一个可防止欺诈的秘密分享方案 [1]

张建中 肖国镇

(西安电子科技大学信息安全与保密研究所 西安 710071)

摘 要 本文利用认证码构造一种可防止欺诈的秘密分享方案. 此方案不仅可防止非法者的假冒, 也可防止子密合法拥有者的欺诈, 特别是可防止某些子密合法拥有者形成团伙对另一合法者的欺诈, 且数据利用率较高.

关键词 秘密分享, 认证码, 欺诈, 子密, 保密通信

中图号 TN918

1 引 言

(k,n) 门限秘密分享方案是 Blakley[1] 和 Shamir[2] 各自分别提出的. 由于它在许多方面有重要应用 [3−5], 如保密通信中对通信密钥的管理, 安全计算, 数据安全, 金融网的安全管理等, 所以它一提出便受到人们的重视. 所谓 (k,n) 门限秘密分享是指: 把给定一个秘密 s 分拆成 n 个子密, 使得

(1) 知道 k 个或更多个子密就可算出 s .

(2) 知道任意 $k-1$ 个或更少个子密无法确定出 s .

设 $P=\{P_1,P_2,\cdots,P_n\}$ 是 n 个参加者, 其中 P_i 分享子密 s_i . 所以 (k,n) 门限秘密分享方案就是把秘密 s 分配给这 n 个参加者, 使得这 n 个参加者中任何 k 个人协作就可恢复该秘密 s , 但任何少于 k 个的参加者都无法求得 s .

秘密分享方案主要考虑防止: (1) 外部欺诈: 非法参加者设法获得秘密 s; (2) 内部欺诈: 合法的子密 s_i 持有者 P_i 为了使恢复的秘密 $s'\neq s$, 而出示伪子密 s'_i .

一个 (k,n) 门限秘密分享方案称作 "完善的" 是指任意少于 k 个的参加者协作都不能得到有关这个秘密 s 的任何部分信息 (从信息论的角度) , 而不管他们有多大的计算能力. 一个门限秘密分享方案称作 "无条件安全的" 是指欺诈成功的概率被限定在一个指定的概率, 而不管欺诈者有多大的计算能力 [4] .

设计秘密分享方案能抵抗欺诈是一个重要的课题, 尤其是如何防止一部分合法参加者形成一伙企图欺诈另外的合法参加者, 比如他们利用合法身份出示伪子密. 许多学者针对上述各种欺诈研究设计了门限秘密方案 [6−11] . McEliece 和 Sarwate 最早利用纠错码构造了一个方案 [12] , 使得任意 $k+2e$ 个参加者, 只要其中欺诈者不超过 e 个, 都能正确恢复原秘密 s . 但当欺诈者超过 e 个时, 所恢复秘密 s' 便是伪秘密. 且不能发现是谁不诚实. Rabin 和 Ben-Or 基于 Shamir 的方案构造了一个秘密分享方案 [13] , 以防止欺诈, 且诚实者可以一定概率发现欺诈者. 但此方案由于每个参加者 P_j 都要保管对每个 $P_i(i\neq j)$ 的认证码而使信息率降低. 本文利用认证码构造一个秘密分享方案, 在性能上优于 Rabin-Ben-Or 方案, 且是完善的及无条件安全的, 不仅可防止非法者的假冒, 也可防止子密合法拥有者的欺诈, 尤其可防止一部分子密合法拥有者形成团伙对另一合法者的欺诈, 特别是数据利用率优于 Rabin-Ben-Or 方案. 具有一定的实用价值.

