秘密共享中的双陪集结构

林群
韩山师范学院 数学与统计学院，广东 潮州 521041
DOI:10.61369/ASDS.2026030008

摘　　要： 线性秘密共享方案（LSSS）为现代密码协议提供了计算高效的基石，而代数结构的引入能极大地丰富其理论与应用内涵。本文旨在将群论中的双陪集结构系统性地嵌入秘密共享框架，构建一个兼具代数严谨性与密码学实用性的新模型。首先，形式化定义了基于双陪集的秘密共享方案，阐明其如何将秘密编码为群中的双陪集，并将份额生成与恢复过程转化为群元素运算。其次，深入探讨了该方案的核心代数基础，即群作用下的轨道空间与访问结构的群论表征。并通过基于矩阵群的具体实例，展示了该模型在实现多级秘密共享方面的独特优势。双陪集结构所提供的代数工具，不仅能够自然地支持多级秘密共享，其内在的对偶性也使得设计高效安全的协议成为可能。这一框架在安全多方计算、分布式存储以及量子密码学等多个前沿领域展现出重要的应用潜力。

关 键 词： 秘密共享；双陪集；对偶方案；访问结构

On the Double Coset Structure in Secret Sharing

Lin Qun
Institute of Mathematics and Statistics, Hanshan Normal University, Chaozhou, Guangdong 521041

Abstract: Linear secret sharing schemes (LSSS) provide a computationally efficient foundation for modern cryptography. To extend their expressiveness and theoretical depth, this paper systematically integrates the double coset structure from group theory into the secret sharing framework, establishing an algebraically rigorous yet practical model. We first formally define a double coset–based secret sharing scheme, explaining how secrets are encoded as double cosets and how share generation and recovery are realized through group operations. We then investigate its core algebraic foundations, particularly the orbit space under group action and the group–theoretic characterization of access structures. A concrete example based on matrix groups is provided to illustrate how to support hierarchical secret sharing. The double coset structures not only enrich the expressiveness of hierarchical secret sharing but also make it possible to design efficient and secure protocols due to its inherent duality. This framework shows significant promise for applications in secure multi–party computation, distributed storage, and quantum cryptography.

Keywords: secret sharing; double coset; dual scheme; access structure

引言

秘密共享是密码学中保障信息分布式安全的核心技术，其标准线性模型（LSSS）因其同态性与计算效率而得到广泛应用[1]。然而，传统 LSSS 通常将秘密视为有限域中的标量，其访问结构的表达能力虽强，但构造方式与代数高阶结构的结合尚有深化空间[2]。近年来，利用群、环、模等代数对象来重构密码原语，已成为提升方案表达能力与安全性的重要研究方向[3–6]。

在群论中，给定一个有限群 G 及其两个子群 H 与 K，双陪集 HgK 构成 G 的一个自然划分。这种结构在表示论、组合设计等领域成果丰硕[7]，其内在的对称性与层次性为编码复杂策略提供了天然的数学语言[8]。将秘密映射为某个双陪集，并将份额设计为该陪集中的随机化元素，可以自然地将参与者的恢复能力与他们在群作用下的“视角”相关联。这种思想最早可追溯到 Blundo 等人关于几何秘密共享的探讨[9]。

本文旨在系统构建一个基于双陪集结构的秘密共享理论框架。通过精心选择群 G 和子群 H，K，双陪集方案可以导出具有明确描述的份额，从而与经典 LSSS 框架无缝衔接。更重要的是，双陪集视角为理解访问结构提供了新的群论诠释：一个参与者子集能否恢复秘密，等价于其对应的群元素集合能否共同确定唯一的双陪集。这种诠释使得我们可以利用群表示的成熟理论[10]，来分析和构造具有复杂权限关系的秘密共享方案。

基金项目：潮州市科技计划项目（2025ZC29），韩山师范学院理科重点项目 (XN202028)。
作者简介：林群，韩山师范学院数学与统计学院，讲师，研究方向为密码学与信息安全。

本文结构如下：第一节阐述线性秘密共享与双陪集的基本定义；第二节形式化定义基于双陪集的秘密共享方案（DCSS），并阐述其通用算法；第三节深入探讨 DCSS 的代数基础，重点分析其访问结构的群论特征及其对偶关系；第四节通过基于一般线性群 $GL(n,F_q)$ 的详细实例，展示 DCSS 如何实现多级秘密共享与灵活的访问控制；最后总结该框架的优势、挑战及未来研究方向。

