安全的矢量空间秘密共享方案

许春香, 陈 恺, 肖国镇
(西安电子科技大学综合业务网国家重点实验室信息保密研究所, 陕西西安 710071)

摘 要: 提出了一个密钥空间为有限域 $GF(q)$ 的安全的矢量空间秘密共享方案, 该方案能更有效地防止欺诈, 欺诈成功的概率仅为 $1/q^2$, 信息率是渐进最优的, 其值为 1/3. 同时对鲁棒的门限方案进行了探讨, 得出了其欺诈成功的概率最大值的解析表达式.

关键词: 秘密共享; 欺诈; 子秘密; 概率; 信息率
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2002) 05-0715-04

A Secure Vector Space Secret Sharing Scheme

XU Chun-xiang, CHEN Kai, XIAO Guo-zhen
(Institute of Information Security, ISN, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: A secure vector space secret sharing scheme with the secret $k \in GF(q)$ is presented. This scheme can detect the cheaters more effectively, with the probability of cheating $1/q^2$ and asymptotically optimal information rate 1/3. Meanwhile, a robust threshold scheme is studied and the expression of its probability of cheating is given.

Key words: secret sharing; cheating; shares; probability; information rate

1 引言

实现访问结构 Γ 的一个完备秘密共享方案是在 n 个参与者的集合(记为 P)中共享秘密 k 的方法: 如果参与者的授权子集 $A \subseteq P$ 中的参与者把他们的子秘密结合在一起, 他们就能确定秘密 k 的值; 而对于参与者的未授权子集 $A \subseteq P$ 即使把他们的秘密放在一起, 也不能得到有关秘密 k 的任何信息.

秘密共享方案自 1979 年被提出来以后已得到了广泛的应用. 在实际使用当中, 针对如何有效地防止欺诈的问题, 许多作者对此进行了深入的研究, 文[1]、[2]、[4]、[6]~[8]分别提出了不同的可防欺诈的秘密共享方案, M. Carpentieri 等人[3]给出了秘密共享方案为防止欺诈参与者所拥有的子秘密长度的下界, 但这些都是针对门限方案进行的研究, 而门限方案是矢量空间秘密共享方案的一种特殊情况. 矢量空间秘密共享方案是一个完备的理想方案, 该方案将秘密 k 分解为子秘密给各参与者, 当授权子集中的若干个参与者联合起来出示伪子密欺诈该授权子集中的另外一些参与者就能成功地非法获取秘密 k, 此时信息率为 1. 针对这种不安全隐患, C. Padró 等人[5]提出了一个安全的解决方案, 即防欺诈的矢量空间秘密共享方案, 它将秘密 k 和 k^2 分别分解为子秘密给各参与者, 当授权子集中的参与者出示其拥有的子秘密, 就能恢复出两个秘密值, 若第一个秘密值等于另外一个的平方, 则此时参与者中没有欺诈者存在, 否则有欺诈者存在, 其欺诈成功的概率为 $1/q$, 信息率是渐进最优的, 为 1/2. 同时得出鲁棒的门限方案欺诈成功的概率最大为 $(2r-3)/(q-r)$, 其中 r 是门限值. 本文把 C. Padró 等人的工作加以推广, 从而得到一个更安全的矢量空间秘密共享方案, 该方案能更有效地防止欺诈, 欺诈成功的概率仅为 $1/q^2$, 信息率是渐进最优的, 其值为1/3. 同时对鲁棒的门限方案进行了探讨, 得出了其欺诈成功的最大概率为 $(2r-3)^2/(q-r)^2$. 在所提方案的基础之上, 同样的思路, 容易构造出防欺诈的概率为 $1-(1/q^n)(n=3,4,\cdots)$、信息率为 $1/(n+1)$ 的安全方案, 此时的信息率仍为最优的.

