线性秘密共享中的自对偶结构

林群

韩山师范学院数学与统计学院，广东 潮州 521041

DOI:10.61369/ASDS.2026010008

摘　　要： 线性秘密共享方案（LSSS）是现代密码学中支撑安全多方计算与密码协议的关键基础。本文旨在系统性地构建一个基于线性码的 LSSS 理论框架。首先，形式化线性秘密共享方案，阐述了份额生成与秘密重构的算法流程。其次，阐明了线性码的理论基础，明确了生成矩阵与校验矩阵的核心作用。本文的贡献在于探讨了自对偶码的数学性质，并通过一个具体的二元域实例加以验证。自对偶码因其内在的对称性和优美的结构，为构建高效安全的线性秘密共享方案提供了理论工具，在信息安全及相关领域中具有重要的应用价值。

关 键 词： 线性秘密共享；访问结构；生成矩阵；自对偶码

On the Self-Dual Structure in Linear Secret Sharing

Lin Qun

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

Abstract: Linear secret sharing schemes (LSSS) are a fundamental cornerstone of modern cryptography, underpinning secure multi-party computation and cryptography protocols. This paper aims to systematically construct a theoretical framework for LSSS based on linear codes. First, we formalize LSSS and elaborates on the algorithmic processes for share generation and secret reconstruction. Second, we clarifies the theoretical foundations of linear codes, emphasizing the central role of generator and parity-check matrices. The contribution of this work lies in exploring the mathematical properties of self-dual codes and validating them through a concrete example over the binary field. Owing to their inherent symmetry and elegant structure, self-dual codes provide a theoretical tool for constructing efficient and secure LSSS, holding significant application value in information security and the related fields.

Keywords: linear secret sharing; access structure; generator matrix; self-dual code

引言

完美保密的秘密共享是现代密码学的核心技术之一，为信息的安全分布式存储与计算提供了根本保障。其核心思想是将秘密值分解为多个份额并分发给一组参与者，确保只有经过授权的参与者集合能够联合恢复该秘密，而任何未授权的集合则无法获取关于秘密的任何信息[1-5]。在众多秘密共享方案中，线性秘密共享方案因其线性同态特性备受关注，它最初由 Jackson 与 Martin 提出[6]。该类方案中，份额的计算与授权集合中秘密的恢复仅依赖于线性映射和线性方程组的求解[7-9]，因此具有计算高效的特点。此外，其同态特性使得该方案能够支持安全多方计算、门限密码等高级密码协议[10-12]，从而在隐私计算和数据安全领域发挥着至关重要的作用。

线性秘密共享方案的构造由生成矩阵与访问结构共同定义。生成矩阵不仅通过线性变换将秘密与随机数映射为各参与者的份额，还内在刻画了方案的访问结构，即明确哪些参与者子集能够重构秘密[13]。这种将访问结构嵌入线性代数框架的表示方式，深刻揭示了秘密共享与编码理论之间的内在联系[14、15]。具体而言，线性秘密共享方案可视为一类特殊的线性码，其中有效的码字对应由合法秘密生成的合法份额集合。

在编码理论中，自对偶码因其独特的对称性与优美的数学结构而受到广泛关注。自对偶码要求线性码与其对偶码完全重合，这一强约束条件使得其生成矩阵与校验矩阵具有同一性，并衍生出一系列非平凡性质。这种内在的高度对称性，使自对偶码成为构建具备高效性与安全性的秘密共享自对偶结构的理想工具。

本文旨在系统阐述基于线性码（尤其是自对偶码）的线性秘密共享方案框架。首先，将介绍线性秘密共享方案的形式化定义、份额生成与秘密重构算法，并深入分析其线性性质与同态特性。随后，阐述线性码的基本理论，重点说明生成矩阵与校验矩阵在描述线性码及其对偶关系中的核心作用。最后，聚焦于自对偶码，详细分析其数学性质，并结合具体实例加以说明，同时进一步阐明该类方案在安全多方计算等高级密码协议中的应用潜力及其与其它研究领域的深刻联系。

