访问结构上的动态先应式秘密共享方案

秦华旺，朱晓华，戴跃伟

(南京理工大学自动化学院 江苏 210094)

【摘要】基于现有的(t, n)门限秘密共享方案，通过引入攻击结构的概念，提出了一种可以应用于访问结构上的动态先应式秘密共享方案，在更新子份额的同时可以改变秘密共享的访问结构。给出了子份额分发和子份额更新的详细步骤，并对方案的有效性进行了充分的证明。与现有方案的性能比较表明，该方案不仅计算量小，而且具有更大的应用灵活性。

关 键 词 访问结构； 密码学； 信息安全； 先应式； 秘密共享

中图分类号 TP393 **文献标识码** A doi:10.3969/j.issn.1001-0548.2012.06.021

Dynamic Proactive Secret Sharing Scheme Based on Access Structure

QIN Hua-wang , ZHU Xiao-hua, and DAI Yue-wei

(School of Automatization, Nanjing University of Science and Technology Nanjing 210094)

Abstract Basing on the existing (t, n) secret sharing scheme, a dynamic proactive secret sharing scheme which can be applied to access structure is proposed by introducing the concept of adversary structure. The access structure can be changed when the shadows are renewed. The detailed process of the distribution and renewal of the shadows is given, and the validity of the scheme is proved perfectly. The comparisons with the existing schemes show that the proposed scheme is more flexible and its computational cost is less.

Key words access structure; cryptography; information security; proactive; secret sharing

先应式秘密共享假设攻击者以一定的速度感染秘密子份额，但子份额也以同样的速度进行恢复，从而保证始终有足够多的子份额用于秘密重构，子份额恢复的基本方法是周期性地更新，经过一次更新后，少于门限个数的旧子份额将不能再用于恢复共享秘密，这样就可以将攻击者的攻击时间从秘密的整个生存周期缩短为秘密的一个更新周期。文献[1]基于文献[2]的可验证秘密共享方案，通过更新拉格朗日插值多项式，首次提出了一种实用性较强的先应式秘密共享方案。在该基础上，又有多种先应式秘密共享方案被提出。如文献[3]利用二维对称多项式，设计了一种无条件先应式秘密共享方案；文献[4]基于椭圆曲线密码系统，设计了一种可验证先应式秘密共享方案；文献[5]利用矩阵映射方法，设计了一种先应式的多秘密共享方案；文献[6]和文献[7]利用线性代数方法，实现了访问结构上的先应式秘密共享；文献[8]通过对子份额的再共享，提出了一种异步环境下的先应式秘密共享方案；文献[9]则给出了异步环境下先应式秘密共享的具体实现技术；文献[10]在其设计的秘密再分发协议中提出了动态先应式秘密共享的思想，在更新子份额时还可以改变秘密共享的结构；文献[11]对文献[10]的方案进行了改进和完善，并给出了其在实际应用中的具体实现方法；此外，文献[12-13]也利用文献[10]的思想设计了相应的动态先应式秘密共享方案；文献[14]基于文献[2]的先应式秘密共享方案，以及文献[1]的可验证秘密共享方案，提出了一种更安全和更高效的动态先应式秘密共享方案。

在上述方案中，文献[10-14]的方案均可以实现动态的秘密共享，即在更新子份额的同时可以改变秘密共享的结构。动态先应式秘密共享具有重要的实际应用价值，由于安全性要求改变、攻击者入侵、秘密共享成员的变更或性质变化等因素，都可能会要求秘密共享的结构发生相应的变化。如当系统怀疑某个成员可能已经遭到入侵时，其可以通过改变秘密共享的结构来降低该成员在秘密重构中的作用，从而继续保持整个系统的安全性。与一般的先应式秘密共享方案相比，动态先应式秘密共享方案

收稿日期：2011－02－22； 修回日期：2011－06－20
基金项目：国家自然科学基金(60374066)
作者简介：秦华旺(1978－)，男，博士，主要从事信息安全方面的研究.