2 工作准备

设 $P=\{p_1, p_2, \cdots, p_n\}$ 是参与者的集合, 访问结构 Γ 是单调的, 如果 $B \in \Gamma$ 且 $B \subseteq C \subseteq P$, 那么 $C \in \Gamma$.

如果 Γ 是一个访问结构, 那么 $B \in \Gamma$ 是最小授权子集, 如果无论何时 $A \subseteq B$, 且 $A \neq B$, 那么 $A \notin \Gamma$, Γ 的最小授权子集的集合记为 Γ_0 且称它为 Γ 的基. 因为 Γ 是由在基 Γ_0 中的子集的所有超子集组成, 因此 Γ 由它的基 Γ_0 唯一确定, 且它是 Γ_0 的函数, 可归纳为数学表达式: $\Gamma=\{C \subseteq P: B \subseteq C, B \in \Gamma_0\}$.

一个秘密共享方案的信息率[9]定义为:

$$\rho=\min\{\rho_i: 1 \le i \le n\}$$

收稿日期: 2001-01-08; 修回日期: 2001-07-20
基金项目: 国家自然科学基金(No. 69673025); 陕西自然科学基金(No. 99x06)资助

其中 $\rho_i = \log|K|/\log|S_i|$, S_i 表示 p_i 可能接受到的所有可能的子秘密的集合.

矢量空间构造[9]是一种针对访问结构构造某些理想方案的方法. 设 $P=\{p_1, p_2, \cdots, p_n\}$ 是 n 个参与者的集合, Γ 是访问结构, $D \notin P$ 是分发者. $K = GF(q)$, $E = K^r$ 是一个矢量空间. 访问结构 Γ 是一个矢量空间访问结构, 如果存在函数

$$\psi: P \cup \{D\} \to E$$

满足特性

$$\psi(D) = (1, 0, \cdots, 0) \in \langle \psi(p_i) = (x_{1i}, x_{2i}, \cdots, x_{ri}) : p_i \in A \rangle \Leftrightarrow A \in \Gamma$$

换句话说, 矢量 $\psi(D)$ 能表示为集合 $\{\psi(p_i): p_i \in A\}$ 中的向量的线性组合当且仅当 A 是一个授权子集. 如果 Γ 是这样一个矢量空间访问结构, 当对所有 $p \in P$ 有 $S_p = K$ 时, 就能够建立一个理想的秘密共享方案: 给定秘密 $k \in K$, 分发者随机选择 $v_2, \cdots, v_r \in K$, 令 $v = (v_1, v_2, \cdots, v_r)$, 其中 $v_1 = k$, 显然有 $v \cdot \psi(D) = k$, 则分配给第 i 个参与者的子秘密将是 $s_i = v \cdot \psi(p_i)$, 即 $s_i = \sum_j v_j x_{ji}$. 函数 ψ 是公开的, 授权子集中的参与者利用他们所拥有的子秘密的线性组合计算出秘密 k. Shamir 方案即 (t, n) 门限方案是矢量空间秘密共享方案的一个特例, 因为只需令 $\psi(p_i) = (1, x_i, x_i^2, \cdots, x_i^{t-1})$, 其中 x_i 是 K 中 n 个不同的非零元素.

当有欺诈存在时, 矢量空间构造方法是不安全的. 如果设 $A = \{p_1, p_2, \cdots, p_l\}$ 是一个授权子集, 则有 $\psi(D) = \lambda_1\psi(p_1) + \lambda_2\psi(p_2) + \cdots + \lambda_l\psi(p_l)$, 其中 $\lambda_i \in K$ 能够被任意参与者计算. 如果参与者 $p_1, p_2, \cdots, p_j (j < l)$ 联合起来欺骗 A 中的其余参与者而出示伪子密 $s_1^* = s_1 + \varepsilon_1, s_2^* = s_2 + \varepsilon_2, \cdots, s_j^* = s_j + \varepsilon_j$, 黑箱将计算出一个伪秘密:

$$k^* = \lambda_1(s_1 + \varepsilon_1) + \lambda_2(s_2 + \varepsilon_2) + \cdots + \lambda_j(s_j + \varepsilon_j) + \lambda_{j+1}s_{j+1} + \cdots + \lambda_t s_t$$

因此 $p_1, p_2, \cdots, p_j (j < l)$ 联合起来能够欺骗其他参与者而得到正确的秘密 $k = k^* - \lambda_1\varepsilon_1 - \lambda_2\varepsilon_2 - \cdots - \lambda_j\varepsilon_j$.

