具有传递性质的接入结构上的秘密分享方案的构造

张福泰[1,2], 王育民[1]
(1. 西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071; 2. 陕西师范大学计算机科学学院, 陕西西安 710062)

摘 要: 引入了具有传递性质的接入结构的概念, 并给出一种构造具有这类接入结构的秘密分享方案的通用方法, 该方法简捷易行. 对要分享的一个秘密, 不管一个参与者属于多少个最小合格子集, 他只需保存一个秘密份额. 而且用于分享多个秘密时, 不需要增加分享者额外的信息保存量. 因而优于已有的其他许多方法. 文中还给出了实例以说明如何具体地构造具有这类接入结构的秘密分享方案.

关键词: 秘密分享; 接入结构; 最小合格子集; 线性无关
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2001) 11-1582-03

Construction of Secret Sharing Schemes on Access Structures with Transfer Property

ZHANG Fu-tai, WANG Yu-min
(1. *Po. Box 119, Key Lab. of ISN, Xidian University, Xi'an, Shanxi 710071, China;*
2. *School of Computer Since, Shanxi Normal University, Xian, Shanxi 710072, China*)

Abstract: We propose the concept of access structure with transfer property, and suggest a general method of constructing secret sharing schemes with this kind of access structures. Our method is simple and practical. Even if a participant is contained in many minimal authorized subsets he needs not to keep more than one secret shares for sharing one secret. There is no need for a participant to keep extra secret data when multiple secrets are to be shared. So our method has advantages over many others. An example is given to show concretely how to construct secret sharing schemes with such access structures.

Key words: secret sharing; access structure; minimal authorized subset; linear independence

1 引言

秘密分享是信息安全和数据保密中的重要手段. 是由 Shamir[1] 和 Blakley[2] 提出的. 它是指将秘密 s 分割成若干个份额在一组参与者 $P=\{P_1, P_2, \cdots, P_n\}$ 中进行分配, 使得每一个参与者都得到关于该秘密的一个秘密份额, 而只有 P 的一些特定的子集(称为合格子集) 才能有效地恢复 s, 而 P 的其它子集不能有效地恢复 s, 甚至得不到关于 s 的任何有用信息.

一个秘密分享系统由秘密的分发者 D, 参与者集合 P, 接入结构 Γ(合格子集的集合) , 秘密空间 S, 份额空间, 分配算法, 恢复算法等构成. 秘密空间给出秘密的取值范围; 参与者集合给出参与秘密分享的人员; 接入结构 Γ 指出哪些参与者可一起恢复秘密, Γ 具有性质: 若 $\boldsymbol{A}\in\Gamma$ 且 $\boldsymbol{A}\subset\boldsymbol{B}$, 则 $\boldsymbol{B}\in\Gamma$; 份额空间给出秘密份额的取值范围; 分配算法给出由秘密产生秘密份额的概率多项式时间算法; 恢复算法是确定性的, 给出接入结构中的 $\boldsymbol{P}$ 的子集如何来恢复秘密. Γ 中的 $\boldsymbol{P}$ 的子集为合格子集. 按包含关系, Γ 中的极小元称为最小合格子集, Γ 由它的极小元的集合 Γ_0 惟一确定, 称 Γ_0 为 Γ 的基.

在秘密分享系统中最常见的是门限体制, 已提出的门限体制有多种[3], 其中 Shamir 的 Lagrange 内插多项式体制[1]、Blakley 的矢量体制[2]、Asmuth 等人的同余类体制[4] 及 Kamin 等人的矩阵法体制[5] 是主要的代表, 已经得到了广泛的应用. 文献[6~8] 中对具有一般接入结构的秘密分享做了一些研究, 给出了几个一般的秘密分享方案. 但在这些方案中, 属于多个最小合格子集的参与者, 需持有同一个秘密的多个秘密份额, 这给参与者带来了不便, 特别是在有多个秘密需要在同一组参与者中分享时, 这一缺点就显得尤为突出, 因而这些方案的实用性较差. 本文将提出一种构造具有传递性质的接入结构上的秘密分享方案的通用方法. 这种方法简捷易行, 具有很强的实用性. 在用这种方法构造的秘密分享方案中, 对每一个秘密, 每一个参与者只需持有它的一个秘密份额, 而不用考虑参与者所在的最小合格子集的个数.