[1] 1998-02-18 收到, 1998-10-23 定稿

2 方案构造

2.1 秘密的分配

设 $a_1, a_2, \cdots, a_{k-1}$ 是 GF(q) 中随机选取的元素，对所有 P_i 保密，$q > n$. 再取 $\alpha_1, \alpha_2, \cdots \alpha_n$ 是 GF(q) 上 n 个互不相同且非零的元素，这些 α_i 是公开的。令

$$q(x) = s + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \tag{1}$$

其中 s 为要分配的秘密。设 $s_{i,0} = q(\alpha_i)$，而 $s_{i,1}, s_{i,2}, \cdots, s_{i,k-1}$ 是 GF(q) 上均匀随机选取的元素。将 $s_i = (s_{i,0}, s_{i,1}, \cdots, s_{i,k-1})$ 分配给 P_i 作为其子密。在 GF(q) 上均匀随机选取 $n-1$ 个非零元：$h_{j,i}$，$i = 1, 2, \cdots, n (i \neq j)$，由分配者计算

$$m_{j,i} = h_{j,i} s_{i,0} + \alpha_j s_{i,1} + \cdots + \alpha_j^{k-1} s_{i,k-1}, \quad i \neq j$$

将 $(h_{j,i}, m_{j,i})$ 分配给 P_j 作为 P_j 对 P_i 的认证码，由 P_j 秘密保存。这样，当 P_i 出示子密 s_i 时，P_j 便计算 $h_{j,i} s_{i,0} + \alpha_j s_{i,1} + \cdots + \alpha_j^{k-1} s_{i,k-1}$，看是否等于 $m_{j,i}$，若相等则接受 s_i，否则断定 P_i 为欺诈者。

2.2 秘密的恢复

设任意 k 个人协作，不妨设 $P_1, P_2, \cdots, P_k$ 协作，出示 $s_i (i = 1, 2, \cdots, k)$，则由方程组

$$\begin{cases} s + a_1\alpha_1 + a_2\alpha_1^2 + \cdots + a_{k-1}\alpha_1^{k-1} &= s_{1,0} \\ s + a_1\alpha_2 + a_2\alpha_2^2 + \cdots + a_{k-1}\alpha_2^{k-1} &= s_{2,0} \\ \vdots & \vdots \\ s + a_1\alpha_k + a_2\alpha_k^2 + \cdots + a_{k-1}\alpha_k^{k-1} &= s_{k,0} \end{cases}$$

可唯一确定解 $(s, a_1, a_2, \cdots, a_{k-1})$。(因其系数阵是 $k \times k$ 满秩阵)，从而可得秘密 s。

3 性能分析

下面分析本方案的性能。

定理 1　本方案符合 (k, n) 门限秘密分享方案的要求 (1), (2)，且是完善的。

证明　由于本方案是基于 Shamir 方案的，故符合 (1), (2)。现设 r 个人协作，$r < k$，如 $P_1, P_2, \cdots, P_r$，得方程组

$$\begin{cases} s + a_1\alpha_1 + a_2\alpha_1^2 + \cdots + a_{k-1}\alpha_1^{k-1} &= s_{1,0} \\ s + a_1\alpha_2 + a_2\alpha_2^2 + \cdots + a_{k-1}\alpha_2^{k-1} &= s_{2,0} \\ \vdots & \vdots \\ s + a_1\alpha_r + a_2\alpha_r^2 + \cdots + a_{k-1}\alpha_r^{k-1} &= s_{r,0}. \end{cases}$$

此方程组关于未知量 $(s, a_1, \cdots, a_{k-1})$，其系数阵是 r 行满秩阵，故其自由变量有 $k-r$ 个，都在 GF(q) 上取值，所以此方程组有 q^{k-r} 个解，从而不能确定 s。特别，s 也可作为自由变量，可取 GF(q) 上任何值，故不能得到秘密 s 的任何信息，即方案是完善的。

对于一个外部欺诈者 $Q \notin \mathcal{P}$，假定 Q 知道系统，但 Q 不知道所有秘密信息。Q 欺诈成功是指：Q 用某个伪子密 $s'_r = (s'_{i,0}, s'_{r,1}, \cdots, s'_{r,k-1})$ 假冒 P_r 参与系统，而不被 $\mathcal{P} - \{P_r\}$ 中的 $k-1$ 个合法者所发现。有两种方式：(a) 针对性欺诈—— Q 假冒 $\mathcal{P}$ 中某个合法者 P_r 欺诈 $\mathcal{P} - \{P_r\}$ 中 $k-1$ 个特定的合法者。比如 Q 假冒 P_n 欺诈 $P_1, P_2, \cdots P_{k-1}$. (b) 随意性欺诈—— Q 假冒 $\mathcal{P}$ 中某个合法者 P_r，只要他能骗过 $\mathcal{P} - \{P_r\}$ 中的 $k-1$ 个人即可，不管这 $k-1$ 个合法者是谁。对于这两种欺诈，显然 (b) 成功的概率要比 (a) 成功的概率大。我们有下面的精确估计。

