**Advances in Applied Mathematics** 应用数学进展, 2024, 13(12), 5147-5152
Published Online December 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.1312497

Hans汉斯

# 基于LCD码的可验证多秘密共享方案

**张玲玲[1]，胡慧丹[1]，林昌露[1,2*]**

[1]福建师范大学数学与统计学院，福建 福州
[2]分析数学及应用教育部重点实验室，福建 福州

收稿日期：2024年11月12日；录用日期：2024年12月5日；发布日期：2024年12月13日

## 摘 要

**为了解决基于线性码的秘密共享在区块链数据隐私保护中容易受到Tompa-Woll攻击以及子秘密只能单次使用的问题，本文提出了一种基于LCD码的可验证多秘密共享方案。该方案旨在应对不诚实用户通过提供错误子秘密而导致诚实用户无法获取秘密的情况。考虑到秘密重构函数的线性特性和其易受Tompa-Woll攻击的特点，本文采用双变量单向函数进行验证，从而有效抵御不诚实用户的恶意行为，并实现子秘密的多次使用。与其他方案的比较结果表明，该方案在性能上优于现有解决方案。**

## 关键词

**多秘密共享方案，多使用，LCD码，可验证，Tompa-Woll攻击**

# Verifiable Multi-Secret Sharing Scheme Based on LCD Code

**Lingling Zhang[1], Huidan Hu[1], Changlu Lin[1,2*]**

[1]School of Mathematics and Statistics, Fujian Normal University, Fuzhou Fujian
[2]Key Laboratory of Analytical Mathematics and Applications, Ministry of Education, Fuzhou Fujian

Received: Nov. 12th, 2024; accepted: Dec. 5th, 2024; published: Dec. 13th, 2024

## Abstract

**To address the vulnerability of linear code-based secret sharing in blockchain data privacy protection-specifically its susceptibility to Tompa-Woll attacks and the single-use limitation of sub-secrets-this paper proposes a verifiable multi-secret sharing scheme based on LCD codes. The scheme targets the issue where dishonest users can cheat by submitting incorrect sub-secrets, preventing honest users from successfully reconstructing the secret. Given the linear nature of the secret**

*通讯作者。

文章引用: 张玲玲, 胡慧丹, 林昌露. 基于LCD码的可验证多秘密共享方案[J]. 应用数学进展, 2024, 13(12): 5147-5152.
DOI: 10.12677/aam.2024.1312497

**creconstruction function and its vulnerability to Tompa-Woll attacks, this paper utilizes a two-variable one-way function for verification, effectively countering malicious behavior from dishonest users. Additionally, the use of the two-variable one-way function enables the reuse of sub-secrets. Comparative results show that this scheme outperforms existing solutions in terms of performance.**

## Keywords

**Multi-Secret Sharing, Mulit-Use, LCD Code, Verifiable, Tompa-Woll Attacks**



## 1. 引言

秘密共享作为保护重要信息的工具，有广泛应用如：门限数字签名、安全多方计算、密钥协商和安全组播等。秘密共享最早由 Shamir [1]和 Blakley [2]在 1979 年分别基于拉格朗日插值多项式和超平面的点构造提出，基本思想为：将要共享的秘密通过分发算法将子秘密或份额分发给一组用户，当一定数量的诚实用户提交子秘密通过重构算法恢复秘密。所有能够恢复秘密的用户的集合称为访问结构。Asmuth 等[3]基于中国剩余定理提出了门限秘密共享方案，该方案重构复杂度优于 Shamir 方案；Chien 等[4]基于线性分组码、双变量单向函数提出多秘密共享方案，实现用户子秘密可多次使用；信息率也是秘密共享的一个重要概念，实质上是秘密的大小与用户子秘密大小的比例。当秘密的大小与用户子秘密大小相等时，称此方案是理想的。基于线性码的秘密共享方案其重构函数是线性易受 Tompa-Woll 攻击[5]。