定义 1[5] 考虑一个最小授权子集 $A \in \Gamma$, $p \in A$, 设 b 是 $A - \{p\}$ 中的参与者所收到的子秘密的集合. 如果 $A - \{p\}$ 中的参与者打算欺骗 p, 他们将选择 b' 使下列概率达到最大:

$$Pr(p \text{ 被 } b' \text{ 欺骗} | A - \{p\} \text{ 有 } b)$$

把上述概率的最大值定义为 $A - \{p\}$ 中的参与者在不知道秘密 k 的情况下欺骗成功的概率. 如果对任意最小的授权子集 $A \in \Gamma$ 和任意的 $p \in A$ 欺骗成功的概率最大为 δ, 我们说具有访问结构 Γ 的秘密共享方案为 (Γ, δ) - 安全方案.

定义 2[5] 如果对任意最小的授权子集 $A \in \Gamma$ 和任意的 $p \in A$, 而 $A - \{p\}$ 中的参与者在知道秘密的情况下欺骗成功的最大概率为 ε, 就说具有访问结构 Γ 的秘密共享方案为 (Γ, ε) - 鲁棒方案.

3 安全的矢量空间方案

首先, 假设有一个值得信赖的秘密分发者和一个用来计算秘密的完全的黑箱. 在此基础上, 将提出一个 (Γ, δ) - 安全方案, 该方案能够在任何矢量空间访问结构上实现, 其欺诈成功的概率为 $\delta = 1/q^2$, $q = |K|$. 该方案的信息率等于 1/3.

设 $E = K^r$ 是特征不等于 2 的有限域 $K = GF(q)$ 上的所有 r 元构成的矢量空间. Γ 是根据下列函数定义的矢量空间访问结构:

$$\psi: P \cup \{D\} \to E$$

分发者 D 随机地选择一个秘密 $k \in K$ 和 $v_{21}, \cdots, v_{r1}, v_{22}, \cdots, v_{r2}, v_{23}, \cdots, v_{r3} \in K$, 令 $v_1 = (k, v_{21}, \cdots, v_{r1})$, $v_2 = (k^2, v_{22}, \cdots, v_{r2})$, $v_3 = (k^4, v_{23}, \cdots, v_{r3})$, 显然 $v_1, v_2, v_3 \in E$, 且满足 $k = v_1 \cdot x_0$, $k^2 = v_2 \cdot x_0$ 和 $k^4 = v_3 \cdot x_0$, 这里 $x_0 = \psi(D)$. D 计算 $s_i = v_1 \cdot x_i$, $t_i = v_2 \cdot x_i$, $u_i = v_3 \cdot x_i$, $x_i = \psi(p_i)$ $(1 \leqslant i \leqslant n)$, 并将子秘密 (s_i, t_i, u_i) 分配给参与者 p_i, $i = 1, 2, \cdots, n$.

设 $A = \{p_1, p_2, \cdots, p_l\}$ 是一个授权子集, $x_0 = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_l x_l$. 当 A 中的参与者出示他们的子秘密后, 黑箱将计算 $k_1 = \lambda_1 s_1 + \lambda_2 s_2 + \cdots + \lambda_l s_l$, $k_2 = \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_l t_l$ 和 $k_3 = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_l u_l$. 如果 $k_1^2 = k_2$, $k_2^2 = k_3$, 黑箱把 k_1 作为正确的秘密值. 如果 $k_1^2 \neq k_2$ 或 $k_2^2 \neq k_3$, 黑箱将警告参与者中有欺诈者存在, 此时, 值 k_1, k_2 和 k_3 必须保密, 也就是说黑箱必须销毁它们.

