# 基于代数半群理论的密钥分享方案 [1]

王永传 李子臣 杨义先

(北京邮电大学信息安全中心 126 信箱 北京 100876)

**摘 要** 如何将密钥信息分配给 $n$ 个被授权的单位 ( 记为: $S_1, S_2, \cdots, S_n$), 每一个被授权单位 $S_i(i = 1, 2, \cdots, n)$ 有 $q_i$ 个被授权人, 使得每一个被授权人所得到的密钥信息与该授权人所在的单位的任何其他被授权人所得到的密钥信息是一致的, 而任意 $k$ 个被授权人所得到的密钥信息, 若至少包含每一个被授权单位中的至少一个被授权人的密钥信息时, 能够恢复完整的密钥信息, 其他情形时, 无法完全恢复密钥信息, 这种需要经常会遇到。本文利用代数半群理论, 给出了一种能实现这种密钥分享的方案.

**关键词** 半群, 密钥分享, 密码学

**中图号** TN918.1

## 1 引 言

由 Blakley[1] 和 Shamir[2] 提出的秘密分享方案, 解决的主要问题为: 如何将一个数据 $D$ 分成 $n$ 块, 使得 $D$ 容易从任意 $k(k \leq n)$ 块中得到, 而即使完全知道 $k-1$ 块中的信息, 也不能得到 $D$ 。现有的文献主要研究如何得到理想的秘密分享方案来解决上述问题, 以及对解决上述问题的秘密分享方案的刻划. 对于现实生活中遇到的其他情形时的问题, 比如: 有一个公司老板, 拥有一个密钥信息, 保管着一些重要的资料。如果老板要出外, 为保证他不在时, 其他人员能够获得密钥信息, 得到所需资料。老板可以授权给几个部门, 每一个被授权部门有几个被授权的人, 每个被授权人获得部分密钥信息。在同一个被授权部门中, 根据任一被授权人被分配到的密钥信息所能得到的信息是相同的, 根据任意几个部门被授权人的密钥信息无法得到其他部门的密钥信息. 而如果任意把至少每一个被授权部门有一个被授权人的密钥信息综合, 就可得到完整的密钥信息。但其他情形无法得到完整的密钥信息. 这种情形, 相当于把一个密钥的信息分成几类, 每一类密钥信息能确定一类特殊信息, 对每一类密钥信息分配给几个被授权人分享, 使得享有同一类密钥信息的任一被授权人能拥有整个这一类的密钥信息, 而任意享有几类密钥信息的被授权人, 无法获得其他类的任何信息。以前的秘密分享方案无法满足这种要求, 需要新型的密钥分享方案。本文把代数半群理论引入密码学, 构造了一种能满足这种要求的密钥分享方案, 该方案与已有的秘密分享方案 $(t, n)$ 门限方案 (比如: 文献 [2] 利用插值方式给出的方案及文献 [3] 利用几何方式给出的方案) 相比, 可以避免同一被授权单位的几个被授权人合谋. 代数半群理论在密码学中的进一步应用, 需要更深入的研究.

## 2 代数半群

一个非空集合 $S$, 具有二元运算 $u$, 即存在一个映射 $u : S \times S \to S$, 则称 $(S, u)$ 为一个群胚或广群; 若映射 $u$ 满足结合律, 即 $(\forall x, y, z \in S)$ 有 $((x, y)u, z)u = (x, (y, z)u)u$, 则称 $(S, u)$ 为一个半群. 记 $(x, y)u = xy$, 称为半群乘积, 记半群为 $(S, \cdot)$ 或简单记为 $S$ 。$S$ 的势 $|S|$ 称为半群 $S$ 的阶。若 $S$ 为一个半群, $T$ 为 $S$ 的非空子集, 如果按照 $S$ 的运算对 $T$ 是封闭的, 称 $T$ 为 $S$ 的一个子半群。如果 $\{U_i : i \in I\}$ 为半群 $S$ 的一族非空子半群, 则 $\bigcap\{U_i : i \in I\}$ 或为空集, 或为 $S$ 的一个子半群. 若 $A$ 为半群 $S$ 的一个非空子集, 则包含 $A$ 的 $S$ 的子半群存在, $S$