一、预备知识

（一）线性秘密共享方案（LSSS）

设 F_q 为有限域，参与者集合为 $P=\{P_1,\ldots,P_m\}$，线性秘密共享方案（LSSS）可以由生成矩阵 $M\in F_q^{l\times m}$ 定义。

秘密 $s\in F_q$ 与随机向量 $\mathbf{r}\in F_q^{l-1}$ 构成向量 $\mathbf{v}=(s,\mathbf{r})$，份额向量 $\mathbf{s}=(s_1,\ldots,s_m)$ 通过 $\mathbf{s}=\mathbf{v}M$ 计算。参与者子集 $A\subseteq P$ 为授权集，当且仅当存在重构系数向量 $\mathbf{c}_A$ 使得 $M_A\mathbf{c}_A^{\top}=(1,0,\ldots,0)^{\top}$，其中 M_A 是 M 中对应于 A 的列构成的子矩阵。此时，秘密可通过授权份额的线性组合恢复，即 $s=\sum_{i\in A}c_is_i$。

（二）陪集

陪集是群论中的一个基本概念，它描述了群在某个子群作用下的轨道结构，为刻画群的对称性与内部划分提供了重要工具[11]。

给定一个群 G 及其子群 $H\le G$，对于 $\forall g\in G$，集合 $gH=\{gh|\ h\in H\}$ 称为 H 在 G 中的一个左陪集，而 $Hg=\{hg|\ h\in H\}$ 则称为右陪集。下面只讨论左陪集。

左陪集的核心性质如下：

1. 划分性质：所有左陪集构成 G 的一个划分，即

$$G=\bigcup_{g\in G}gH$$

且不同陪集无公共元素。

2. 等势性：每个左陪集与子群 H 等势，即 $|gH|=|H|$。

3. 陪集代表元：左陪集中的任意元素均可作为该陪集的代表元，即若 $g'\in gH$，则 $g'H=gH$。

4. 陪集空间与商群：所有左陪集的集合记作 G/H，称为 H 在 G 中的陪集空间。当 H 是正规子群（即对 $\forall g\in G$，$gH=Hg$ 成立）时，可在 G/H 上定义群运算，使之成为一个群，称为商群。

（三）双陪集

设 G 为有限群，子群 $H,K\le G$。对于 $g\in G$，集合 $HgK=\{hgk|\ h\in H,k\in K\}$ 称为 g 的 (H,K) - 双陪集。所有双陪集的集合记为 $H\backslash G/K$，它也构成 G 的一个划分。

双陪集所具有的这种自然划分结构，可作为秘密共享中的理想数学载体。

（四）(k,n) 门限方案

(k,n) 门限方案是秘密共享中最基本且最重要的一类方案，其定义如下[12]：设秘密为 $s\in S$（秘密空间），参与者为 $P=\{P_1,\ldots,P_n\}$。一个 (k,n) 门限方案包含以下两个算法：

1. 份额生成算法

由可信的经销商执行。输入秘密 S，输出 n 个份额 $\{S_i\}_{i=1}^n$，并将 S_i 安全地分发给参与者 P_i。

2. 秘密恢复算法

由参与者子集执行。输入至少 k 个不同的份额，输出原始秘密 S。

注：(k,n) 门限方案的访问结构 Γ 为：$\Gamma=\{A\subseteq P:|A|\ge k\}$，即所有基数至少为 k 的子集都是授权集，所有基数小于 k 的子集都是禁止集。

二、基于双陪集的秘密共享方案

定义 1 双陪集秘密共享方案 (DCSS)