定理 1 该方案是一个实现访问结构 Γ 的完备秘密共享方案且信息率为 1/3.

证明 很显然任何授权子集 $A \in \Gamma$ 的参与者集合能够重构秘密 k. 而参与者集 $A = \{p_1, p_2, \cdots, p_l\} \notin \Gamma$ 如果想利用他们所拥有的子秘密重构秘密 k, 必须根据下列方程组计算出 $k = v_1 \cdot x_0$.

$$\begin{cases} s_1 = v_1 \cdot x_1 \\ s_2 = v_1 \cdot x_2 \\ \cdots \\ s_l = v_1 \cdot x_l \end{cases}, \begin{cases} t_1 = v_2 \cdot x_1 \\ t_2 = v_2 \cdot x_2 \\ \cdots \\ t_l = v_2 \cdot x_l \end{cases}, \begin{cases} u_1 = v_3 \cdot x_1 \\ u_2 = v_3 \cdot x_2 \\ \cdots \\ u_l = v_3 \cdot x_l \end{cases} \quad (v_1 \cdot x_0)^2 = v_2 \cdot x_0, \quad (v_2 \cdot x_0)^2 = v_3 \cdot x_0$$

这里未知数是 v_1, v_2 和 v_3. 由于 $x_0 \notin \langle x_1, \cdots, x_l \rangle$, 不难看出 $k = v_1 \cdot x_0$ 将以相同的概率取 K 中的所有值. 因此 $A \notin \Gamma$ 的参与者得不到关于秘密 k 的任何信息. 考虑到秘密 k 可在 K 中等概率地选取, 而子秘密在 K^3 中等概率地选取, 所以容易得出信息率为 1/3.

定理 2 该方案是一个 (Γ, δ) - 安全方案, 其中 $\delta = 1/q^2$

证明 设 $A = \{p_1, p_2, \cdots, p_l\} \in \Gamma$ 是一个最小授权子集, $T = \{p_1, p_2, \cdots, p_{l-1}\} \subset A$ 是欺诈者的集合, 把他们称为联合欺诈者. 假定 T 中的参与者不知道秘密 k. 如果 T 中的第 i 个参与者出示伪子密 $(s_i^*, t_i^*, u_i^*) = (s_i + \varepsilon_i, t_i + \delta_i, u_i + \theta_i)$, $(i = 1, 2, \cdots, l-1)$, 黑箱计算

$$k_1 = \sum_{i=1}^{l} \lambda_i s_i + \sum_{i=1}^{l-1} \lambda_i \varepsilon_i = k + \sum_{i=1}^{l-1} \lambda_i \varepsilon_i = k + \varepsilon$$

$$k_2 = \sum_{i=1}^{l} \lambda_i t_i + \sum_{i=1}^{l-1} \lambda_i \delta_i = k^2 + \sum_{i=1}^{l-1} \lambda_i \delta_i = k^2 + \delta$$

和

$$k_3 = \sum_{i=1}^{l} \lambda_i u_i + \sum_{i=1}^{l-1} \lambda_i \theta_i = k^4 + \sum_{i=1}^{l-1} \lambda_i \theta_i = k^4 + \theta$$

也就是说联合欺诈者能够选择任何 $\varepsilon, \delta, \theta \in K$, $\varepsilon \neq 0$ 来篡改他们所拥有的子秘密, 欺诈者不会被发现当且仅当 $k_1^2 = k_2$ 和

$k_2^2 = k_3$, 即当且仅当 $2k\varepsilon + \varepsilon^2 = \delta, 2k^2\delta + \delta^2 = \theta$. 由于欺诈者们不知道秘密 k, 所以找到一个合适的$(\varepsilon, \delta, \theta)$的概率为 $1/q^2$.