2 相关工作

文[8] 给出了一个实现具有一般接入结构的秘密分享方案的方法. 按其方法每一参与者不需要保存一个秘密的多个秘密份额, 而只需保存一个秘密的内插多项式, 多项式的次数是参与者所在的最小合格子集的个数减 1. 而保存一个多项式需要保存其各次项的系数, 因此每一参与者分享一个秘密需保存的秘密数据的个数仍然等于他所属的最小合格子集的个数, 并没有给参与者带来方便. 他们的方法如下:

设参与者的集合 $P=\{P_1, P_2, \cdots, P_n\}$, 接入结构 Γ 的基 $\Gamma_0=\{A_1, A_2, \cdots, A_m\}$ (给 Γ_0 的元素排了序, A_j 的序号为 j), 假

收稿日期: 2000-07-12; 修回日期: 2000-12-08
基金项目: 国家自然科学基金(No. 19931010)

定参与者 P_i 所属的最小合格子集为 $A_{i1}, A_{i2}, \cdots, A_{ik}$, 那么应给 P_i 分发 k 个秘密份额 $S_{i1}, S_{i2}, \cdots, S_{ik}$ 依次相应于他所属的 k 个最小合格子集, 于是由 k 个点 $(i_1, S_{i1}), (i_2, S_{i2}), \cdots, (i_k, S_{ik})$ 可惟一确定一个 $k-1$ 次多项式 $f_i(x)$, 最后分发者把 $f_i(x)$ 秘密地发送给 P_i, P_i 只需保存一个秘密的多项式而不是 k 个秘密份额. 当他作为最小合格子集 A_{ij} 的成员恢复秘密时, 他提供的秘密份额为 $f_i(i_j)$.

若要在 $P=\{P_1, P_2, \cdots, P_n\}$ 中同时分享多个秘密, 则需把用于分享各秘密的接入结构的基中的所有元素依次编号, 然后用上述方法给每一个参与者确定一个秘密的多项式.

这种方法把参与者本应持有的各秘密份额巧妙地用一个多项式联系了起来, 然而并没有减少参与者应保存的秘密数据的量, 也就是说, 一个参与者属于多少个最小合格子集他就得保存同样个数的秘密数据, 增加了计算量而没有给分享者带来实际的方便. 同时, 一旦某一参与者丢失或记错了他的秘密多项式的某一项系数, 那么他所属的所有最小合格子集都将无法恢复秘密.

3　具有传递性质的一类接入结构上的秘密分享方案的构造方法

本节给出一类接入结构及其上的秘密分享体制的构造方法. 这类接入结构包含了所有的门限接入结构, 因而该结构上的秘密分享体制具有广泛的应用价值.

设秘密的分发者为 D, 参与者的集合为 $P=\{P_1, P_2, \cdots, P_n\}$, 秘密空间为 $S=GF(q)$ (q 为某一素数幂), 份额空间亦为 $GF(q)$, 接入结构为 Γ, Γ 的基为 Γ_0, 最小合格子集的最大势(元素个数)为 t. 不失一般性可设每一最小合格子集至少含有两个参与者, 且每一参与者至少属于一个最小合格子集.

3.1　具有传递性质的接入结构

设 A 是有限集合, φ 是 A 的一些子集构成的集合, 若 φ 满足: 对任意 X, $Y\in\varphi$, X 与 Y 不相交, 或对任意的 $a\in X\cap Y$, 均存在 $C\in\varphi$ 使得 $C\subseteq((X\cup Y)-\{a\})$, 则称 φ 在 A 上具有传递性质. 例如, 设 $A=\{1, 2, 3, 4, 5\}$, 则 $\varphi_1=\{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{4, 5\}\}$ 在 $\{1, 2, 3, 4, 5\}$ 上具有传递性质, 而 $\varphi_2=\{\{1, 2\}, \{2, 3\}, \{1, 3, 4\}\}$ 不具有传递性质. 任何门限体制的接入结构的基均具有传递性质.

若接入结构 Γ 的基 Γ_0 具有传递性质, 则称 Γ 具有传递性质. 任何门限接入结构都是具有传递性质的接入结构, 有大量的非门限接入结构具有传递性质, 如以上面例子中的 φ_1 为基的 A 上的接入结构.

3.2　有传递性质的接入结构上的秘密分享体制的构造方法

设 Γ 是具有传递性质的接入结构, 可按如下方法构造以 Γ 为接入结构的秘密分享方案.

3.2.1　D 进行预计算

(1) 随机选取 $GF(q)^t$ 中的一个非零列向量 $\alpha=(a_1, a_2, \cdots, a_t)^T$.