具有更高的安全性和更大的应用灵活性。

本文基于文献[9]的(t,n)秘密共享方案，通过在其中引入攻击结构的概念，提出了一种可以应用于访问结构上的秘密共享方案，并通过在更新子份额的同时改变秘密共享的访问结构，实现动态先应式的秘密共享。与现有的基于拉格朗日插值的动态先应式秘密共享方案[10-14]相比，本文方案不仅计算量小，而且还可以应用于访问结构上。

1 访问结构和攻击结构

用$U=\{U_1, U_2,\cdots, U_n\}$表示$n$个成员所组成的集合，则集合$U$上秘密共享的访问结构$\Gamma$由定义1给出。

定义 1 访问结构：若$\Gamma=\{P|P$中的成员合作能够重构共享秘密，且$(P\in\Gamma, P\subseteq P'\subseteq U)\Rightarrow(P'\in\Gamma)\}$，则$\Gamma$是$U$上秘密共享的访问结构。

访问结构Γ中的元素P称为集合U的授权子集或合格子集，访问结构Γ即为U的所有授权子集的汇集。由定义1可知，访问结构是单调递增的，即若P是访问结构Γ中的元素，且$P\subseteq P'\subseteq U$，则P'也是访问结构Γ中的元素；若访问结构中的任意两个元素之间不存在包含关系，则称该访问结构为最小访问结构。

定义 2 最小访问结构：若$\Gamma_0\subseteq\Gamma$，且$\Gamma_0=\{P$ | 如果P'满足$P'\subseteq P\subseteq U$，则$P'\notin T_0\}$，则Γ_0是U上秘密共享的最小访问结构。

为了将文献[12]的(t, n)秘密共享方案应用于访问结构，本文引入文献[15]中定义的攻击结构概念。

定义 3 攻击结构：若$A=\{P|P$中的成员合作不能重构共享秘密，且$(P\in A, P'\subseteq P\subseteq U)\Rightarrow(P'\in\mathrm{A})\}$，则$A$是$U$上秘密共享的攻击结构。

之所以称为攻击结构，是因为这些集合中的成员即使在被攻击者同时攻陷的情况下，也不会影响到共享秘密的安全性。由定义3可知，攻击结构是单调递减的。若攻击结构中的任意两个元素之间不存在包含关系，则称该攻击结构为最大攻击结构。

定义 4 最大攻击结构：若$A_0\subseteq A$，且$A_0=\{P|$如果P'满足$P\subseteq P'\subseteq U$，则$P'\notin A_0\}$，则A_0是U上秘密共享的最大攻击结构。

2 文献[12]的方案介绍

文献[12]的(t,n)秘密共享方案的子份额分发过程可以概括为以下几步：

1) 通过从n个成员$U_1, U_2,\cdots, U_n$中任意选取t–1个成员，构造$k=C_n^{t-1}$个成员子集，分别记为$P_1, P_2,\cdots, P_k$；

2) 将共享秘密S拆分为k个不同的子份额，分别记为$S_1, S_2,\cdots, S_k$；

3) 对于子集P_j，若其包含成员U_i，则不将子份额S_j分发给U_i；否则将子份额S_j分发给U_i，以此规律遍历所有的k个子集(该步将使集合P_j中的所有成员不持有子份额S_j)。

如对于一个(2,4)秘密共享方案，按上述过程进行子份额分发后，每个成员的子份额持有情况如表1所示。可以看出，4个成员中的任意两个成员可以重构共享秘密，而任意一个成员均不能重构共享秘密。

表1 子份额持有情况

成员	子份额
U_1	S_2, S_3, S_4
U_2	S_1, S_3, S_4
U_3	S_1, S_2, S_4
U_4	S_1, S_2, S_3

3 本文方案

文献[9]的方案只能应用于(t,n)门限结构，本文通过在该方案中引入攻击结构的概念，提出一种可以应用于访问结构上的秘密共享方案，并通过对其子份额的更新和访问结构的改变，实现动态先应式的秘密共享。