[1] 1998-11-10 收到, 1999-05-19 定稿
国家自然科学基金资助课题 (批准号: 69772035, 69882002), 国家 "863" 项目

即为其中一个。半群 $S$ 的所有包含 $A$ 的子半群的交也是一个 $S$ 的子半群，记为 $< A >$。若 $A=\{a_1,a_2,\cdots,a_n\}$，则记 $< A >=< a_1,a_2,\cdots,a_n >$。若 $A=\{a\}$，则 $< a >=\{a,a^2,a^3,\cdots\}$，这时称 $< a >$ 为由 $a$ 生成的 $S$ 的单演子半群；若 $S=< a >$，则称 $S$ 为单演半群。$< a >$ 的阶称为 $a$ 的阶。若 $\{x\in N:(\exists y\in N)a^x=a^y,x\neq y\}\neq\emptyset$，称这个集合的最小元素 $m$ 为 $a$ 的指数；这时 $\{x\in N:a^{m+x}=a^m\}$ 非空集且存在最小元素 $r$，称为 $a$ 的周期。$m,r$ 亦分别称为 $< a >$ 的指数和周期。这时 $< a >=\{a,a^2,\cdots,a^m,a^{m+1},\cdots,a^{m+r-1}\}$。

**引理 1** 若半群 $S=< A >$，$A$ 为非空子集，则 $S$ 的所有元素可表示为 $A$ 中有限个元素的乘积。

这时，$A$ 称为半群 $S$ 的生成子集合或称 $A$ 为 $S$ 的生成集。

**引理 2** 设有一个半群 $S=< a_1,a_2,\cdots,a_n >$，对于 $\forall a_i(i=1,2,\cdots,n)$ 有 $|< a_i >|=q_i,q_i$ 为素数，且 $a_i$ 的周期为 $q_i$，则对于任意 $x_i\in< a_i >,x_i\neq a_i^{q_i}$，有 $< x_i >=< a_i >$，且 $S=< x_1,x_2,\cdots,x_n >$。

**证明** 若 $|< a_i >|=q_i,q_i$ 为素数，且 $a_i$ 的周期为 $q_i$，则 $a_i^{q_i}$ 为单位元，且 $< a_i >$ 为一个循环群。对于 $x_i\in< a_i >$，不妨令 $x_i=a_i^l$，因为 $q_i$ 为素数，则 $(l,q_i)=1$。存在 $n,t\in Z$，有 $lt+nq_i=1$，于是 $a_i=a_i^{lt+nq_i}=a_i^{lt}a_i^{nq_i}=(a_i^l)^t=(x_i)^t$，由引理 1，$< a_i >=< x_i >$ 成立。对于任意 $x\in< a_1,a_2,\cdots,a_n >$，$x$ 为 $\{a_1,a_2,\cdots,a_n\}$ 中元素的有限个乘积，而每一个 $a_i$ 可表示为 $x_i$ 的幂，故 $< a_1,a_2,\cdots,a_n >\subseteq< x_1,x_2,\cdots,x_n >$，而显然 $< x_1,x_2,\cdots,x_n >\subseteq< a_1,a_2,\cdots,a_n >$，$S=< x_1,x_2,\cdots,x_n >$。 证毕

## 3 密钥分享方案

为了解决引言中提出的问题，我们把一个满足引理 2 中条件的半群 $S=< a_1,a_2,\cdots,a_n >$ 作为密钥信息，把 $S$ 的子半群 $S_i=< a_i >(i=1,2,\cdots,n)$ 作为被授权的部门，每一个被授权部门中有 $q_i-1$ 个被授权人得到部分密钥信息，每一个部分密钥信息为从 $< a_i >$ 中取的 (不包含其单位元) 任意元素，由引理 2，这时满足：