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：密码学与信息安全。

一、预备知识

（一）线性秘密分享方案的形式化描述

定义1.（线性秘密分享方案）

一个在域F_p上关于参与者集合$P=\{U_1,...,U_m\}$的线性秘密分享方案（LSSS）由以下两个核心组件完全定义[8]：

1. 生成矩阵$M_{l\times m}$：其中1（行数）指秘密向量$v=(s,r_2,r_3,\ldots,r_l)$的维度，S是真正的秘密，$r_2,r_3,...,r_l$是随机数，用于隐藏秘密。m（列数）指参与者的数量，也等于生成的份额数量。

2. 单调访问结构$\Gamma\subseteq 2^P$：这是一个参与者子集的集合，定义了哪些参与者组合可以合法地重构出秘密。它必须满足单调性：即若$A\subseteq B$且$A\in\Gamma$，则必有$B\in\Gamma$。

（二）份额生成算法

算法1.LSSS份额生成

- 输入：秘密$s\in\mathbf{F}_p$，
- 输出：份额向量$(s_1,s_2,\ldots,s_m)\in F_p^m$。

步骤：

1. 构造秘密向量$\mathbf{v}=(s,r_2,r_3,\ldots,r_l)\in\mathbf{F}_p^l$，其中$r_2,r_3,...,r_l$为均匀随机选择的随机数。

2. 计算份额$(s_1,s_2,\ldots,s_m)=\mathbf{v}\cdot M$，并将份额$s_i$分配给参与者$U_i$（$i=1,2,\ldots,m$）。

（三）访问结构的矩阵表征

生成矩阵M不仅定义了如何生成份额，还隐式地定义了访问结构（即哪些参与者集合可以恢复秘密）。

定义2.（授权集[8]）对于生成矩阵$M\in\mathbf{F}_p^{l\times m}$，参与者子集$A\subseteq P$称为授权集，当且仅当存在系数向量$\boldsymbol{c}=(c_1,c_2,\ldots,c_{|A|})\in\mathbf{F}_p^{|A|}$，使得$M_A\cdot\boldsymbol{c}^T=(1,0,0,...,0)^T$. 其中$M_A$表示矩阵$M$中对应于集合$A$的列的子矩阵。访问结构$\Gamma$即为所有授权集的集合$\Gamma=\{A\subseteq P\mid\exists\boldsymbol{c}\in\mathbf{F}_p^{|A|}$使 $M_A\cdot\boldsymbol{c}^T=(1,0,0,...,0)^T\}$。

（四）秘密重构算法

算法2.LSSS秘密重构

- 输入：授权集$A\in\Gamma$及其份额$\{s_i\}_{i\in A}$，
- 输出：秘密$s\in\mathbf{F}_p$.

步骤：

1. 求解线性方程组$M_A\cdot\boldsymbol{c}^T=(1,0,0,...,0)^T$，得到重构系数$\boldsymbol{c}=(c_1,c_2,\ldots,c_{|A|})$.

2. 计算秘密：

$$s=\sum_{i\in A}c_i s_i$$

即秘密可以通过将授权集中的份额进行线性组合恢复出来。

（五）线性性质

LSSS满足以下线性性质[8]：

1. 份额生成线性：每个份额$s_i(i=1,2,\ldots,m)$是秘密s和随机数r_j（$j=2,\ldots,l$）的线性函数。

2. 秘密重构线性：秘密s可表示为授权份额$\{s_i\}_{i\in A}$的线性组合，其中$A\in\Gamma$.

3. 同态性：假定两个秘密s，s'的对应份额分别为$\{s_i\}_{i\in A}$，$\{s'_i\}_{i\in A}$，则$\{s_i+s'_i\}_{i\in A}$是秘密$s+s'$对应的有效份额。

二、基于线性码的LSSS框架

定义3.（线性码[8]）设F_p是一个包含p个元素的有限域，其中p为素数。一个参数为$[n,k]$的线性码C是向量空间F_p^n的一个k维线性子空间。其中n称为码的长度，即码字的长度。k称为码的维数，即子空间的维度。码中的码字总共有$|C|=p^k$个。

