性地产生一份新的秘密份额替换旧的秘密份额，使得移动敌手在前一周期内获得的信息完全无效，从而提高了系统的安全性。1995 年 Herzberg 等人[8] 对动态秘密进行研究，给出了动态秘密共享的具体实现方案。文献[9]提出了一个基于无可信中心动态秘密共享的身份认证方案，方案在无须可信中心的环境下，系统 t 个诚实成员协同为用户创建公钥证书。文献[12]提出了一种无可信中心可动态删除成员的秘密共享方案，由于动态秘密共享的安全性、健壮性、可用性都很高，其研究与应用广泛[12~15]。

尽管现有的动态秘密共享方案[12,15] 解决了成员增加和成员删除的问题，但没有考虑新增成员秘密份额的动态更新问题。本文基于 PKI(public key infrastructure)应用，提出了一种新的无可信中心动态秘密共享方案，有效地解决了新增成员份额的动态更新问题，t 个或者 t 个以上诚实成员在不泄露秘密份额的情况下能够相互合作，动态地更新秘密份额，提高系统的安全性。

1　无可信中心的动态秘密共享方案

1.1　方案概述

本文提出的无可信中心动态秘密共享方案是基于多 CA (certification authority)的公钥认证系统。在本方案中，CA 是由 n 个成员组成，成员互相合作产生各自的秘密份额，协同为用

收稿日期：2012-06-30；**修回日期**：2012-08-08　**基金项目**：安徽省自然科学基金资助项目(090412051)；广东省教育部产学研结合项目(2008B0905002400)

作者简介：何二庆(1988-)，女，安徽芜湖人，硕士研究生，主要研究方向为密码学、网络安全(heerqing@126.com)；侯整风(1958-)，男，教授，硕导，主要研究方向为计算机网络、信息安全；朱晓玲(1974-)，女，博士研究生，主要研究方向为信息安全、无线自组织网络.

户产生公钥证书,用户 U_A 向 CA 申请公钥证书,用户 U_B 验证 U_A 的证书;此外,成员可以动态地更新自身秘密份额,增加新成员,且新增成员也可以动态更新自身秘密份额。该系统框架如图 1 所示。

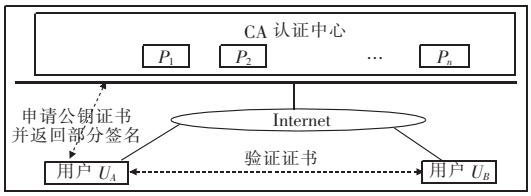

图 1 系统框架

1.2 初始化

设系统成员为 $P=\{P_1,P_2,\cdots,P_n\}$,成员标志符为 ID_i,且公开。公开参数 p、q、g,其中 p 和 q 都是大素数,且 q 是 $p-1$ 的素因子,g 是 $\mathrm{GF}(p)$ 上的 q 阶生成元,成员 $P_i\in P$ 的私钥为 d_i,公钥 $y_i=g^{d_i} \bmod p$。

a)在初始化时,每个成员 $P_i\in P$ 运用私钥 d_i 产生一个 $t-1$ 维的秘密多项式 $f_i(x)$,其中随机系数 $\{a_{i,k}\mid k=1,2,\cdots,t-1\}\in|Z_q^*|$。

$$f_i(x)=d_i+a_{i,1}x+\cdots+a_{i,t-1}x^{t-1} \bmod q \tag{1}$$

P_i 计算秘密的影子 $f_i(\mathrm{ID}_j)$,为保证安全性,P_i 用私钥 d_i 对其签名 $\mathrm{SIG}_i(f_i(\mathrm{ID}_j))$,然后将签了名的 $f_i(\mathrm{ID}_j)$ 发送给 P_j,保留 $f_i(\mathrm{ID}_i)$,公开参数 $\{g^{a_{i,k}}\mid k=1,2,\cdots,t-1\}$。

b)当成员 P_j 接收到 P_i 秘密的影子 $f_i(\mathrm{ID}_j)$ 时,验证其正确性:

$$g^{f_i(\mathrm{ID}_j)}=g^{d_i}\cdot(g^{a_{i,1}})^{\mathrm{ID}_j}\cdot\cdots\cdot(g^{a_{i,t-1}})^{\mathrm{ID}_j^{t-1}} \bmod p \tag{2}$$