定理 2 一个外部欺诈者假冒某个合法者欺诈另一合法者成功的概率为 $1/q$。

证明 不妨假设 Q 假冒 P_n 欺诈 P_1。所有可能的“子密”空间为 $S = \{(y_0, y_1, \cdots, y_{k-1}) \mid y_i \in \mathrm{GF}(q), i = 0, 1, \cdots, k-1\}$，$|S| = q^k$。而对 Q 欺诈成功有利的“子密”是满足认证方程

$$h_{1,n}s'_{n,0} + \alpha_1 s'_{n,1} + \cdots + \alpha_1^{k-1} s'_{n,k-1} = m_{1,n} \tag{2}$$

的“子密”，即方程 (2) 的解空间，记为 R。由于此方程有 $k-1$ 个自由未知量，且都在 $\mathrm{GF}(q)$ 上取值，故 $|R| = q^{k-1}$。所以 Q 成功的概率为 $|R|/|S| = q^{k-1}/q^k = 1/q$。

定理 3 外部欺诈者 Q 针对性欺诈成功的概率为 $1/q^{k-1}$。

证明 假设 Q 假冒 P_n 欺诈 P_1, P_2, $\cdots$, P_{k-1}。由于 Q 欺诈每个 P_i 成功的概率均为 $1/q$，而这些 $P_1, P_2, \cdots, P_{k-1}$ 互相独立，故 Q 欺诈 $P_1, P_2, \cdots, P_{k-1}$ 成功的概率为 $1/q^{k-1}$。如果从认证方程看，Q 需在 S 的 q^k 个“子密”中选一个满足下列 $k-1$ 个认证方程：

$$\begin{cases} h_{1,n}y_0 + \alpha_1 y_1 + \cdots + \alpha_1^{k-1} y_{k-1} = m_{1,n} \\ h_{2,n}y_0 + \alpha_2 y_1 + \cdots + \alpha_2^{k-1} y_{k-1} = m_{2,n} \\ \vdots \qquad\qquad\qquad\qquad\quad \vdots \\ h_{k-1,n}y_0 + \alpha_{k-1} y_1 + \cdots + \alpha_{k-1}^{k-1} y_{k-1} = m_{k-1,n}, \end{cases}$$

由于此方程组系数阵的秩为 $k-1$，故有一个自由未知量，从而解为 q 个。故 Q 欺诈 $P_1, P_2, \cdots, P_{k-1}$ 成功的概率为 $q/q^k = 1/q^{k-1}$。

定理 4 外部欺诈者 Q 随意性欺诈成功的概率为 $\sum_{r=k-1}^{n} \binom{n}{r}(1/q)^r(1-1/q)^{n-r}$。

证明 由于 Q 欺诈每个 P_i 成功的概率为 $1/q$(定理 2)，我们用 $b(r, n, 1/q)$ 表示 Q 恰好欺诈成功 $\mathcal{P}$ 中 r 个合法者的概率。那么由概率论二项分布知道 $b(r, n, 1/q) = \binom{n}{r}(1/q)^r(1-1/q)^{n-r}$。而 Q 随意性欺诈成功等价于 Q 至少欺诈成功 $\mathcal{P}$ 中 $k-1$ 个人，故所求概率为 $\sum_{r=k-1}^{n} b(r, n, 1/q) = \sum_{r=k-1}^{n} \binom{n}{r}(1/q)^r(1-1/q)^{n-r}$。