一个线性码C可以由以下两种矩阵之一完全描述：

（一）生成矩阵

设$\{g_1,g_2,\ldots,g_k\}\subset F_p^n$是子空间$C$的一组基。将其作为行向量，构成一个$k\times n$的矩阵$G$，称为码$C$的生成矩阵，即

$$G=\begin{pmatrix}g_1\\g_2\\\vdots\\g_k\end{pmatrix}=\begin{pmatrix}g_{11}&g_{12}&\cdots&g_{1n}\\g_{21}&g_{22}&\cdots&g_{2n}\\\vdots&\vdots&\ddots&\vdots\\g_{k1}&g_{k2}&\cdots&g_{kn}\end{pmatrix}$$

码$C=\{u\cdot G\in F_p^n\mid u\in F_p^k\}$可以由其生成矩阵$G$线性生成，即信息向量$u$通过线性变换$G$被编码为码字$c=u\cdot G$。

（二）校验矩阵

作为一个k维子空间，线性码C在F_p^n中的对偶空间（或零化空间）是$n-k$维的。这个对偶空间本身也是一个线性码，记为$C^\perp$，称为C的对偶码[8]。设$C^\perp$的一组基为$\{h_1,h_2,\ldots,h_{n-k}\}$，将这些基向量作为行，形成一个$(n-k)\times n$的矩阵$H$，称为码$C$的校验矩阵。即

$$H=\begin{pmatrix}h_1\\h_2\\\vdots\\h_{n-k}\end{pmatrix}$$

码C可以等价地定义为校验矩阵H的零空间：

$$C=\{c\in F_p^n\mid H\cdot c^T=0\in F_p^{n-k}\}$$

这种对偶关系在秘密共享中有重要应用：若线性码C定义一个线性秘密分享方案S，则$C^\perp$对应S的对偶方案S^*。

（三）生成矩阵与校验矩阵的关系

如果一线性码C有一个$k\times n$的生成矩阵G，那么它就存在一个$(n-k)\times n$的校验矩阵H，使得$H\cdot G^T=0$或者$G\cdot H^T=0$.

这意味着生成矩阵G的所有行向量都与校验矩阵H的所有行向量正交。

结论：1. 校验矩阵H其实就是对偶码$C^\perp$的生成矩阵。

2. 码C由G的行张成，而对偶码$C^\perp$由H的行张成。

三、自对偶码

定义4.（自对偶码[8]）如果一个码C满足$C=C^\perp$，则称C为一

个自对偶码。这意味着：一个向量是C的一个有效码字，当且仅当它与C中的每一个码字都正交，即点积为零。

从定义$C=C^{\perp}$可以推导出以下性质：

性质1：自对偶码的码字长度n必须是偶数，并且其维度$k=\frac{n}{2}$。

证：设一个码C的长度是n，维度是k，则它的对偶码的维度是$n-k$。

由于$C=C^{\perp}$，它们的维度必须相等，即$k=n-k$，

从而推出$k=\frac{n}{2}$，n必为偶数。

性质2：生成矩阵与校验矩阵本质一致。

证：由于$C=C^{\perp}$，生成矩阵G能张成C，也必能张成$C^{\perp}$，

而$C^{\perp}$的生成矩阵是原码C的校验矩阵H。

因此，生成矩阵G和校验矩阵H在本质上是同一个矩阵，它们张成相同的行空间。所以，通常使用同一个矩阵G来同时担任生成和校验的角色，即$G=H$。

性质3：生成矩阵G必须满足正交性$GG^{T}=0$。

证：生成矩阵G和校验矩阵H满足$GH^{T}=0$，又由性质2，知$G=H$，从而推出$GG^{T}=0$。

例：在二元域 构造生成矩阵$G=\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}$，

有 $GG^{T}=\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix}^{T}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$。

给定F_2上向量$\mathbf{u}=(u_1,u_2)$，计算码字$c=\mathbf{u}\cdot G$，推出

$$C=\left\{\mathbf{u}\cdot G|\ \mathbf{u}\in F_2^2\right\}=\left\{(0,0,0,0),(1,0,0,1),(0,1,1,0),(1,1,1,1)\right\}$$