3.1 初始化

设$U=\{U_1, U_2, \cdots, U_n\}$为$n$个成员所组成的集合，为了实现访问结构$\Gamma$上的动态先应式秘密共享，可信中心PKG首先要根据访问结构Γ求出其对应的最大攻击结构A_0，步骤如下：

1) 根据定义2删除访问结构Γ中的冗余子集，得到最小访问结构Γ_0；

2) 根据Γ_0求出攻击结构A，若$\Gamma_0=\{P_1, P_2, \ldots, P_\alpha\}$ ($P_i\subseteq U, i=1,2, \cdots, \alpha$)，则$A=\{P|P\subseteq U$，且$P_i\not\subset P, i=1, 2, \cdots, \alpha\}$，即$A$为既不和$P_i$相同也不包含$P_i$的子集汇集；

3) 根据定义4删除A中的冗余元素，使任意两个元素之间不存在包含关系，从而得到最大攻击结构A_0。

用S表示需要共享的秘密，若最大攻击结构$A_0=\{Q_1, Q_2, \cdots, Q_\beta\}$($Q_i\subseteq U, i=1, 2, \cdots, \beta$)，则PKG随机选取$\beta$–1个正整数，分别记为$S_1^0, S_2^0, \cdots, S_{\beta-1}^0$，并令$S_\beta^0=S_1^0\oplus S_2^0\oplus\cdots\oplus S_{\beta-1}^0\oplus S$，符号$\oplus$为按位异或运算，$S_1^0, S_2^0, \cdots, S_\beta^0$即为共享秘密$S$在初始周期(0周期)的$\beta$个子份额。

3.2 子份额分发

1) PKG设定n个相同的集合$H_i=\{S_1^0, S_2^0, \cdots, S_\beta^0\}$, $i=1, 2, \cdots, n$；

2) PKG执行以下运算：

for(i=1; $i\leqslant\beta$; i++)

{
L=Q_i中成员的个数;
for(j=1; j≤L; j++)
{
r=Q_i中第j个成员在集合U中的下标号(即Q_i中第j个元素为成员U_r);
将集合H_r中的子份额S_i^0删除;
}
}

3) PKG利用安全通道，将H_i中保留的子份额秘密发送给成员U_i, i =1, 2, …, n。

在步骤2)中将使集合Q_i中的所有成员不持有子份额S_i^0，如Q_2={U_1, U_3, U_4}，则成员U_1、U_3和U_4都将不持有子份额S_2^0。

3.3 子份额更新

为了防止PKG的单点失效，在完成首次子份额分发后，PKG将处于离线状态，因此子份额的更新将由所有成员来共同完成。动态的先应式秘密共享方案，要求可以在更新子份额的同时改变秘密共享的结构。不失一般性，设子份额由t周期更新为t+1周期时，秘密共享的访问结构由Γ^t变成了Γ^{t+1}，则子份额S_j^t更新为S_j^{t+1}的过程如下：

1) 按3.1节中所述步骤由访问结构Γ^{t+1}求出其对应的最大攻击结构A_o^{t+1}={Q_1^{t+1}, Q_2^{t+1}, …, $Q_{\beta'}^{t+1}$}($Q_i^{t+1}\subseteq U$, i=1, 2, …, β');

2) 设成员U_i持有子份额S_j^t，则U_i随机选取β'−1个正整数$S_{j1}^t, S_{j2}^t, \cdots, S_{j(\beta'-1)}^t$，并令$S_{j\beta'}^t = S_{j1}^t \oplus S_{j2}^t \oplus \cdots \oplus S_{j(\beta'-1)}^t \oplus S_j^t$;

3) 对A_o^{t+1}中的某个元素Q_k^{t+1}，若其包含成员U_m，m=1, 2, …,n，则U_i不将S_{jk}^t发送给U_m；若Q_k^{t+1}不包含成员U_m，则U_i就将S_{jk}^t发送给U_m;