本文基于 LCD 码和双变量单向函数，提出了一个可验证多秘密共享方案。本方案实现用户的子秘密可多次使用，减少计算与通信成本。

**本文主要贡献如下所示：**

1) 通过利用双变量单向函数，该方案具备了可验证性，使得用户能够有效识别接收到的子秘密的真实性，从而有效抵抗 Tompa-Woll 攻击。

2) 通过与现有的方案对比显示，该方案是理想的，能够同时具备可验证性、子秘密多次使用的功能。

**本文相关工作：**1981 年 McEliece 等[6]发现秘密共享方案与 Reed-Solomon 码的关系。1993 年 Massey [7]基于线性码提出了完备的秘密共享方案并说明其访问结构的特征，访问结构与其对偶码的极小码字一一对应。2013 年宋云等[8]基于极小线性码提出秘密共享方案；同年 Tentu 等[9]利用 MDS 码和单向函数提出了合取分成访问结构的秘密共享方案，其方案是理想的、计算上完备的。2020 年 Alahmadi 等[10]利用 LCD 码的性质，即 LCD 码与其对偶码的交为零向量，提出了多秘密共享方案。Ghosh 等[11]基于 Alahmadi 的方案进行改进，其共享的秘密与 LCD 码的码长相等。2024 年伍高飞和张玉清[12]给出两类最优五元循环码，并基于五元循环码提出秘密共享方案。抵抗 Tompa-Woll 攻击有两种主要方法：第一类是在线性码的秘密共享方案的基础上添加可验证的功能；第二类是将线性码通过映射变成非线性码，基于非线性码提出秘密共享方案。2010 年郭玉娟等[13]利用极小线性码链、离散对数和大素数分解提出动态可验证秘密共享方案，其计算开销大。2019 年李富林等[14]利用 Hamming 码和双变量单向函数提出了可验证多秘密共享方案，实现用户子秘密可重复使用。2020 年 Agrawal 等[15]基于非线性码提出秘密共享方案，并给出基于非线性 Nordstrom-Robinson 码的秘密共享访问结构。2022 年 Agrawal 等[16]利用 Gray 映射将 $Z_4$ 环上的线性码映射成 $F_2$ 上的非线性码，使用非线性码构造秘密共享方案。同年，Hossain 等[17]

利用循环码和双变量单向函数给出可验证多秘密共享方案。

**本文结构：**第 1 节介绍预备知识，第 2 节给出可验证多秘密共享方案的具体构造，第 3 节对提出的可验证多秘密共享方案进行安全分析，第 4 节是与相关工作进行对比分析，第 5 节对文章进行总结。

## 2. 预备知识

本节分别对秘密共享方案，LCD 码，双变量单向函数，Tompa-Woll 攻击进行简单的介绍。

### 2.1. 秘密共享方案

秘密共享方案由分发阶段和重构阶段构成。在分发阶段，诚实分发者 dealer 执行分发算法将秘密 $s$ 拆分成 $k$ 个子秘密 $s_1,s_2,\cdots,s_k$，并将子秘密 $s_i$ 共享给用户 $P_i\ (i=1,2,\cdots,n)$。在重构阶段，任意大于等于 $k$ 个用户可以用户重构秘密 $s$，任意小于 $k$ 个用户无法获得秘密的任何信息，其中任意大于等于 $k$ 个用户构成的集合称为授权集，任意小于 $k$ 个用户构成的集合称为非授权集。所有的授权集构成的集合称为访问结构 $\Gamma$，如下所示：

$$\Gamma=\left\{A\middle|A\subseteq P,|A|\geq k\right\}。$$

定义 **1** (完备的秘密共享方案[18])在 $n$ 个用户集合中，共享秘密 $s$，其访问结构为 $\Gamma$。满足以下两个条件的秘密共享方案称为完备的秘密共享方案：

1) 正确性：对于任意授权子集 $\gamma\in\Gamma$，$\gamma$ 中用户合作可以恢复秘密 $s$。

2) 安全性：对于任意非授权子集 $\eta\notin\Gamma$，$\eta$ 中用户合作得不到秘密 $s$ 的任何信息。

### 2.2. LCD 码

定义 **2** (线性码[19])设 $F_q^n$ 是有限域 $F_q$ 上 $n$ 维向量空间。$(n,k)$ 码 $C$ 是 $F_q$ 上大小为 $k$ 的子集。$(n,k)$ 码 $C$ 是线性码当且仅当码 $C$ 是 $F_q$ 上 $k$ 维线性子空间记作 $[n,k]$。将 $(c_n,c_1,\cdots,c_{n-1})\in F_q^n$ 称为码 $C$ 的码字。

线性码有两种表达方式 $C=\left\{\vec{v}G\,|\,\forall\vec{v}\in F_q^k\right\}=\left\{c\in F_q^n\,|\,Hc^{\perp}=0\right\}$，其中 $G$ 是线性码的生成矩阵，$H$ 是线性码的校验矩阵。