下面讨论内部欺诈。所谓内部欺诈，我们指一个合法子密拥有者 P_r 将其真子密 $s_r = (s_{r,0}, s_{r,1}, \cdots, s_{r,k-1})$ 改换为伪子密 $s'_r = (s'_{r,0}, s'_{r,1}, \cdots, s'_{r,k-1}), s'_r \neq s_r$，企图欺诈另一诚实者。这在两点上与外部欺诈不同 (为了叙述方便，设 P_n 企图欺诈 P_1)：(1) P_n 所取伪子密 $s'_n = (s'_{n,0}, s'_{n,1}, \cdots, s'_{n,k-1})$，不但要通过 P_1 的认证，而且要使 $s'_{n,0} \neq s_{n,0}$，而对 Q 就无此要求；(2) P_n 拥有真子密 $s_n = (s_{n,0}, s_{n,1}, \cdots, s_{n,k-1})$，从而知道 P_1 对 P_n 的认证码 $(h_{1,n}, m_{1,n})$ 的关系 $h_{1,n}s_{n,0} + \alpha_1 s_{n,1} + \cdots + \alpha_1^{k-1} s_{n,k-1} = m_{1,n}$，而 Q 就不知道。

定理 5 一个内部欺诈者针对性欺诈另一诚实者成功的概率为 $1/(q-1)$。

证明　不妨设 P_n 企图欺诈 P_1，如上所述，P_n 拥有真子密 $s_n=(s_{n,0},s_{n,1},\cdots,s_{n,k-1})$，从而知道 P_1 对 P_n 的认证码 $(h_{1,n},m_{1,n})$ 之关系：

$$h_{1,n}s_{n,0}+\alpha_1 s_{n,1}+\cdots+\alpha_1^{k-1}s_{n,k-1}=m_{1,n}.$$

所以 P_n 只要能猜对 $h_{1,n}$ 的值，P_n 就可求得 $m_{1,n}$，然后易选 $s'_n=(s'_{n,0},s'_{n,1},\cdots,s'_{n,k-1}),(s'_{n,0}\neq s_{n,0})$，满足认证方程

$$h_{1,n}y_0+\alpha_1 y_1+\cdots+\alpha_1^{k-1}y_{k-1}=m_{1,n}$$

而使欺诈成功。但 $h_{1,n}\in \mathrm{GF}(q)-\{0\}$ 有 $q-1$ 个值均匀随机出现，故 P_n 成功的概率为 $1/(q-1)$。

推论　一个内部欺诈者随意性欺诈另一诚实者成功的概率为 $1-(1-1/(q-1))^{n-1}$。

证明　不妨设 P_n 为欺诈者，由定理 5 知 P_n 欺诈其他 $n-1$ 个诚实者中每个人成功的概率均为 $1/(q-1)$，故与定理 4 证明类似，得所求概率为 $\sum\limits_{r=1}^{n-1}b(r,n-1,1/(q-1))$。但 $\sum\limits_{r=0}^{n-1}b(r,n-1,1/(q-1))=1$，所以 $\sum\limits_{r=1}^{n-1}b(r,n-1,1/(q-1))=1-b(0,n-1,1/(q-1))=1-(1-1/(q-1))^{n-1}$。

如果 r 个内部欺诈者形成集团欺诈另一诚实者，由于他们掌握了较多信息，情况会对他们有利，我们有下列结果。

定理 6　(1) 当 $r<k-1$ 时，r 个内部欺诈者形成集团针对性欺诈另一诚实者成功的概率为 $1/(q-1)$; 随意性欺诈另一诚实者成功的概率为 $1-(1-1/(q-1))^{n-r}$。

(2) 当 $k-1\leq r\leq n-1$ 时，r 个内部欺诈者形成集团针对性欺诈另一诚实者成功的概率为 $1-(1-1/(q-1))^{r-k+2}$; 随意性欺诈另一诚实者成功的概率为 $1-(1-1/(q-1))^{(n-r)(r-k+2)}$。