4) U_i按照步骤3)中的原则，遍历A_o^{t+1}中包含的所有元素;

5) 当U中的某个成员收集到所有的S_{1j}^t, $S_{2j}^t, \cdots, S_{\beta' j}^t$后，通过计算$S_j^{t+1} = S_{1j}^t \oplus S_{2j}^t \oplus \cdots \oplus S_{\beta' j}^t$产生新的子份额$S_j^{t+1}$，并删除$S_{1j}^t, S_{2j}^t, \cdots, S_{\beta' j}^t$以及其保存的所有$t$周期的子份额。

在步骤3)和步骤4)中，将保证集合Q_k^{t+1}中的成员不会收到其他成员发送的S_{jk}^t，由于在秘密共享方案中不会让一个成员保存所有的子份额，因此，集合Q_k^{t+1}中的成员也就不可能收集到所有的S_{jk}^t，j=1, 2,…, β'，从而也就不能计算出新的子份额S_k^{t+1}。此外，上述的子份额更新过程还将保证除集合Q_k^{t+1}中成员以外的其他成员均能得到S_{jk}^t, j=1, 2,…, β' (别的成员发送的或者自己产生的)，因此这些成员也就可以计算出新的子份额S_k^{t+1}。

由于一个旧子份额可能被多个成员重复保存，而为了使子份额更新时只产生唯一有效的新子份额(步骤5))，就必须保证一个旧子份额只能被分解一次(步骤2))。因此，在每个周期的子份额更新过程中，首先规定各个成员的子份额分解顺序，如按照成员标号依次从U_1到U_n，然后当U_i分解其保存的子份额时，对于U_{i-1}已经分解过的子份额将不再进行分解，而且一旦所有的子份额都被分解过，后面的成员将不再分解其保存的子份额。

3.4 秘密的重构

设U的某个授权子集X要重构共享秘密S，重构过程如下：

1) X中的每个成员都将其保存的子份额发送给秘密生成者;

2) 秘密生成者删除掉多余的相同子份额，每个子份额只保留一份，然后通过计算S= $S_1^t \oplus S_2^t \oplus \cdots \oplus S_\gamma^t$，恢复出共享秘密S，其中$t$为当前的周期标号，$\gamma$为当前访问结构所对应的最大攻击结构包含的元素数量。

4 有效性证明

定义 5 秘密重构性：如果一个秘密共享方案可以保证访问结构中的所有授权子集均能够重构共享秘密，则称该方案具有秘密重构性。

定义 6 秘密保密性：如果一个秘密共享方案可以保证除访问结构中授权子集以外的所有其他子集均不能重构共享秘密，则称该方案具有秘密保密性。

显然，一个既具有秘密重构性又具有秘密保密性的秘密共享方案才是有效的方案。下面对方案的有效性进行证明。

4.1 子份额分发的有效性

定理 1 经过3.2节中所述的子份额分发，如果U的某个子集X中的所有成员全部缺少某个子份额S_i^0，则$X\subseteq Q_i$，其中$Q_i\in A_o$，A_o为最大攻击结构。

证明：用反证法。假设X中的所有成员全部缺少子份额S_i^0且$X\not\subset Q_i$。因为$X\not\subset Q_i$，所以X中必然至少包括某个Q_i中没有的成员U_j，即$U_j\in X$，$U_j\notin Q_i$。根据子份额的分发过程(3.2节中的步骤2))可知，只有集合Q_i中的成员才缺少子份额S_i^0，而其他成员均持

有子份额 S_i^0，由于 $U_j \notin Q_i$，因此成员 U_j 中必然有子份额 S_i^0，而由于 $U_j \in X$，从而使 X 中的成员并不全部缺少子份额 S_i^0，这显然与最初假设的条件矛盾，所以假设不成立，定理1得证。