码 $C$ 的对偶码 $C^{\perp}$ 表示为 $C^{\perp}=\left\{\vec{x}\in F_q^n\,|\,\vec{x}c=0,\forall c\in C\right\}$。当 $C\subseteq C^{\perp}$ 成立时，称码 $C$ 自正交。当 $C=C^{\perp}$ 成立时，称码 $C$ 自对偶。当 $C\cap C^{\perp}=\{0\}$ 成立时，称码 $C$ 为线性互补对偶码即 LCD 码。

定义 **3** (LCD 码[20])令 $C$ 为 $[n,k]$ 线性码，$G$ 是其生成矩阵、$H$ 是其校验矩阵。码 $C$ 为 LCD 码当且仅当矩阵 $GG^{\perp}$ 非奇异，当且仅当矩阵 $\begin{pmatrix}G\\H\end{pmatrix}$ 非奇异。

### 2.3. 双变量单向函数

定义 **4** (双变量单向函数[18])。$f(x,y)$ 表示一个有两个变量的单向函数，能够将任意的 $x$ 和 $y$ 映射到固定的函数值。该函数有以下性质：

1) 已知 $x$ 和 $y$，$f(x,y)$ 易于计算。

2) 已知 $y$ 和 $f(x,y)$，求 $x$ 在计算上是不可行的。

3) 在 $y$ 未知的情况下，对于任意的 $x$，难以计算 $f(x,y)$。

4) 已知 $y$ 的情况下，找到不同的 $x_1$ 和 $x_2$ 满足 $f(x_1,y)=f(x_2,y)$ 是不可行的。

5) 已知 $x$ 和 $f(x,y)$，求 $y$ 在计算上是不可行的。

6) 已知任意多的 $(x_i,f(x_i,y))$ 对，求 $f(x',y)$ 是不可行的，其中 $x'\neq x_i$。

### 2.4. Tompa-Woll 攻击

以 Shamir 的门限秘密共享方案为例，假设分发者有多项式 $f(x)=13+10x+2x^2$，其中秘密为 $s=13$。假设有三个用户 $\{P_1,P_2,P_3\}$，用户 $P_1$ 得到的子秘密为 $f(x_1)=f(1)=25$，用户 $P_2$ 得到的子秘密为 $f(x_2)=f(2)=41$，用户 $P_3$ 得到的子秘密为 $f(x_3)=f(3)=61$。则秘密 $s$ 恢复如下：

$$s=3f(x_1)-3f(x_2)+f(x_3)。$$

秘密 $s$ 恢复函数是用户 $P_1,P_2,P_3$ 子秘密的线性组合。若用户 $P_1$ 发起 Tompa-Woll 攻击，即用户 $P_1$ 提交的子秘密为 $f(x_1)+\varepsilon$，其中 $\varepsilon$ 是只有用户 $P_1$ 已知。则恢复的秘密 $s$ 如下

$$s'=3\left(f(x_1)+\varepsilon\right)-3f(x_2)+f(x_3)=s+3\varepsilon。$$

用户 $P_1,P_2,P_3$ 分别拿到秘密 $s'$ 由于用户 $P_1$ 已知 $\varepsilon$，于是用户 $P_1$ 可以恢复的真正秘密 $s$。

## 3. 方案构造

本文利用 LCD 码其性质和双变量单向函数给出一个可验证门限多秘密共享方案，其中本方案实现用户的子秘密可多次使用。本方案主要由初始化、子秘密生成、重构、验证、子秘密多次使用算法构成，具体实现过程如下所示：

算法 **1** **初始化算法**

1) 诚实分发者 dealer，随机选取 $F_q$ 上长为 $n$ 的 LCD 码，其生成矩阵为 $G$。随机选取 $r$ 和双变量单向函数 $f(x,y)$，公开 $f(r,y)$。$n$ 个用户集为 $\{P_1,P_2,\cdots,P_n\}$。

2) 诚实分发者 dealer 设置 $k$ 个秘密分别为 $S=(s_1,s_2,\cdots,s_k)$。

算法 **2** **子秘密生成算法**

1) 用户 $P_i$ 选择一个 $1\times k$ 的向量 $\vec{l}_i=(c_{i1},c_{i2},\cdots,c_{ik})$，利用公开的双变量单向函数计算 $\left(f(r,c_{i1}),f(r,c_{i2}),\cdots,f(r,c_{ik})\right)$，将 $\left(f(r,c_{i1}),f(r,c_{i2}),\cdots,f(r,c_{ik})\right)$ 记为 $f\left(r,\vec{l}_i\right)$。