(1) 任一被授权人所得到的部分密钥信息，与同一个被授权部门的其他被授权人所得到的部分密钥信息一致；

如果半群 $S$ 同时满足：

($\star$) 对任意 $i(1\leq i\leq n)$，有 $< a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n >\bigcap< a_i >=\emptyset$，则按照上述密钥分享方法，满足：

(2) 任一被授权人依据所得到的部分密钥信息，无法得到其他被授权部门的密钥信息；

(3) 根据任意 $k$ 个被授权人，如果至少包含每一个被授权部门的至少一个被授权人，所得到的密钥信息，能够完整的恢复密钥信息。

(4) 从任意几个被授权部门所拥有的密钥信息中，无法得到其他被授权部门的密钥信息. 这样，解决我们提出的问题，归结为寻找一个半群 $S$，使得 $S$ 满足条件 ($\star$) 和引理 2 中的条件。

## 4 方案的实现

Step 1 任意选择 $n$ 个两两互不相交的有限群，$G_1,G_2,\cdots,G_n$，使得 $|G_i|=q_i$，$q_i$ 为素数；

Step 2 选择一个良序的半格 $Y$，使得 $|Y|=n$，并且对任意 $\alpha,\beta\in Y$，有 $\alpha\leq\beta$ 或 $\beta\leq\alpha$ 总成立；令 $S=\bigcup\{G_i:1\leq i\leq n\}$，定义一个 $S$ 到 $Y$ 的满射 $\phi$，使得 $G_i=\phi^{-1}\alpha$，重新记

$G_i = G_\alpha$, 依次下去；对于每一对 $Y$ 中的元素 $\alpha, \beta$, 不妨设 $\alpha \geq \beta$, 令 $\varphi_{\alpha,\beta} : G_\alpha \to G_\beta$, 为一个同态映射，满足：

(1) 对任意 $\alpha \in Y$, $\varphi_{\alpha,\alpha}$ 是 $G_\alpha$ 上的恒等映射；

(2) 对于 $\alpha, \beta, \gamma \in Y, (\alpha \geq \beta \geq \gamma)$, 有 $\varphi_{\alpha,\beta}\varphi_{\beta,\gamma} = \varphi_{\alpha,\gamma}$ .

Step **3**　在 $S$ 上定义乘法运算 "$*$": 对任意 $a_\alpha \in G_\alpha, b_\beta \in G_\beta$, 有

$$a_\alpha * b_\beta = (a_\alpha \varphi_{\alpha,\alpha\beta})(b_\beta \varphi_{\beta,\alpha\beta});$$

对任意 $a, b \in G_\alpha, a * b = a \cdot b$, 这里 "$\cdot$" 作为群的乘法. 这样得到的 $(S, *)$ 为一个半群，满足引理 2 的条件和条件 $(\star)$ .

**5 方案的讨论**

(1) 首先，本文引言部分给出的问题，在现实生活中经常会遇到，比如：在军事上，将军拥有的密钥信息，控制着某些重要材料，可以授权给下属几个兵种的上校，从而可以按照我们给出的方案；在学生的档案管理方面，每个学校的所有档案由校长所拥有的密钥信息控制，校长可以授权给各个系主任部分密钥信息，也可按照我们给出的方案. 总之，我们的方案有其广泛的应用背景.

(2) 我们把问题归结为寻求满足某些特定条件的半群，从而把半群理论应用于密码学的研究之中，为半群理论在密码学中的进一步应用的更深入研究创造了条件.

(3) 本文给出的仅是一种构造方法，比如：在 Step3 中，我们定义 S 的乘法 "$*$" 为 $\forall a, b \in S$, 如果存在 $G_i$, $a, b \in G_i$, 则 $a * b$ 按照 $G_i$ 中的乘法；若 $\exists i, j (i \neq j)$, 有 $a \in G_i, b \in G_j$, 则 "$*$" 按照左零运算，即 $a * b = a$, 只要一元素在左边，与任意不与 $a$ 在同一群中的元素进行 "$*$" 运算时，总是等于该元素. 这时 $(S, *)$ 亦为满足条件的半群. 寻找比较好的构造方法，构造这种类型的半群，是一类值得研究的半群构造问题，可以利用已有的这类半群的构造方法，这归结为文献 [4] 中的 "Unions of Groups" 问题.