推论 1 经过3.2节中所述的子份额分发后，如果 U 的某个子集 $X \not\subset Q_i$，i=1,2,⋯,β(β为 A_o 中包含的元素数量)，则 X 中的成员能够重构共享秘密 S。

证明：用反证法，假设 $X \not\subset Q_i$, i=1,2,⋯,β，且 X 中的成员不能重构共享秘密 S。由于 X 中的成员不能重构共享秘密 S，那么 X 中的所有成员至少全部缺少 S 的某个子份额 S_i^0，由定理1可知，$X \subseteq Q_i$，显然这与初始的假设条件 $X \not\subset Q_i$ 矛盾，所以假设不成立，推论1得证。

定理 2 如果 U 的某个子集 $X \in \Gamma$(Γ 为 U 的访问结构)，则 $X \not\subset Q_i$，i=1,2,⋯,β；反之，如果 $X \notin \Gamma$，则 X 一定会被 A_o 中的某个元素包含。

证明：仍然采用反证法，假设 $X \in \Gamma$ 且 $X \subseteq Q_i$，根据 $X \subseteq Q_i$，可知 $X \in A_o$，由于 $A_o \subseteq A$，因此 $X \in A$，即子集 X 既属于访问结构又属于攻击结构，这显然是不可能的，所以此假设不成立。若假设 $X \notin \Gamma$ 且 $X \not\subset Q_i$，i=1,2,⋯,β，由于 $X \not\subset Q_i$，i=1,2,⋯,β，根据最大攻击结构 A_o 的定义可知，$X \notin A$，即子集 X 既不属于访问结构又不属于攻击结构，这显然也是不可能的，所以此假设也不成立。综上所述，定理2得证。

经过3.2节中所述的子份额分发后，对于 U 的某个授权子集 $X \in \Gamma$，由定理2可知，$X \not\subset Q_i$，i=1,2,⋯,β，再由推论1可知，X 中的成员能够重构共享秘密 S，所以子份额的分发能够保证秘密重构性；对于 U 的某个非授权子集 $X' \notin \Gamma$，由定理2可知，$X' \subseteq Q_i$，根据子份额的分发过程(3.2节中的步骤2))可知，集合 Q_i 中的成员全部缺少子份额 S_i^0，因此 X' 中的成员也全部缺少子份额 S_i^0，故集合 X' 不能重构共享秘密 S，所以子份额的分发能够保证秘密保密性。

4.2 子份额更新的有效性

设子份额由 t 周期更新为 t+1周期时，秘密共享的访问结构由 Γ^t 变成了 Γ^{t+1}，并设 Γ^{t+1} 对应的最大攻击结构 A_o^{t+1}={ Q_1^{t+1}, Q_2^{t+1}, ⋯, $Q_{\beta'}^{t+1}$ }($Q_i^{t+1} \subseteq U$, i=1,2,⋯,β')。由3.3节所述的子份额更新过程可知，在子份额更新后，集合 Q_k^{t+1} 中的成员不能计算出新的子份额 S_k^{t+1},而除集合 Q_k^{t+1} 中成员以外的其他成员均能计算出新的子份额 S_k^{t+1}。因此，各个成员在访问结构 Γ^{t+1} 下的子份额保存原则，与子份额分发时在访问结构Γ下的子份额保存原则是一致的。所以，只需保证 $S_1^{t+1} \oplus S_2^{t+1} \oplus \cdots \oplus S_{\beta'}^{t+1} = S$，就可以根据4.1节中的证明，得出此时方案仍然具有秘密重构性和秘密保密性。