上述方案能识别出不知道秘密的骗子, 下面将证明该方案具有最优的信息率.

引理 **1**[5]　对任何(Γ, δ)-安全秘密共享方案有信息率

$$\rho \leq \frac{\log q}{\log[1 + (q-1)/\delta]}$$

其中 $q = |K|$.

定理 **3**　任何(Γ, δ)-安全$(\delta = 1/q^2)$门限秘密共享方案的信息率是渐近最优的.

证明　由定理 1 可知, 该方案的信息率为 1/3, 而

$$\lim_{q\to\infty} \frac{\log q}{\log(1 + \frac{q-1}{\delta})} = \lim_{q\to\infty} \frac{\log q}{\log(q^3 - q^2 + 1)} = \frac{1}{3}$$

由引理 1 可知, 该方案的信息率是渐近最优的.

4　鲁棒的门限方案

这一节, 将得出一个(r, n, ε)-鲁棒门限方案欺骗成功的最大概率为$(2r-3)^2/(q-r)^2$.

首先, 对 Shamir 方案作一修改, 分发者独立随机地选取有限域 $K = GF(q)$ 中 n 个不同的非零元素 $x_1, x_2, \cdots, x_n$, 这些值是保密的. 对于任意给定的秘密 $k \in K$, 分发者再独立随机地选取次数为 $r-1$ 的多项式 $\varphi_1(x)$, $\varphi_2(x)$ 和 $\varphi_3(x)$, 使其满足 $k = \varphi_1(0)$, $k^2 = \varphi_2(0)$ 和 $k^4 = \varphi_3(0)$. 然后分发者分配(x_i, s_i, t_i, u_i)给 p_i 作为其子秘密, 其中 $s_i = \varphi_1(x_i)$, $t_i = \varphi_2(x_i)$, $u_i = \varphi_3(x_i)$, $1 \leqslant i \leqslant n$. 在我们的方案里, 三个秘密值 k, k^2 和 k^4 采用 Shamir 方案分配, 除此以外, 值 x_i 在 Shamir 方案中是公开的, 而在本文的这方案中是保密的. 此方案可以看成是上一节所提出的方案的一种变形. 唯一的不同是在该方案中, 函数

$$\phi: P \cup \{D\} \to K^r$$
$$D \to x_0 = (1, 0, 0, \cdots, 0)$$
$$p_i \to x_i = (1, x_i, x_i^2, \cdots, x_i^{r-1})$$

不是公开的, 因为分发者所选定的值 $x_1, x_2, \cdots, x_n \in K$ 是保密的. 由定理 1 和定理 2, 我们可类似得到如下两个定理.

定理 **4**　该方案是一个具有信息率 1/4 的完备的(r, n)门限方案.

定理 **5**　该方案是一个(r, n, δ)-安全方案, 其中 $\delta = 1/q^2$.

为了得出(r, n, ε)-鲁棒门限方案欺骗成功的概率的上界, 需要下面的引理.

引理 **2**[5]　设 $x_1, \cdots, x_{r-1}, x_r$ 是 $K = GF(q)$ 中不同的非零元素, $\phi(x)$ 是次数不大于 $r-1$ 的多项式且满足 $\phi(x_i) = s_i$, $(1 \leqslant i \leqslant r)$, 则

$$\phi(0) = x_r\Psi_r(0)\left(\sum_{i=1}^{r-1} \frac{s_i}{(x_i - x_r)\Gamma'(x_i)} + \frac{s_r}{\Gamma_r(x_r)}\right)$$

其中 $\Psi_r(x) = (x - x_1)\cdots(x - x_{r-1})$, $\Gamma_r(x) = x\Psi_r(x)$ 和 $\Gamma'_r(x_i) = x_i \prod_{k=1, k\neq i}^{r-1}(x_i - x_k)$.