如果式(2)成立,则 P_j 接收 $f_i(\mathrm{ID}_j)$,否则 P_j 拒绝接收。

c)当 P_j 接收到其他所有诚实成员正确的影子时,通过式(3)计算自身的秘密份额:

$$F(\mathrm{ID}_j)=\sum_{i=1}^{n}f_i(\mathrm{ID}_j) \bmod q \tag{3}$$

然后广播 $g^{F(\mathrm{ID}_j)} \bmod p$。

d)根据 Shamir[1] 的 (t,n) 门限秘密共享方案,每个成员通过 Lagrange 插值公式计算 CA 的公钥:

$$y=g^{F(0)} \bmod p=g_i^{\sum_{i=1}^{t}F(\mathrm{ID}_i)}\prod_{j=1,j\neq i}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j} \bmod q \bmod p \tag{4}$$

1.3 证书创建与验证

当用户 U_A 向 CA 申请公钥证书时,需要向 CA 中所有成员广播自身信息 $C=(\mathrm{ID}_A\parallel y_A\parallel \mathrm{otherInfo})$,其中,$\mathrm{ID}_A$ 是 U_A 的唯一标志,$y_A(y_A=g^{X_A} \bmod p)$ 是 U_A 的公钥,CA 中 t 个或者 t 个以上成员协同为 U_A 创建公钥证书。不失一般性,定义任意 t 个成员为 $W=\{P_1,P_2,\cdots,P_t\}$。

a)每个成员 $P_i\in W$ 选择一个随机数 $k_i\in|Z_q^*|$,然后广播 $r_i=g^{k_i} \bmod p$。

b)每个成员 P_i 对信息 C 生成自己的部分签名 (r,s_i):

$$r=g_i^{\sum_{i=1}^{t}k_i} \bmod p=\prod_{i=1}^{t}g^{k_i} \bmod p=\prod_{i=1}^{t}r_i \bmod p \tag{5}$$

$$s_i=k_i\cdot C+r\cdot F(\mathrm{ID}_i)\prod_{j=1,j\neq i}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j} \bmod q \tag{6}$$

然后发送 (C,r,s_i) 给 U_A。

c)当 U_A 接收到 t 个来自 W 的部分签名后,U_A 计算群签名:

$$s=C\sum_{i=1}^{t}k_i+r\cdot F(0) \bmod q=\sum_{i=1}^{t}s_i \bmod q \tag{7}$$

(C,r,s) 就是用户 U_A 的公钥证书。

d)当用户 U_B 接收到 U_A 的证书后,由式(8)验证其正确性。

$$g^s\equiv r^C\cdot y^r \bmod p \tag{8}$$

如果式(8)成立,验证成功。

$$g^s\equiv g^{C\cdot\sum k_i+r\cdot F(0)} \bmod p\equiv g^{C\cdot\sum k_i}\cdot g^{r\cdot F(0)} \bmod p\equiv r^C\cdot y^r \bmod p$$

1.4 份额更新

为了提高系统的安全性,成员需要定期更新秘密份额。设更新周期为 $T=\{1,2,3,\cdots\}$。

a)在更新周期 T 开始时,每个成员 $P_i(i=1,\cdots,n)$ 随机选择一个常数项为零的 $t-1$ 维多项式,随机系数 $\{c_{i,k}\mid k=1,2,\cdots,t-1\}\in|Z_q^*|$:

$$\delta_i(x)=c_{i,1}x+\cdots+c_{i,t-1}x^{t-1} \tag{9}$$

P_i 计算出 $\delta_i(\mathrm{ID}_j)$,并将 $\delta_i(\mathrm{ID}_j)$ 发送给 P_j,公开参数 $\{g^{c_{i,k}} \bmod p\}$。

b)当 P_j 接收到 P_i 发送来的 $\delta_i(\mathrm{ID}_j)$ 后,通过式(10)验证其正确性:

$$g^{\delta_i}(\mathrm{ID}_j)=(g^{c_{i,1}})^{\mathrm{ID}_j}\cdot\cdots\cdot(g^{c_{i,t-1}})^{\mathrm{ID}_j^{t-1}} \bmod p \tag{10}$$