一个双陪集秘密共享方案由以下五元组定义：(G,H,K,f,ψ)，其中：

G：基础群，是方案所有运算和元素所在的“舞台”。

H,K 为 G 的子群（分别称为左掩码子群与右掩码子群）。

$f:S\to H\backslash G/K$：从秘密空间 S 到双陪集空间的单射（称为秘密编码映射）。

$\psi:G\to P$：一个份额分配函数，将群元素映射给参与者。

（一）份额生成算法

算法 1：DCSS 份额生成

- 输入 : 秘密 $s\in S$。

- 输出：分配给各参与者的份额 $\{s_i\}_{i=1}^m\subset G$。

步骤：

1. 编码：计算秘密对应的双陪集 $D=f(s)=Hg_sK$，其中 g_s 为该双陪集的一个代表元。

2. 随机化：独立均匀随机选取 $h\in H$，$k\in K$。

3. 构造核心元素：计算 $x=hg_sk\in D$，注意 x 是双陪集 D 中的一个随机元。

4. 生成与分配份额：利用份额分配函数 ψ，从元素 x 衍生出 m 个份额元 $s_i\in G$，并分配给参与者 P_i。

（二）秘密恢复算法

算法 2：DCSS 秘密恢复

- 输入 : 授权集 $A\subseteq P$ 及其持有的份额 $\{S_i\}_{i\in A}$。

- 输出 : 秘密 $s\in S$。

步骤：

1. 份额合并：授权参与者利用其份额，通过预定的群运算（如比较、乘法、解方程等）共同确定一个双陪集$D'\in H\backslash G/K$。

2. 解码：计算逆映射 $s=f^{-1}(D')$，恢复秘密 s。

注：授权集必须能够从他们的份额中唯一确定秘密所属的双陪集D，而非授权集则不能。

（三）访问结构的群论表征

在 DCSS 中，访问结构Γ由群G，子群H,K以及份额分配方式ψ共同决定。

定义2（双陪集可区分性）：参与者子集A是授权集，当且仅当对于任意两个不同的秘密s_0与s_1，其对应的随机化份额分布（由算法1产生）在A的视角下是可区分的。等价地，A能从其份额计算出一个与双陪集D相关的不变量。

（四）对偶结构

在 LSSS 中，对偶方案由对偶码来定义。在 DCSS 中，存在自然的群论对偶[13]。

定义3（对偶 DCSS）：给定一个 DCSS 方案$\Pi=(G,H,K,f,\psi)$，其对偶方案定义为$\Pi^{\perp}=(G,K,H,f^{\perp},\psi^{\perp})$，其中$f^{\perp}$是将秘密映射到双陪集$K\backslash G/H$的编码，$\psi^{\perp}$是相应的份额分配。若$\Pi$实现访问结构$\Gamma$，则$\Pi^{\perp}$实现其对偶访问结构$\Gamma^{*}$[14、15]，即授权集与禁止集互换。

当$H=K$且方案满足某种自同构性时，可得到自对偶的双陪集方案，这对应于 LSSS 中的自对偶码方案。此时，方案具有最优的份额效率边界。

三、实例分析：基于$GL(2,F_q)$的秘密共享

本节构造一个具体的 DCSS，展示其实现秘密共享的功能。

（一）方案设定

1. 环境群：$G=GL(2,F_q)$，即域F_q上所有2阶可逆矩阵构成的群。

2. 掩码子群：

左掩码子群 $H=\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\middle| a\in F_q\right\}$，（剪切子群，同构于加法群$F_q$）

右掩码子群 $K=\left\{\begin{pmatrix}b & 0\\ 0 & 1\end{pmatrix}\middle| b\in F_q^{*}\right\}$，（缩放子群，同构于乘法群$F_q^{*}$）

3. 秘密编码：对于秘密$s\in F_q$，令其对应的双陪集代表元为

$$g_s=\begin{pmatrix}1 & 0\\ s & 1\end{pmatrix}$$

因此，秘密s被编码为双陪集$D_s=Hg_sK$。

4. 参与者：P_1，P_2 P_3共3人。

（二）份额生成

1. 经销商选择秘密$s\in F_q$，随机选取$a\in F_q$（作为二级秘密）和$b\in F_q^{*}$（作为随机掩码）。

2. 计算核心元素

$$x=hg_sk=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ s & 1\end{pmatrix}\begin{pmatrix}b & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}b(1+as) & a\\ bs & 1\end{pmatrix}$$

3. 构造份额：为每个参与者“绑定”一个特定的a_i，其中$a_1=a$（秘密），a_2,a_3随机选取但满足$a_1+a_2+a_3=0$。参与者P_i获得的份额为：

$$s_i=(u_i,a_i),\quad \text{其中}u_i=b(1+a_is)$$

即(u_i,a_i)实质上是矩阵x_i第一行的两个元素。

（三）秘密恢复

1. 恢复主要秘密s

任意两个参与者P_i,P_j合作。他们拥有$(u_i,a_i),(u_j,a_j)$。注意到

$$u_i=b(1+a_is),\quad u_j=b(1+a_js)$$

两式相除可得

$$\frac{u_i}{u_j}=\frac{1+a_is}{1+a_js}\quad\Rightarrow\quad u_i(1+a_js)=u_j(1+a_is).$$

整理得

$$s(u_ia_j-u_ja_i)=u_j-u_i\quad\Rightarrow\quad s=\frac{u_j-u_i}{u_ia_j-u_ja_i}\quad(\text{假设分母非零})$$