设 t 周期时的访问结构 Γ^t 对应的最大攻击结构 A_o^t 中包含 δ 个元素，由3.3节所述的子份额更新过程可知：

$$S_1^{t+1} \oplus S_2^{t+1} \oplus \cdots \oplus S_{\beta'}^{t+1} = (S_{11}^t \oplus S_{21}^t \oplus \cdots \oplus S_{\delta 1}^t) \oplus (S_{12}^t \oplus S_{22}^t \oplus \cdots \oplus S_{\delta 2}^t) \oplus \cdots (S_{1\beta'}^t \oplus S_{2\beta'}^t \oplus \cdots \oplus S_{\delta\beta'}^t) = (S_{11}^t \oplus S_{12}^t \oplus \cdots \oplus S_{1\beta'}^t) \oplus (S_{21}^t \oplus S_{22}^t \oplus \cdots \oplus S_{2\beta'}^t) \oplus \cdots \oplus (S_{\delta 1}^t \oplus S_{\delta 2}^t \oplus \cdots \oplus S_{\delta\beta'}^t) = S_1^t \oplus S_2^t \oplus \cdots \oplus S_\delta^t$$

由于 $S_1^0 \oplus S_2^0 \oplus \cdots \oplus S_\beta^0 = S$，所以 $S_1^{t+1} \oplus S_2^{t+1} \oplus \cdots \oplus S_{\beta'}^{t+1} = S$。

5 性能分析

对于先应式的秘密共享而言，在子份额更新时各个成员间需要进行交互，而为了保证这些交互信息的保密性、完整性以及通信效率，需要对这些信息进行加密、签名，并设计合理的通信协议；为了防止成员在子份额更新时提供虚假信息，还应能够对成员提供的信息进行验证；此外，为了保证各个成员子份额更新步骤的一致性，还需要提供一个同步时钟或可靠的异步通信协议。已有的先应式秘密共享方案[3-14]已经进行了大量研究，而且很多研究成果均可以应用于本文的方案中。如将文献[8]或文献[9]的异步通信协议应用于本文方案中，则可以实现异步环境下的先应式秘密共享；为了能够对子份额进行验证，只需将本文中的异或操作改为模加操作(这一改变不会影响本文方案的性能)，然后就可以应用文献[2]所提出的子份额验证方法。对于损坏子份额的检测可以采用文献[1]中提出的同步更新验证信息加数字签名的方法，而损坏的子份额可以利用其他成员持有的相同子份额进行恢复，但若某个子份额只被一个成员持有，则其损坏时将无法被恢复，这是本方案的一个不足之处(但一般情况下都会有多个成员持有同一个子份额)。由于上述的子份额验证、损坏子份额检测以及异步通信协议等已有较多研究成果，且这些研究成果一般均具有较好的可移植性，因此本文方案中不再研究，只重点研究先应式秘密共享方案中子份额分发和子份额更新的方法。

表2从子份额分发和更新的计算复杂度、秘密共享的结构、秘密共享结构的动态性3个方面，给出了本文方案与几种已有典型先应式秘密共享方案之间的性能比较。可以看出，在输入规模为 m 的情况下，由于文献[11]和文献[12]的方案均是基于拉格朗日插值来实现子份额分发和更新，其计算复杂度为

$O(m\log_2 m)$；文献[6]的方案基于矩阵乘法实现子份额分发和更新，因此其计算复杂度为$O(m^3)$；本文和文献[9]方案的子份额分发和更新中的主要运算为简单的异或操作，计算复杂度为$O(m)$，比其他方案显然要低得多。文献[9]和文献[11-12]的方案只能应用于(t,n)门限结构，而文献[6]和本文的方案可以应用于访问结构，因此应用范围更广。文献[6]和文献[9]方案的秘密共享结构不能改变，而文献[11-12]以及本文方案可以在更新子份额的同时改变秘密共享的结构。

与所列出的其他方案相比，本文方案的缺点是解密者需要保存较多的子份额，此外由于本文未设计具体的通信协议，因此也未能给出关于通信代价方面的一些性能比较，这也是以后需要进一步研究的问题。