(4) 在我们所采用的构造方法中，首先是一系列的素数阶的群，可以采用群论中给出的构造方法实现.

(5) Step2 中先要选择一个有特殊条件的良序半格，这种半格是容易找到的，比如：对于一系列自然数集合 $N$, 在其上定义大小关系为数的大小比较关系，定义其乘法运算 "$\circ$": 任意 $a, b \in N$, $a \circ b = b \circ a = a \iff a \leq b$, 则 $(N, \leq, \circ)$ 构成一个满足我们要求的良序半格.

(6) Step2 中另一个需要考虑的重要方面是，同态映射 $\varphi$ 的构造，可以参见文献 [4] 中给出的内容，比如 Clifford 半群为群的强半格，就给出了一种特殊的同态映射.

(7) 本方案的安全性依赖于 "Unions of Groups" 的多样性，及半群定义条件的简单性. 半格算法，同态映射算法，半群算法，以及各个群的算法只要有一个不知道，就无法确定整个半群信息. 而每一种算法都有多种，足以提供对方案的安全保障.

(8) 如果每一个群仅含有一个元素，这时得到的半群为带 (每一个元素都为幂等元的半群)，这时密钥信息的分享方案中，将部分密钥分给每一个人，成为一个 $(n, n)$- 门限方案，从这种意义上讲，本文的方案为一个广义化的门限方案.

总之，相信对这类方案的研究会引起人们的关注.

**致谢**　感谢审稿者提出的有益建议和修改意见，审稿者指定的参考文献及对本文的修正，作者受益颇深.

## 参 考 文 献

[1] Blakley G R. Safeguarding cryptographic keys, In proceedings of the AFIPS 1979 national computer conference, Arlington: 1979, 313-317.

[2] Shamir A. How to share a secret, Communications of the ACM, 1979, 22(1): 612-613.

[3] Simmons G J. How to (really) share a secret, Proc. of crypto'88, LNCS403, Springer-verlag, Berlin: 1990, 390-448.

[4] Howie J M. An introduction to semigroup theory, Academic Press, Inc., New York: 1976, 89-124.

[5] Stinson D.R. Cryptography : Theory and practice, New York : CRC Press, Inc., 1995. 259-281, 327-359.

# A SECRET KEY DISTRIBUTIONS SCHEME BASED ON THE THEORY OF ALGEBRAIC SEMIGROUPS

Wang Yongchuan Li Zichen Yang Yixian

(*Beijing University of Posts and Telecommunications, Beijing* 100876)

**Abstract** How to distribute a secret key information to $n$ authorized departments (denoted as: $S_1, S_2, \cdots, S_n$, respectively). For every autherized department $S_i (i = 1, 2, \cdots, n)$, there are $q_i$ authorized persons, and every authorized person has the same secret key information as that of any other authorized persons in the same authoried department. The secret key information can be reconstructed completely from the secret key information of any $k$ authorized persons, if there is at least one authorized person included for every authorized department. But other cases, the secret key information cannot be reconstructed completely. In this paper, based on the algebraic semigroup theory, a secret key sharing scheme is proposed, which can satisfy the demand.

**Key words** Semigroup, Secret key sharing, Cryptography

王永传： 男， 1969 年生，博士，主要研究方向：现代密码学，信息安全，认证理论，数字签名，密钥分享等.

李子臣： 男， 1964 年生，博士，主要研究方向：密码学，信息安全，数字签名等.

杨义先： 男， 1961 年生，教授，博士生导师，全国政协委员，主要研究方向：编码密码学，信息安全，Internet/Intranet 技术，神经网络，防火墙技术，数字水印，替像术，叠像术，替音术，信息伪装，应用数学等.