(2) 选取 $GF(q)$ 上的 $t\times n$ 阶矩阵 $G=(G_1, G_2, \cdots, G_t)$ (其中 G_j 为 G 的第 j 个列向量)使得

ⅰ 若 $A=\{P_{j_1}, P_{j_2}, \cdots, P_{j_l}\}\in\Gamma_0$, 则 $G_{j_1}, G_{j_2}, \cdots, G_{j_l}$ 线性无关, 且 α 可由 $G_{j_1}, G_{j_2}, \cdots, G_{j_l}$ 线性表示.

ⅱ 若 $A=\{P_{j_1}, P_{j_2}, \cdots, P_{j_l}\}\notin\Gamma$, 则 α 不能由 $G_{j_1}, G_{j_2}, \cdots, G_{j_l}$ 线性表示.

做完这些预计算后, D 公开接入结构 Γ, α 和 G.

3.2.2　分配算法

(1) 对秘密 $s\in S$, D 在 $U(s)=\{(b_1, b_2, \cdots, b_t)\in GF(q)^t \mid \sum_{j=1}^{t} a_jb_j=s\}$ 中随机选取一个向量 $(b_1, b_2, \cdots, b_t)$.

(2) D 计算 $(s_1, s_2, \cdots, s_n)=(b_1, b_2, \cdots, b_t)G$, $s_1, s_2, \cdots, s_n$ 依次为分发给 $P_1, P_2, \cdots, P_n$ 的关于秘密 s 的秘密份额.

3.2.3　恢复算法

若 $A=\{P_{j_1}, P_{j_2}, \cdots, P_{j_l}\}\in\Gamma$, 则由于相应的 $G_{j_1}, G_{j_2}, \cdots, G_{j_l}$ 可线性表示 α, A 中成员可找到 $x_1, x_2, \cdots, x_l$ 使得 $(G_{j_1}, G_{j_2}\cdots, G_{j_l})(x_1, x_2, \cdots, x_l)^T=\alpha$, 然后可协作计算出 $s=(s_{j_1}, s_{j_2}, \cdots, s_{j_l})(x_1, x_2, \cdots, x_l)^T$.　　恢复算法正确性的证明.

由秘密份额的产生方法可知,

$(s_{j_1}, s_{j_2}, \cdots, s_{j_l})(x_1, x_2, \cdots, x_l)^T=(b_1, b_2, \cdots, b_t)(G_{j_1}, G_{j_2}, \cdots, G_{j_l})(x_1, x_2, \cdots, x_l)^T=(b_1, b_2, \cdots, b_t)\alpha=s$.

反之, 若 $A=\{P_{j_1}, P_{j_2}, \cdots, P_{j_l}\}\notin\Gamma$, 则由于 α 不能由 $G_{j_1}, G_{j_2}, \cdots, G_{j_l}$ 线性表示, A 中成员不能得到关于秘密 s 的任何有用信息.

3.3　实例

3.3.1　非门限方案的例子

设 $P=\{P_1, P_2, \cdots, P_5\}$, $\Gamma_0=\{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_2, P_4, P_5\}, \{P_1, P_4, P_5\}, \{P_3, P_4, P_5\}\}$, 则以 Γ_0 为基的接入结构 Γ 具有传递性质且 $t=3$. 取 $\alpha=(3, 5, 6)^T$, 下面选取矩阵 $G=(G_1, G_2, \cdots, G_t)$ (其中 G_j 为 G 的第 j 个列向量):

先从势最大的最小合格子集着手, 如选 $\{P_1, P_4, P_5\}$, 则 G_1, G_4, G_5 的选取应使它们线性无关且能线性表示 α, 而且它们之中任何两个不能线性表示 α. 为此, 可使它们与 α 之中的任何三个线性无关即可. 这是容易办到的. 取 $G_1=(1, 1, 1)^T$, $G_4=(2, 4, 7)^T$, $G_5=(4, 5, 9)^T$, 经验证, 它们满足要求. G_2 的选择应使它与 G_1 线性无关且它们两个能线性表示 α, 取 $G_2=\alpha-G_1=(2, 4, 5)^T$. 同理, 可取 $G_3=\alpha-2G_1=(1, 3, 4)^T$. 易验证 G_2, G_4, G_5 线性无关, G_3, G_4, G_5 线性无关, G_2, G_3 线性无关且能线性表示 α. 因此, 这样选择的 $G=(G_1, G_2, \cdots, G_t)$ 能满足要求.