可以检验C中的码字两两正交，所以C是自对偶码。

对于一个自对偶的LSSS，其访问结构Γ满足：一个集合是授权集，当且仅当它的补集是禁止集。

自对偶码具有强烈的内在对称性，这使其在理论和应用上成为一个非常强大的工具。它具有重要的应用价值：

1. 优美的对称性：它具有极其优美的数学结构，这使其更容易分析和实现。

2. 在密码学中的应用：它是构建自对偶线性秘密分享方案的基础，并能提供最优的效率和安全性，所以经常应用在安全多方计算和其它高级密码协议中。

3. 与其它领域的联系：自对偶码与群论、组合设计、甚至量子计算中的稳定子码都有着深刻的联系。

四、结束语

本文系统阐述了线性秘密分享方案（LSSS）的形式化定义、基于线性码的理论框架，以及自对偶码所蕴含的完美对称性与重要价值。这不仅为密码方案的设计提供了坚实的数学基础，也为其在安全多方计算等前沿密码协议中的高效实现开辟了道路。这一理论体系充分体现了代数方法在构建安全高效的可计算秘密共享机制中的核心作用，也为后续研究更复杂的访问结构以及跨领域的应用衔接提供了清晰的理论视角。

参考文献

[1]Gharahi M ,Khazaei S .Optimal linear secret sharing schemes for graph access structures on six participants[J].Theoretical Computer Science,2019,7711-8.DOI:10.1016/j.tcs.2018.11.007.

[2]Jafari A ,Khazaei S .On Abelian Secret Sharing: duality and separation.[J].IACR Cryptology ePrint Archive,2019,2019575.

[3]Gharahi M ,Dehkordi H M .The complexity of the graph access structures on six participants[J].Designs, Codes and Cryptography,2013,67(2):169-173.DOI:10.1007/s10623-011-9592-z.

[4]Kaboli R , Khazaei S , Parviz M .On Ideal and Weakly-Ideal Access Structures[J].IACR Cryptol. ePrint Arch. 2020, 2020:483.DOI:10.3934/AMC.2021017.

[5]M á t é G ,P é ter L .On the information ratio of graphs without high-degree neighbors[J].Discrete Applied Mathematics,2021,30455-62.DOI:10.1016/J.DAM.2021.07.011.

[6]Jackson W A , Martin K M .Geometric secret sharing schemes and their duals[J].Designs Codes & Cryptography, 1994, 4(1):83-95.DOI:10.1007/BF01388562.

[7]Padr ó C ,V á zquez L ,Yang A .Finding lower bounds on the complexity of secret sharing schemes by linear programming[J].Discrete Applied Mathematics,2013,161(7-8):1072-1084.DOI:10.1016/j.dam.2012.10.020.

[8]Padr ó C .Lecture Notes in Secret Sharing.[J].IACR Cryptology ePrint Archive,2012,2012674.

[9]Farras O ,Kaced T ,Martin S , et al.Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing[J].IEEE Transactions on Information Theory,2020,PP(99):1-1.DOI:10.1109/tit.2020.3005706.

[10]Gharahi M ,Khazaei S .Reduced access structures with four minimal qualified subsets on six participants.[J].Advances in Mathematics of Communications,2018,12(1):199-214.DOI:10.3934/AMC.2018014.

[11]Csirmaz L .Secret sharing and duality.[J].IACR Cryptology ePrint Archive,2019,20191197.

[12]Jafari A , Khazaei S .Partial Secret Sharing Schemes[J].IEEE Transactions on Information Theory, 2023, 69(8):5364-5385.DOI:10.1109/TIT.2023.3265093.

[13]Mart í -Farr é J ,Padr ó C .On Secret Sharing Schemes, Matroids and Polymatroids.[J].IACR Cryptology ePrint Archive,2006,200677.

[14]Xing C , Yuan C .Evolving Secret Sharing Schemes Based on Polynomial Evaluations and Algebraic Geometry Codes.[J].IEEE Transactions on Information Theory, PP[2025-12-10].DOI:10.1109/TIT.2024.3379278.

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