定理 **6**　该方案是(r, n, ε)-鲁棒方案且 $\varepsilon \leqslant (2r-3)^2/(q-r)^2$.

证明　设 $T = \{p_1, p_2, \cdots, p_{r-1}\}$ 是试图欺骗参与者 p_r 的参与者的集合, 当重构秘密 k 时, T 中的参与者出示伪子密 $(x_i^*, s_i^*, t_i^*, u_i^*)$, $(i = 1, 2, \cdots, r-1)$. 利用子秘密和秘密 k, T 中的参与者能够求出多项式 $\phi_1(x)$, $\phi_2(x)$ 和 $\phi_3(x)$. 但是, 由于他们不知道 x_r 的值, 故不能确定参与者 p_r 的子秘密.

下面我们考虑次数为 $r-1$ 的多项式 ϕ_1^*, ϕ_2^* 和 ϕ_3^*, 满足 $\phi_1^*(0) = k$, $\phi_2^*(0) = k^2$, $\phi_3^*(0) = k^4$, $\phi_1^*(x_i^*) = s_i^*$, $\phi_2^*(x_i^*) = t_i^*$ 和 $\phi_3^*(x_i^*) = u_i^*$, $1 \leqslant i \leqslant r-1$. 另外, 设 $s_r^* = \phi_1^*(x_r)$, $t_r^* = \phi_2^*(x_r)$ 和 $u_r^* = \phi_3^*(x_r)$. 由引理 2, 得到

$$k = x_r\Psi_r(0)\left(\sum_{i=1}^{r-1} \frac{s_i^*}{(x_i^* - x_r)\Gamma'_r(x_i^*)} + \frac{s_r^*}{\Gamma_r(x_r)}\right)$$

$$k^2 = x_r\Psi_r(0)\left(\sum_{i=1}^{r-1} \frac{t_i^*}{(x_i^* - x_r)\Gamma'_r(x_i^*)} + \frac{t_r^*}{\Gamma_r(x_r)}\right)$$

$$k^4 = x_r\Psi_r(0)\left(\sum_{i=1}^{r-1} \frac{u_i^*}{(x_i^* - x_r)\Gamma'_r(x_i^*)} + \frac{u_r^*}{\Gamma_r(x_r)}\right)$$

其中 $\Psi_r(x) = (x - x_1^*)\cdots(x - x_{r-1}^*)$, $\Gamma_r(x) = x\Psi_r(x)$. 如果 p_r 是诚实的, 黑箱将计算

$$k_1 = x_r\Psi_r(0)\left(\sum_{i=1}^{r-1} \frac{s_i^*}{(x_i^* - x_r)\Gamma'_r(x_i^*)}\right) + \frac{s_r}{\Gamma_r(x_r)} = k + \frac{x_r\Psi_r(0)}{\Gamma_r(x_r)}(s_r - s_r^*)$$

$$k_2 = k^2 + \frac{x_r\Psi_r(0)}{\Gamma_r(x_r)}(t_r - t_r^*)$$

$$k_3 = k^4 + \frac{x_r\Psi_r(0)}{\Gamma_r(x_r)}(u_r - u_r^*)$$

欺诈成功当且仅当 $\Psi_r(x_r) \neq 0$, $k_1^2 = k_2$, $k_2^2 = k_3$, 也就是当且仅当 $\Psi_r(x_r) \neq 0$ 和

$$2k\frac{\phi_1(x_r) - \phi_1^*(x_r)}{\Psi_r(x_r)} + \frac{\Psi_r(0)}{\Psi_r^2(x_r)}(\phi_1(x_r) - \phi_1^*(x_r))^2 = \frac{\phi_2(x_r) - \phi_2^*(x_r)}{\Psi_r(x_r)}$$

$$2k\frac{\phi_2(x_r) - \phi_2^*(x_r)}{\Psi_r(x_r)} + \frac{\Psi_r(0)}{\Psi_r^2(x_r)}(\phi_2(x_r) - \phi_2^*(x_r))^2 = \frac{\phi_3(x_r) - \phi_3^*(x_r)}{\Psi_r(x_r)}$$