如果式(10)成立,P_j 接收 $\delta_i(\mathrm{ID}_j)$,否则拒绝接收。

c)当 P_j 接收到其他所有诚实成员正确的 $\delta_i(ID_j)$ 后,通过式(11)计算更新多项式值。

$$\delta(\mathrm{ID}_j)=\sum_{i=1}^{n}\delta_i(\mathrm{ID}_j) \bmod q \tag{11}$$

最后计算新的秘密份额并广播 $g^{F^T(\mathrm{ID}_j)} \bmod p$:

$$F^{\mathrm{T}}(\mathrm{ID}_j)=F^{T-1}(\mathrm{ID}_j)+\delta(\mathrm{ID}_j) \bmod q \tag{12}$$

d)当诚实成员 P_j 通过式(10)检测到 P_i 错误的 $\delta_i(\mathrm{ID}_j)$ 时,按如下方法删除成员 P_i:首先将 P_i 加入不诚实列表 E 中,广播 P_i 为不诚实成员,并广播 $\delta_i(\mathrm{ID}_j)$;其次,系统其他诚实成员收到消息后,根据式(9)重新选择多项式,然后将新产生的 $\delta_i(\mathrm{ID}_j)$ 发给除 E 集合外的所有诚实成员,直到接收到所有诚实成员正确的 $\delta_i(\mathrm{ID}_j)$ 后,计算新的更新多项式:

$$\delta(\mathrm{ID}_j)=\sum_{i=1,i\notin E}^{n}\delta_i(\mathrm{ID}_j) \bmod q \tag{13}$$

最后根据式(12)计算新的秘密份额:

$$F^{\langle T\rangle}(\mathrm{ID}_j)=F^T(\mathrm{ID}_j)+\delta(\mathrm{ID}_j) \bmod q=$$
$$F^T(\mathrm{ID}_j)+\sum_{i=1,i\notin E}^{n}\delta_i(\mathrm{ID}_j) \bmod q \tag{14}$$

1.5 增加新成员

设 D 为所有诚实成员的集合,P_r 为新增加成员,标志符为 ID_r。为了保证成员秘密份额不被泄露,当系统增加一个新成员 P_r 时,集合 D 中的成员将各自的影子秘密份额 $F'(\mathrm{ID}_j)$ 发送给新成员 P_r,P_r 通过接收到的影子秘密份额 $F'(\mathrm{ID}_j)$ 计算出自身的秘密份额 $F(\mathrm{ID}_r)$。

a)成员 $P_i\in D$ 随机地选择一个 $t-1$ 维多项式 $\theta_i(x)$,其中 $\{w_{i,k}\mid k=1,2,\cdots,t-1\}\in|Z_q^*|$ 且满足 $\theta_i(\mathrm{ID}_r)=0$。

$$\theta_i(x)=w_{i,0}+w_{i,1}x+\cdots+w_{i,t-1}x^{t-1} \bmod q \tag{15}$$

P_i 计算 $\theta_i(\mathrm{ID}_j)$,并将 $\theta_i(\mathrm{ID}_j)$ 发送给其他所有诚实成员 P_j,公开参数 $\{g^{w_{i,k}} \bmod p,k=0,1,\cdots,t-1\}$。

b)当 P_j 接收到 $\theta_i(\mathrm{ID}_j)$ 后,通过式(16)验证 $\theta_i(\mathrm{ID}_j)$ 的正确性:

$$g^{\theta_i}(\mathrm{ID}_j)=(g^{w_{i,1}})^{\mathrm{ID}_j}\cdot\cdots\cdot(g^{w_{i,t-1}})^{\mathrm{ID}_j^{t-1}} \bmod p \tag{16}$$

c)当 P_j 接收到所有成员正确的 $\theta_i(\mathrm{ID}_j)$ 后,计算自身的影子秘密份额:

$$F'(\mathrm{ID}_j)=(F(\mathrm{ID}_j)+\sum\theta_i(\mathrm{ID}_j)) \bmod p \tag{17}$$

然后将 $F'(\mathrm{ID}_j)$ 发送给 P_r。

d)P_r 接收到 t 个或 t 个以上的诚实成员的 $F'(\mathrm{ID}_i)$ 后,通

过 Lagrange 插值公式计算自身秘密份额 $F(\mathrm{ID}_r)$。

因为 $\sum\theta_j(\mathrm{ID}_r)=0$,得

$$F(\mathrm{ID}_r)=\sum_{i=1}^{t}(F(\mathrm{ID}_i)+\sum\theta_j(\mathrm{ID}_i))\prod_{j=1,j\neq i}^{t}\frac{\mathrm{ID}_r-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}\bmod q=\sum_{i=1}^{t}F'(\mathrm{ID}_i)\prod_{j=1,j\neq i}^{t}\frac{\mathrm{ID}_r-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}\bmod q \tag{18}$$