因此，任意两人可恢复s，实现了 (2,3) 门限。

2. 恢复二级秘密a

份额s_i直接包含$a_1=a$，因此任何包含P_1的集合都能恢复a。

（四）性质分析

1. 线性性：份额u_i和a_i均是秘密s、二级秘密a和随机数b的双线性函数（在域F_q上）。因此，该 DCSS 方案在定义下是线性的。

2. 多级秘密：方案自然嵌入了主要秘密s和附属秘密a，且二者具有不同的访问策略，即主要秘密s需要任意两个参与者合作才能恢复，附属秘密a仅需包含P_1的任意集合即可恢复。

注：此实例清晰地展示了双陪集结构如何通过群的自然作用，将复杂的访问策略编码进简单的代数运算中。

四、结束语

本文系统构建了基于双陪集结构的秘密共享代数框架，将秘密共享的构造范式从传统的有限域向量空间，提升至更具一般性的群作用层面。双陪集视角为该领域带来了以下显著优势：

（一）丰富的表达力：能够自然地支持多级秘密共享，并灵活构建复杂的非门限访问结构，突破传统线性方案在策略表达上的局限。

（二）深刻的对称性：对偶方案与自对偶方案的定义在群结构下显得尤为自然，这种对称性源于群自身的代数性质，为方案

分析与优化提供了内在依据。

（三）跨领域工具的可接入性：可充分借助群表示论、代数几何等成熟数学工具，对方案进行严谨的安全性分析与效率优化，促进密码学与纯数学的融合。

展望未来，本研究方向仍具有广阔发展空间：其一，可进一步探索非可解群作为基础群时方案的全新特性；其二，研究双陪集结构在抗量子攻击密码学中的潜在优势；其三，推动该框架在函数秘密共享等高级密码协议中的实际应用。双陪集结构恰如一座桥梁，紧密连接了抽象的代数理论与实用的密码设计，有望催生出更多高效灵活且具备高安全性的新型秘密共享方案。

参考文献

[1]Cramer R, Damgård I, Maurer U. General secure multi-party computation from any linear secret-sharing scheme[C]. In: EUROCRYPT 2000. LNCS, vol. 1807. Springer, 2000: 316-334.

[2] Habeeb M, Kahrobaei D, Koupparis C, et al. Secret sharing using group theory[J]. International Journal of Foundations of Computer Science, 2013, 24(4): 523-536.

[3] Kaboli R, Khazaei S, Parviz M. On ideal and weakly-ideal access structures[J]. Advances in Mathematics of Communications, 2021, 15(1): 17-36.

[4] Xing C, Yuan C. Evolving secret sharing schemes based on polynomial evaluations and algebraic geometry codes[J]. IEEE Transactions on Information Theory, 2024, 70(5): 3718-3728.

[5] Abram D, Roy L, Scholl P. Succinct homomorphic secret sharing[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer Nature Switzerland, 2024: 301-330.

[6] Jafari A, Khazaei S. On Abelian secret sharing: duality and separation[J]. Cryptology ePrint Archive, Report 2019/575, 2019.

[7] Jafari A, Khazaei S. Partial secret sharing schemes[J]. IEEE Transactions on Information Theory, 2023, 69(8): 5364-5385.

[8] Martí-Farré J, Padró C. On secret sharing schemes, matroids and polymatroids[J]. Journal of Mathematical Cryptology, 2010, 4(2): 95-120.

[9] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes.[J].Cryptology 1995, 8(1): 39 - 64.

[10] Alon B, Beimel A, Lasri O. Simplified PIR and CDS protocols and improved linear secret-sharing schemes[C]. In: TCC 2025, LNCS, vol. 16269. Springer, 2025: 365-398.

[11] Beimel A, Othman H, Peter N. Quadratic secret sharing and conditional disclosure of secrets[J]. IEEE Transactions on Information Theory, 2023, 69(11): 7295-7316.

[12] Paskin-Cherniavsky A, Radune A. On polynomial secret sharing schemes[C]. In: ITC 2020, LIPIcs, vol. 163. 2020: 12:1-12:21.

[13] Matúš F. Algebraic matroids are almost entropic[J]. Proceedings of the American Mathematical Society, 2024, 152(1): 1-6.

[14] Beimel A, Farràs O, Moya A. Polynomial secret sharing schemes and algebraic matroids[C]. In: TCC 2025, LNCS, vol. 16269. Springer, 2025: 428-461.

[15] Csirmaz L. Secret sharing and duality[J]. Journal of Mathematical Cryptology, 2021, 15(1): 157-173.