设秘密 $s=20$, 则 $U(s)=U(20)=\{(b_1, b_2, b_3)\mid 3b_1+5b_2+6b_3=20\}$. 如取 $(b_1, b_2, b_3)=(2, 4, -1)$, 则由秘密份额的产生方法可知相应的秘密份额为

$(s_1, s_2, s_3, s_4, s_5)=(b_1, b_2, b_3)G=(5, 15, 10, 13, 19)$.

当 P_1, P_3 要恢复秘密时, 他们先求出 $(G_1, G_2)(x_1, x_2)^T=\alpha$ 的一个解, 如 $x_1=1$, $x_2=1$, 然后可计算出 $s=x_1s_1+x_2s_2=5+15=20$.

当 P_1, P_2, P_3 要恢复秘密时, 他们先求出 $(G_1, G_2, G_3)(x_1, x_2, x_3)^T=\alpha$ 的一个解, 如 $x_1=5$, $x_2=-3$, $x_3=4$ 然后可计算出 $s=x_1s_1+x_2s_2+x_3s_3=25-45+40=20$. 类似地, 其它

合格子集亦可容易地恢复出秘密.

又,当 P_1, P_5 试图恢复秘密时,由于 G_1, G_5, α 线性无关,他们无法得到 x_1, x_2 使 $s = x_1 s_1 + x_2 s_2$,只能对 x_1, x_2 做随机猜测,因而得不到关于 s 的任何有用信息.

3.3.2 门限方案的例子

Shamir 门限方案和矩阵方法门限方案都是我们的方法的特例,先来看 Shamir 门限方案:

设有 n 个参与者,门限为 t. 参与者集合为 $P = \{P_1, P_2, \cdots, P_n\}$,这时接入结构的基 $\Gamma_0 = \{A \subset P \mid |A| = t\}$. 分发者 D 首先选择 $GF(q)$ 上的 n 个互不相同的非零元 $a_1, a_2, \cdots, a_n$,可取 $G_j = (1, a_j, a_j^2, \cdots, a_j^{t-1})^T$, $j = 1, 2, \cdots, n$, $G = (G_1, G_2, \cdots, G_n)$. 取 $\alpha = (1, 0, 0, \cdots, 0)^T$,容易证明 G 的任意 t 列是线性无关的并且可以线性表示 α,而 G 的任意 $t-1$ 列都不能线性表示 α. 对秘密 s 来说, $U(s) = \{(s, c_1, c_2, \cdots, c_{t-1}) \mid c_j \in GF(q)\}$. 随机取 $c_1, c_2, \cdots, c_{t-1} \in GF(q)$,令 $(b_1, b_2, \cdots, b_t) = (s, c_1, c_2, \cdots, c_{t-1})$. 于是 D 可计算出秘密份额 $(s_1, s_2, \cdots, s_n) = (s, c_1, c_2, \cdots, c_{t-1}) G$,其中 $s_j = s + c_1 a_j + c_2 a_j^2 + \cdots + c_{t-1} a_j^{t-1}$, $j = 1, 2, \cdots, n$,即 D 用于分发秘密的多项式 $f(x) = s + c_1 x + c_2 x_2 + \cdots + c_{t-1} x^{t-1}$. 若某 t 个参与者,不妨设为 $P_1, P_2, \cdots, P_t$ 要一起恢复秘密,他们可由 $(G_1, G_2, \cdots, G_t)(x_1, x_2, \cdots, x_t)^T = \alpha$,解出 $(x_1, x_2, \cdots, x_t)$,然后可计算出秘密 $s = (s_1, s_2, \cdots, s_t)(x_1, x_2, \cdots, x_t)^T$,这一表示式与由拉格朗日插值公式得到的结果完全相同.

矩阵方法门限方案明显地是本文方法的特例,也是 Shamir 门限方案地一般化表示,在此就不做详细叙述了.

4 性能分析

4.1 计算复杂度分析

分配算法的复杂度为 $O(t^2)$,所需的乘法次数为 nt.

恢复算法的复杂度 $O(t^3)$,所需的乘除法次数的上界为 $t^3/3 + t/3$,其中主要的计算量($t^3/3 - 2t/3$ 次乘除法)来自最小合格子集中的 t 个成员(从最坏的情况考虑)合作解一个 t 元线性方程组. 而这一过程可进行预计算并可根据 G 的具体取值进行简化,对效率并无大的影响.

4.2 安全性

在参与者及分发者都是诚实的假设下,对这类分享体制的攻击有两种:

(1)攻击者试图找出分发者分发秘密时所用的 $(b_1, b_2, \cdots, b_t)$. 由于 $(b_1, b_2, \cdots, b_t)$ 是在 $U(s)$ 中随机选取的,且 $|U(s)| = q^{t-1}$,攻击者找到正确的 $(b_1, b_2, \cdots, b_t)$ 的概率仅为 $1/q^{t-1}$.