2　方案分析

2.1　份额更新

1)份额更新的有效性　本文 1.4 节中在成员秘密份额的动态更新过程中,式(9)是常数项为零的多项式,即 $\delta_i(0)=0$,保证了份额更新后系统原秘密不变,即 $F^T(0)=F^{T-1}(0)+0=\cdots=F(0)$,从而系统的公钥 $y=g^{F(0)}\bmod p$ 不变。

2)能够动态地删除成员　在 1.4 节中,当检测到不诚实成员 P_i 时,为了删除该成员,系统其他诚实成员需要立即协同更新各自的秘密份额,使得 P_i 的秘密份额失效,不能再参与用户证书的创建。由式(14)可知,不诚实成员 P_i 没有获得 $\delta(\mathrm{ID}_i)$,其秘密份额仍为 $F^{\mathrm{T}}(\mathrm{ID}_i)$,此时其他成员的秘密份额已经更新为 $F^{(T)}(\mathrm{ID}_j)=F^T(\mathrm{ID}_j)+\delta(\mathrm{ID}_j)\bmod q$,所以 P_i 的秘密份额已经失效,故份额的动态更新可以删除不诚实成员。

3)能够安全地增加新成员　在 1.5 节中,为了不泄露成员的秘密份额,当增加一个新成员时,系统其他诚实成员需要选择多项式,计算各自的影子秘密份额 $F'(\mathrm{ID}_j)$,如式(17)所示;然后将各自的影子秘密份额发送给新增成员。因此新增成员只能通过影子秘密份额计算自身的秘密份额,也就是说,新增成员在整个增加过程中并不知道其他成员的秘密份额,保证了份额不被泄露,提高了系统的安全性。

2.2　新增成员的有效性

1)新增成员参与用户证书的创建　设在当前更新周期,新增成员 P_r 与系统其他 $t-1$ 个诚实成员构成集合 $W=\{P_1,P_2,\cdots,P_{t-1},P_r\}$,为用户 U_A 创建公钥证书。

a)根据式(5)(6),成员 P_r 为消息 C 产生的部分签名记为 (r',s'_r),其中:

$$r'=g^{\sum_{i=1}^{t-1}k_i}\cdot g^{k_r}\bmod p=\prod_{i=1}^{t-1}g^{k_i}\cdot g^{k_r}\bmod p \tag{19}$$

$$s'_r=k_r\cdot C+r'\cdot F(\mathrm{ID}_r)\prod_{j=1,j\neq r}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_r-\mathrm{ID}_j}\bmod q \tag{20}$$

其余 $t-1$ 个诚实成员 P_i 为消息 C 产生的部分签名为 (r',s'_i),其中 r 同式(19),s'_i 如下:

$$s'_i=k_i\cdot C+r'\cdot F(\mathrm{ID}_i)\prod_{j=1,j\neq i}^{t-1}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}\cdot\frac{-\mathrm{ID}_r}{\mathrm{ID}_i-\mathrm{ID}_r}\bmod q$$

b)当用户 U_A 收到 t 个部分签名后,根据式(7)合成群签名 s,得到公钥证书 (C,r',s'),并将其发送给用户 U_B 验证。

$$s'=\sum_{i=1}^{t-1}s'_i+s'_r=C(\sum_{i=1}^{t-1}k_i+k_r)+r'\cdot(\sum_{i=1}^{t-1}F(\mathrm{ID}_i)\cdot\prod_{j=1,j\neq i}^{t-1}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}\cdot\frac{-\mathrm{ID}_r}{\mathrm{ID}_i-\mathrm{ID}_r}+F(\mathrm{ID}_r)\prod_{j=1,j\neq r}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_r-\mathrm{ID}_j})\bmod q$$

c)当 U_B 接收到 U_A 的签名 (C,r,s) 后,根据式(8)验证其正确性,验证过程如下:

$$g^{s'}=g^{C(\sum_{i=1}^{t-1}k_i+k_r)+r'\cdot(\sum_{i=1}^{t-1}F(\mathrm{ID}_i)\prod_{j=1,j\neq i}^{t-1}\frac{-\mathrm{ID}_j}{\mathrm{ID}_i-\mathrm{ID}_j}\cdot\frac{-\mathrm{ID}_r}{\mathrm{ID}_i-\mathrm{ID}_r}+F(\mathrm{ID}_r)\prod_{j=1,j\neq r}^{t}\frac{-\mathrm{ID}_j}{\mathrm{ID}_r-\mathrm{ID}_j})\bmod q}$$

$$\bmod p=g^{C(\sum_{i=1}^{t-1}k_i+k_r)}\cdot g^{r'\cdot F(0)}\bmod p\equiv r^C\cdot y^{r'}\bmod p \tag{21}$$