表2　性能比较

方案	性能		
	子份额分发/更新的计算复杂度	秘密共享结构	秘密共享结构的动态性
文献[6]方案	$O(m^3)$	访问结构	结构不可变
文献[9]方案	$O(m)$	(t,n)门限结构	结构不可变
文献[11]方案	$O(m\log_2 m)$	(t,n)门限结构	结构可变
文献[12]方案	$O(m\log_2 m)$	(t,n)门限结构	结构可变
本文方案	$O(m)$	访问结构	结构可变

6　结 束 语

先应式秘密共享方案通过周期性的更新成员持有的子份额，来进一步提高共享秘密的安全性。本文提出了一种动态先应式秘密共享方案，可以在更新子份额的同时改变秘密共享的访问结构。文中详细介绍了该方案的子份额分发和子份额更新的方法，并对其有效性进行了充分的证明。与现有的基于拉格朗日插值的先应式秘密共享方案相比，本文方案不仅计算量小，而且还可以应用于访问结构上。

参 考 文 献

[1] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1987: 427-437.

[2] HERZBERG A, JARECKI S, KRAWCZYK H, et al. Proactive secret sharing, or how to cope with perpetual leakage[C]//Cryptology-Crypto'95. Berlin: Springer-Verlag, 1995: 339-352.

[3] STINSON D, WEI R. Unconditionally secure proactive secret sharing scheme with combinatorial structures[C]// SAC'1999, LNCS 1758. Berlin: Springer-Verlag, 1999: 200-214.

[4] SUN H, ZHENG X F, YU Y K. A proactive secret sharing scheme based on elliptic curve cryptography[C]//2009 First International Workshop on Education Technology and Computer Science. Wuhan: IEEE Press, 2009: 666-669.

[5] BAI L, ZOU X K. A proactive secret sharing scheme in matrix projection method. International[J]. Journal of Security and Networks, 2009, 4(4): 201-209.

[6] NIKOV V, NIKOVA S, PRENEEL B, et al. Applying general access structure to proactive secret sharing schemes[C]//Proceedings of the 23rd Symposium on Information Theory. Benelux: [s.n.], 2002: 197-206.

[7] MA C G, DING X F. Proactive verifiable linear integer secret sharing scheme[C]//ICICS'2009, LNCS 5927. Berlin: Springer-Verlag, 2009: 439-448.

[8] CACHIN C, KURSAWE K, LYSYANSKAYA A, et al. Asynchronous verifiable secret sharing and proactive cryptosystems[C]//Proceedings of the 9th (ACM) Conference on Computer and Communications Security. New York: ACM Press, 2002: 88-97.

[9] ZHOU L, SCHNEIDER F, ROBBERT R. APSS: Proactive secret sharing in asynchronous systems[J]. ACM Transactions on Information and System Security, 2005, 8(3): 259-286.

[10] DESMEDT Y, JAJODIA S. Redistributing secret shares to new access structures and its applications[C]//Technical Report ISSE TR-97-01. George Mason University: [s.n.], 1997.

[11] WONG T M, WANG C, WING J. Verifiable secret redistribution for archive systems[C]//Proceedings of the 1st International IEEE Security in Storage Workshop. Pittsburgh: IEEE Press, 2002.

[12] YU J, KONG F Y, LI D X. Verifiable secret redistribution for proactive secret sharing schemes[J]. Journal of Shanghai Jiaotong University (Science), 2006, E-11(2): 236-241.

[13] 于佳，李大兴，范玉玲. 基于加法共享的可验证秘密再分发协议[J]. 计算机研究与发展，2006, 43(1): 23-27.
YU Jia, LI Da-xing, FAN Yu-ling. Verifiable secret redistribution protocol based on additive sharing[J]Journal of Computer Research and Development, 2006, 43(1): 23-27.

[14] SCHULTZ D A. Mobile proactive secret sharing[C]// Proceedings of the 27th ACM Symposium on Principles of Distributed Computing. Toronto: ACM Press, 2008.

[15] HIRT M, MAURER U. Player simulation and general adversary structures in perfect multi-party computation[J]. Joural of Cryptology, 2000, 13(1): 31-60.

编　辑　张　俊