(2)非合格子集试图恢复秘密. 设有 k 个参与者 $P_{j1}, P_{j2}, \cdots, P_{jk}$,他们构成一个非合格子集. 他们要恢复秘密 s,就必须找到 $x_{j1}, x_{j2}, \cdots, x_{jk}$,使 $x_{j1}s_{j1} + x_{j2}s_{j2} + \cdots + x_{jk}s_{jk} = s$. 由于 $x_{j1}s_{j1} + x_{j2}s_{j2} + \cdots + x_{jk}s_{jk} = (s_{j1}, s_{j2}, \cdots, s_{jk})(x_{j1}, x_{j2}, \cdots, x_{jk})^T = (b_1, b_2, \cdots, b_t)(G_{j1}, G_{j2}, \cdots, G_{jk})(x_{j1}, x_{j2}, \cdots, x_{jk})^T$,要使其值等于 $s = (b_1, b_2, \cdots, b_t)\alpha$,就必须使 $\beta = (G_{j1}, G_{j2}, \cdots, G_{jk})(x_{j1}, x_{j2}, \cdots, x_{jk})^T$ 满足 $(b_1, b_2, \cdots, b_t)(\alpha - \beta) = 0$ 且 β 不同与 α(因为 $(G_{j1}, G_{j2}, \cdots, G_{jk})(x_{j1}, x_{j2}, \cdots, x_{jk})^T = \alpha$ 是无解的). 由于 $(b_1, b_2, \cdots, b_t)$ 是未知的,他们无法得到这样的 β,因此也就无法得到使 $x_{j1}s_{j1} + x_{j2}s_{j2} + \cdots + x_{jk}s_{jk} = s$ 的 $x_{j1}, x_{j2}, \cdots, x_{jk}$,于是他们攻击成功就相当于在 $GF(q)$ 中随机猜测 s 取得成功,这样的概率仅为 $1/q$.

因此我们的体制是安全的. 至于在参与者及分发者中存在不诚实者的情况下,如何检测行骗者也是重要问题,需另进行讨论.

5 结束语

非门限秘密分享体制在信息安全与数据保密中有着广泛的应用. 本文提出了具有传递性质的接入结构的概念,这一类接入结构包含了所有的门限接入结构,又含有大量的非门限接入结构,因而在实际中具有重要意义. 同时本文还给出了构造这类接入结构上的秘密分享体制的一种简单易行的方法. 在以本文的方法构造的秘密分享方案中,信息速率为 1,当一组参与者分享一个秘密时,不管一个参与者属于多少个最小合格子集,他都只需保存一个秘密份额,而不需要象在其它一些非门限方案中那样,参与者属于多少个最小合格子集就得保存多少个秘密数据. 一些常见的门限体制是我们体制的特例. 由于这些特点,本文的方法具有很大的实用价值. 分析表明以本文的方法构造的秘密分享体制是安全可靠的.

参考文献:

[1] Shamir A. How to share a secret [J]. Communications of the ACM, 612 – 613.

[2] Blakley G R. Safeguarding cryptographic keys [A]. Proceedings of the National Computer Conference [C], 1979, 48: 242 – 268.

[3] 王育民, 刘建伟. 通信网的安全-理论与技术 [M]. 西安: 西安电子科技大学出社, 1999: 215 – 218.

[4] Asmuth C, et al. A Modular approach to key safeguarding [J]. IEEE Transactions on Information Theory, 1983, IT-29(2): 208 – 210.

[5] Kamin E D, et al. On sharing secret systems [J]. IEEE Trans. On Information Theory, 1983, IT-29(4): 35 – 41.

[6] Benaloh J, et al. Generalized secret sharing and monotone functions [A]. Advances in Cryptology-CRYPTO' 88 [C], Spring, Berlin, 1990: 27 – 35.

[7] Dawson E, et al. The breadth of Shamir's secret sharing scheme [J]. Computers and security, 1995, 13(2): 69 – 78.

[8] Tan K J, et al. General secret sharing scheme [J]. Computer Communications, 1999, 22: 755 – 757.

作者简介:

张福泰 男. 1965 年生于山西省陇县. 1990 年获基础数学专业硕士学位. 现为陕西师范大学计算机科学学院副教授,西安电子科技大学密码学专业博士研究生. 主要研究兴趣为信息安全及电子商务.