证明　(1) $r<k-1$。　不妨设 r 个合法者 $P_1,P_2,\cdots,P_r$ 形成集团针对 P_n 进行欺诈。他们的最佳策略 [8] 为 $P_1,P_2,\cdots,P_{r-1}$ 保持其子密 $s_1,s_2,\cdots,s_{r-1}$ 不改变，而让 P_r 的子密 s_r 改为 $s'_r\neq s_r$ $(s'_{r,0}\neq s_{r,0})$。由定理 5 知 P_r 欺诈 P_n 成功的概率为 $1/(q-1)$。这就证明了前半部分。对于随意性欺诈，只要 P_r 能欺诈其余 $n-r$ 个诚实者 $P_{r+1},P_{r+2},\cdots,P_n$ 中的任一人即可。类似于定理 5 推论的证明，得集团随意性欺诈另一诚实者成功的概率为 $1-(1-1/(q-1))^{n-r}$。

(2) $k-1\leq r\leq n-1$。设 $P_1,P_2,\cdots,P_r$ 形成集团对 P_n 欺诈。他们的最佳策略为 $P_1,P_2,\cdots,P_{k-2}$ 保持子密 $s_1,s_2,\cdots,s_{k-2}$ 不变，而让第 $k-1$ 个人 $(P_1,P_2,\cdots,P_r$ 中一人$)P_{i_{k-1}}$ 将其子密 $s_{i_{k-1}}$ 改为 $s'_{i_{k-1}}\neq s_{i_{k-1}},(s'_{i_{k-1},0}\neq s_{i_{k-1},0})$。由定理 5，$P_{i_{k-1}}$ 欺诈 P_n 成功的概率为 $1/(q-1)$。现在只要 $r-(k-2)$ 个人 $P_{k-1},P_k,\cdots,P_r$ 中有一人能欺诈 P_n 成功即可。而所有这 $r-(k-2)$ 个人都被 P_n 发现为欺诈者的概率为 $(1-1/(q-1))^{r-(k-2)}$。故集团欺诈 P_n 成功的概率为 $1-(1-1/(q-1))^{r-k+2}$。对于随意性欺诈，这个集团只要能骗过其他 $n-r$ 个人 $P_{r+1},P_{r+2},\cdots,P_n$ 中的任一人即可。由于 $P_{k-1},P_k,\cdots,P_r$ 都被 $P_j(r+1\leq j\leq n)$ 发现为欺诈者的概率是 $(1-1/(q-1))^{r-(k-2)}$，所以 $P_{k-1},P_k,\cdots,P_r$ 都被所有 $P_{r+1},P_{r+2},\cdots,P_n$ 发现为欺诈者的概率为 $(1-1/(q-1))^{(r-(k-2))(n-r)}$。故

$P_{k-1}, P_k, \cdots, P_r$ 中有一人不被 $P_{r+1}, P_{r+2}, \cdots, P_n$ 中至少一人发现为欺诈者 (即集团随意性欺诈成功) 的概率为 $1-(1-1/(q-1))^{(n-r)(r-k+2)}$ 。

注 1 由定理 6(2) 可见，即使有 $n-1$ 个人形成集团 $(r=n-1)$ 欺诈另一诚实者，其成功的概率也只能为 $1-(1-1/(q-1))^{(n-r)(r-k+2)}=1-(1-1/(q-1))^{n-k+1}$ 。也就是说，一个诚实者能以概率 $(1-1/(q-1))^{n-k+1}$ 发现其余 $n-1$ 人形成集团对他的欺诈。并且能发现谁是欺诈者 (子密被窜改) 。

注 2 k 个合法者形成集团就可完全确定 $q(x)$ 并掌握其他 $n-k$ 个人的子密. 但由定理 6 知这对于他们 k 人集团的欺诈成功并无多大帮助。

关于此方案的信息率，我们考虑分送给每个 P_i 的子密 $s_i=(s_{i,0}, s_{i,1}, \cdots, s_{i,k-1})$ 包含 GF(q) 的 k 个元素，另外得到的认证码 $\{(h_{i,j}, m_{i,j}): j=1,2,\cdots,n,\ j\neq i\}$ 包含 GF(q) 的 $2(n-1)$ 个元，所以 P_i 共拥有 GF(q) 的 $k+2(n-1)$ 个元素。而恢复秘密 s 只用 $s_{i,0}$ ，故信息率为 $1/(k+2(n-1))$ 。Rabin-Ben-Or 方案中每个 P_i 要保存子密 $d_i \in$GF$(q), n-1$ 个随机数 $v_{i,j}(j=1,2,\cdots,n, j\neq i)$ ，还有 $n-1$ 个认证码 $(w_{i,j}, z_{i,j})(j=1,2,\cdots,n.\ j\neq i), v_{i,j}, w_{i,j}, z_{i,j}$ 都在 GF(q) 上取值. 所以 P_i 共保存 $1+(n-1)+2(n-1)=3(n-1)+1$ 个 $GF(q)$ 上的元素，故信息率为 $1/(3(n-1)+1)$ 。