2) 用户 $P_i$ 将 $f\left(r,\vec{l}_i\right)$ 发给诚实分发者 dealer。记 $GG^{\mathrm{T}}S^{\mathrm{T}}=\vec{y}$，诚实分发者将 $\vec{y}$ 公开。

算法 **3** **秘密重构与验证算法**

1) 假设任意 $k$ 个用户集为 $\left\{P_{v_1},P_{v_2},\cdots,P_{v_k}\right\}$ 合作恢复秘密，诚实分发者公开

$$\vec{X}=f\left(r,\vec{l}_{v_1}\right)+f\left(r,\vec{l}_{v_2}\right)+\cdots+f\left(r,\vec{l}_{v_k}\right)。$$

2) 用户 $P_{v_i}$ 给用户 $P_{v_j}$ 自己的伪子秘密 $f\left(r,\vec{l}_{v_i}\right)$，合作恢复秘密的用户将伪子秘密相加 $\vec{X}'=\sum_{i=1}^{k}f\left(r,\vec{l}_{v_i}\right)$，验证 $\vec{X}=\vec{X}'$ 等式是否成立。若等式不成立停止协议。若等式成立继续执行协议。

3) 用户 $P_{v_i}$ 利用公开的 $\vec{y}$ 与收集到的伪子秘密 $f\left(r,\vec{l}_{v_i}\right)$，计算 $f\left(r,\vec{l}_{v_i}\right)\vec{y}=x_{v_i}$，$(1\le i\le k)$。

4) 考虑线性方程组 $f\left(r,\vec{l}_{v_i}\right)GG^{\mathrm{T}}S^{\mathrm{T}}=x_{v_i}$，由于 $GG^{\mathrm{T}}$ 是非奇异且秩为 $k$。线性方程组有唯一解，因此秘密 $S=(s_1,s_2,\cdots,s_k)$ 被恢复。

算法 **4** **子秘密多使用性算法**

当秘密 $S=(s_1,s_2,\cdots,s_k)$ 从更新为 $S'=(s_1',s_2',\cdots,s_k')$，分发者重新公开 $GG^{\mathrm{T}}S'^{\mathrm{T}}=\vec{y}'$ 用户 $P_{v_i}$ 利用公开的 $\vec{y}'$ 与收集到的伪子秘密 $f\left(r,\vec{l}_{v_i}\right)$ $(1\le i\le k)$，计算 $f\left(r,\vec{l}_{v_i}\right)\vec{y}'=x'_{v_i}$。考虑新的线性方程组 $f\left(r,\vec{l}_{v_i}\right)GG^{\mathrm{T}}S'^{\mathrm{T}}=x'_{v_i}$，由于 $GG^{\mathrm{T}}$ 是非奇异且秩为 $k$。线性方程组有唯一解，因此秘密 $S'=(s_1',s_2',\cdots,s_k')$ 被恢复。实现用户的子秘密可多次使用。

## 4. 安全分析

本节通过定理 1 与定理 2 证明所提出的动态可验证多秘密关系方案，满足正确性与安全性。

定理 **1** (正确性分析) 设$\{P_1,P_2,\cdots,P_n\}$是用户集合，任意 $k$ 个用户可以恢复秘密。

证明：任意 $k$ 个诚实用户利用公开的 $\vec{y}$ 与收集到的伪子秘密 $f\left(r,\vec{l}_{v_i}\right)$ $(1\le i\le k)$，计算 $f\left(r,\vec{l}_{v_i}\right)\vec{y}=x_{v_i}$。由于矩阵 $G$ 是 LCD 码的生成矩阵，于是 $GG^{\mathrm{T}}$ 是非奇异且秩为 $k$。线性方程组 $f\left(r,\vec{l}_{v_i}\right)GG^{\mathrm{T}}S^{\mathrm{T}}=x_{v_i}$ 有唯一解，因此秘密 $S=\left(s_1,s_2,\cdots,s_k\right)$ 被恢复。于是任意 $k$ 个用户合作可以恢复秘密。