由此可知,新增加成员 P_r 在当前更新周期可以参与用户公钥证书的创建,即 P_r 的份额是有效的。

2)新增成员份额在下一周期是可更新的　设在下一个更新周期 T 时,新增成员 P_r 与系统其他所有诚实成员协同更新秘密份额,根据 2.1 节更新过程,P_r 更新后的秘密份额为

$$F^T(\mathrm{ID}_r)=F^{T-1}(\mathrm{ID}_r)+\delta(\mathrm{ID}_r)\bmod q \tag{22}$$

系统其他所有诚实成员更新后的秘密份额为

$$F^T(\mathrm{ID}_i)=F^{T-1}(\mathrm{ID}_i)+\delta(\mathrm{ID}_i)\bmod q \tag{23}$$

因此,新增加成员份额不仅是有效的,而且还可以周期性地、动态地更新秘密份额,提高了系统的安全性。

3　结束语

本文提出了一种新的无可信中心动态秘密共享方案,给出了成员份额的动态更新过程、用户公钥证书的创建、增加新成员以及删除成员等功能,很好地解决了新增成员秘密份额的动态更新问题;此外,新增成员秘密份额更新后仍可以参与公钥证书的创建,且可以与系统其他诚实成员在无可信中心环境下协同合作,剔除不诚实成员,有效地防止了移动敌手的攻击,因此该方案在一定程度提高了系统的安全性与实际应用价值,且为研究更高效的无可信中心动态秘密共享提供了坚实的基础。

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 [C]//Proc of National Computer Conference. Montvale:AFIPS Press,1979:313-317.

[3] ASMUTH C, BLOOM J. A modular approach to key safeguarding [J]. IEEE Trans on Information Theory,1983,29(2):101-105.

[4] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proc of the 28th IEEE Symposium on Foundations of Computer Science. 1987:427-437.

[5] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Proc of the 11th Annual International Conference on Advances in Cryptology. London: Springer-Verlag, 1991:129-140.

[6] INGEMARSSON I,SIMMONS G J. A protocol to set up shared secret schemes without the assistance of a mutually trusted party[C]//Proc of Workshop on Advances in Cryptology. 1991:266-282.

[7] HARM L. Group-oriented (t,n) threshold digital signature scheme and digital multisignature [J]. IEE Proceeding of Computer and Digital and Techniques,1994,141(5):307-313.

[8] HERZBERG A,JARECKI S,KRAWCZYK H,*et al*. Proactive secret sharing or:how to cope with perpetual leakage[C]//Proc of the 15th Annual International Conference on. London:Springer-Verlag,1995: 339-352.

[9] HOU Zheng-feng,HAN Jiang-hong,HU Dong-hui. A new authentication scheme based on proactive verifiable secret sharing[C]//Proc of Internetional Conference on Computer Science and Software Engineering. 2008:1028-1030.

[10] 甘元驹.谢仕义,付东洋,等.防欺诈的动态(t,n)门限多秘密共享方案[J].四川大学学报:工程科学版,2006, 38(6):131-134.

[11] OSTROVSKY R,YUNG M. How to withstand mobile virus attacks [C]//Proc of the 10th Annual ACM Symposium on Principles in Distributed Computing. New York:ACM Press,1991:51-59.

[12] 濮光宁,殷凤梅,侯整风.无可信中心秘密共享方案的成员删除协议[J].重庆科技学院学报:自然科学版,2011,13(3):163-165.

[13] ZHOU Li-dong,SCHNEIDER F B,Van RENESSE R. APSS:proactive secret sharing in asynchronous systems[J]. ACM Trans on Information and Systems Security,2005,8(3):259-286.

[14] GUPTA V H,GOPINATH K. An extended verifiable secret redistribution protocol for archival systems[C]//Proc of the 1st International Conference on Availability, Reliability and Security. 2006:100-107.

[15] 周孟创,余昭平.一个无可信中心的动态(t,n)门限密钥共享方案[J].计算机应用研究,2011,28(8):3061-3063.