因此欺诈成功当且仅当 $\Psi_r(x_r) \neq 0$, 且 x_r 是下列两个多项式的根:

$$\Phi_1(x) = 2k\Psi_r(x)(\phi_1(x) - \phi_1^*(x)) + \Psi_r(0)(\phi_1(x) - \phi_1^*(x))^2 - \Psi_r(x)(\phi_2(x) - \phi_2^*(x))$$

$$\Phi_2(x) = 2k^2\Psi_r(x)(\phi_2(x) - \phi_2^*(x)) + \Psi_r(0)(\phi_2(x) - \phi_2^*(x))^2 - \Psi_r(x)(\phi_3(x) - \phi_3^*(x))$$

由于 $\deg(\Phi_j(x)) \leqslant 2r-2$, $j = 1, 2$ 且 0 是 $\Phi_j(x)$ $(j = 1, 2)$ 的根, 所以 x_r 最多可以取 $2r-3$ 个值. 故欺诈成功的最大概率为$(2r-3)^2/(q-r)^2$.

5　结束语

本文提出的安全矢量空间秘密共享方案, 能有效地防止欺诈, 欺诈成功的概率仅为 $1/q^2$, 信息率为 1/3, 满足渐近最优性. 同时得出了鲁棒的门限方案欺诈成功的最大概率$(2r-$

$3)^2/(q-r)^2$. 显然, 本文所提出的方案可进一步加以推广, 容易得到欺诈成功的概率为 $1/q^n(n=3, 4, \cdots)$ 的秘密共享方案, 此时信息率为 $1/(n+1)$, 仍满足渐进最优性.

参考文献:

[1] M Carpentieri. A perfect threshold secret sharing scheme to identify cheaters [J]. Designs, Codes and Cryptography, 1995, 5(3): 183-197.

[2] J Rifa-Coma. How to avoid the cheaters succeeding in the key sharing scheme [J]. Designs, Codes and cryptography, 1993, 3(3): 221-228.

[3] M Carpentieri, A De Santis, U Vaccaro. Size of shares and probability of cheating in threshold schemes [A]. Advances in Cryptology-CRYPTO'94 [C]. Berlin: Springer-Verlag, 1994. 118-125.

[4] B Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting [A]. Advances in Cryptology-CRYPTO'99 [C]. Berlin: Springer-Verlag, 1999. 148-164.

[5] C Padró, G Sáez. Detection of cheaters in vector space secret sharing schemes [J]. Designs, Codes and Cryptography, 1999, 16(1): 75-85.

[6] A Herzberg, S Jarecki, H Krawczyk, M Yung. Proactive secret sharing or: how to cope with perpetual leakage [A]. Advances in Cryptology-CRYPTO'95 [C]. Berlin: Springer-Verlag, 1995. 339-352.

[7] 张建中, 肖国镇. 可防止欺诈的秘密共享方案 [J]. 通信学报, 2000, 21(5): 81-83.

[8] E F Brickell, D R Stinson. The detection of cheaters in threshold scheme [A]. Advances in Cryptology-CRYPTO'88 [C]. New York: Springer-Verlag, 1988. 564-577.

[9] D R Stinson. Cryptography: Theory and Practice [M]. New York: CRC Press, 1995. 343-350.

作者简介:

许春香 女, 1965 年生于湖南长沙, 副教授, 博士研究生, 主要研究方向为信息安全和密码学.

陈 恺 男, 1970 年生, 讲师, 博士研究生, 主要研究方向为信息安全和密码学.

肖国镇 男, 1934 年生, 教授, 博士生导师, 主要研究方向为密码学和编码学.