4 结束语

本文基于 Shamir 的 (k,n) 门限秘密分享方案，结合认证码构造了一个可防止欺诈的 (k,n) 门限秘密分享方案，讨论了此方案的性能。结果表明此方案是完善的及无条件安全的。特别是一个诚实者能以很大概率发现其他几人 (甚至是 $n-1$ 个人) 形成集团对他的欺诈，并能确定谁是欺诈者 (伪子密) 。由于采用了共享信息，使信息利用率得到提高。

参 考 文 献

[1] Blakley G R. Safeguarding cryptographic keys. Proc. AFIPS 1979, National Computer Conference, 1979, Vol.48, 313–317.

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

[3] Denning D. Cryptography and Data Security. Reading, MA: Addison-Wesley, 1983, 135–185.

[4] Simmons G J. An introduction to shared secret and/or shared control schemes and their application. in Contemporary Cryptology: The Science of Information Integrity, G. J. Simmons(Ed.), New York: IEEE Press, 1992, 441–497.

[5] 王育民，何大可. 保密学——基础与应用. 西安：西安电子科技大学出版社， 1990, 246–342.

[6] Carpentieri M, Santis A D, Vaccaro U. Size of shares and probability of cheating in threshold schemes. Advances in Cryptology—EUROCRYPT'93 (T. Helleseth,ed.), Lecture Notes in Computer Science vol.765, Springer-Verlag, New York: 1994, 118–125.

[7] Karnin E D, Greene J W, Hellman M E. On secret sharing systems. IEEE Trans. on IT, 1983, IT-29(1): 35–41.

[8] Stinson D R. Decomposition constructions for secret sharing schemes. IEEE Trans. on IT, 1994, IT-40(1): 118–125.

[9] Blundo C, Gressti A, Santis A D, Vaccaro U. Fully dynamic secret sharing schemes. Proc. Crypto'93, 1994, LNCS vol.773, 110–125.

[10] 王新梅. 级连码 (K,N) 门限通信密钥分散保管系统. 通信学报， 1987, 8(1): 1–9.

[11] 郑宝东. 关于 (K,N) 门通信密钥分散保管系统的讨论. 通信学报， 1994, 15(1): 23–28.

[12] McEliece R J, Sarwate D V. On sharing secrets and Reed-Solomon codes. Communication of the ACM, 1981, 24(8): 583-584.

[13] Rabin T, Ben-Or M. Verifiable secrets sharing and multiparty protocols with honest majority. Proc. 21st ACM Symposium on Theory of Computing, New York: ACM Press, 1989, 73-85.

A THRESHOLD SECRET SHARING SCHEME TO IDENTIFY CHEATERS

Zhang Jianzhong Xiao Guozhen

(*The Institute of Information Security and Secrecy, Xidian University, Xi'an* 710071)

Abstract In this paper a threshold secret sharing scheme to identify cheaters is proposed by using authentication codes.The performance of the scheme is discussed. The results show that in the scheme the valid shareholders not only can identify the impersonation of an adversary, but also are able to detect the cheating of some valid shareholders, in particular one honest shareholder is able to detect the cheating of the other participants forming a coalition, and the information rate of the scheme is higher than that of others.

Key words Secret sharing, Authentication codes, Cheating, Share, Privacy communication

张建中： 男，1960 年生，副教授，博士生，主要从事信息安全及认证理论的研究.
肖国镇： 男，1934 年生，教授，博士生导师，主要从事密码学与编码学的研究工作.