定理 **2** (安全性分析) 设$\{P_1,P_2,\cdots,P_n\}$是用户集合，任意 $k-1$ 个用户得不到秘密的任何信息。

证明：任意 $k-1$ 个用户利用公开的 $\vec{y}$ 与收集到的伪子秘密 $f\left(r,\vec{l}_{v_i}\right)$ $(1\le i\le k-1)$，计算 $f\left(r,\vec{l}_{v_i}\right)\vec{y}=x_{v_i}$。由于矩阵 $G$ 是 LCD 码的生成矩阵，于是 $GG^{\mathrm{T}}$ 是非奇异且秩为 $k$。线性方程组 $f\left(r,\vec{l}_{v_i}\right)GG^{\mathrm{T}}S^{\mathrm{T}}=x_{v_i}$ 有无穷多解。于是任意 $k-1$ 个用户合作得不到秘密的任何信息。

**抵抗 Tompa-Woll 攻击：**

若用户 $P_{v_i}$ 发起 Tompa-Woll 攻击，提交伪子秘密为 $f\left(r,\vec{l}_{v_i}\right)+\varepsilon$，其中 $\varepsilon$ 是用户 $P_{v_i}$ 已知。在重构阶段参与重构的用户将伪子秘密相加得 $\vec{X}'=\vec{X}+\varepsilon$ 与分发者公开的 $\vec{X}$ 不相等，则用户集$\left\{P_{v_1},P_{v_2},\cdots,P_{v_k}\right\}$有人提交假的子秘密，停止协议。可以抵抗用户 $P_{v_i}$ 发起的 Tompa-Woll 攻击。

## 5. 方案对比

本文利用 LCD 码和双变量单向函数提出一个可验证多秘密共享方案。该方案是理想的且能有效抵抗 Tompa-Woll 攻击，实现用户子秘密的多次使用。当秘密向量更新时，分发者只需要重新公开新的 $\vec{y}$ 即可。表 1 给出了基于 LCD 码多秘密共享方案的功能性比较。

表 1 给出 Alahmadi 和 Ghosh 方案与本文方案功能性比较。文献[10]将码字作为要共享的秘密，利用 LCD 码生成矩阵的性质解线性方程组。此方案不能实现用户子秘密多使用性，且不能验证用户是否诚实提交子秘密。文献[11]基于 LCD 码构造的方案适用于有限域 $F_q$ 与局部环 $R$ 上，共享的秘密与码字等长。此方案是完备的，但不能实现用户子秘密多使用性，且不能验证用户是否诚实提交子秘密。

表 1 分别通过与 Alahmadi 和 Ghosh 方案的比较，说明了本方案在，用户子秘密多使用性，验证性等方面性能优势。

**Table 1.** Functional comparison of multi secret sharing schemes based on LCD codes
**表 1.** 基于 LCD 码多秘密共享方案功能性比较

| 方案 | 子秘密多使用 | 可验证 |
|---|---|---|
| Alahmadi [10] | × | × |
| Ghosh [11] | × | × |
| 本文方案 | √ | √ |

符号说明：√表示具备性质；×表示不具备性质。

## 6. 总结

本文利用 LCD 码和双变量单向函数提出一个可验证多秘密的秘密共享方案，该方案是理想的且能有效抵抗 Tompa-Woll 攻击，实现用户子秘密的多次使用。与其他方案相比，该方案加强功能以及降低计算开销。

## 基金项目

福建省高校产学合作科技计划项目(2023H6012)。

## 参考文献

[1] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. https://doi.org/10.1145/359168.359176

[2] Blakley, G.R. (1979) Safeguarding Cryptographic Keys. 1979 *International Workshop on Managing Requirements Knowledge* (*MARK*), New York, 4-7 June 1979, 313-318. https://doi.org/10.1109/mark.1979.8817296

[3] Asmuth, C. and Bloom, J. (1983) A Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, **29**, 208-210. https://doi.org/10.1109/tit.1983.1056651

[4] Chien, H.Y., Jan, J.K. and Tseng, Y.M. (2000) A Practical (t,n) Multi-Secret Sharing Scheme. *IEICE Transactions on Fundamentals*, **83**, 2762-2765.

[5] Tompa, M. and Woll, H. (n.d.) How to Share a Secret with Cheaters. In: Odlyzko, A.M., Eds., *Advances in Cryptology—CRYPTO'*86, Springer, 261-265. https://doi.org/10.1007/3-540-47721-7_20

[6] McEliece, R.J. and Sarwate, D.V. (1981) On Sharing Secrets and Reed-Solomon Codes. *Communications of the ACM*, **24**, 583-584. https://doi.org/10.1145/358746.358762

[7] Massey, J.L. (1993) Minimal Codewords and Secret Sharing. *Proceedings of the* 6*th Joint Swedish-Russian International Workshop on Information Theory*, 1993, 276-279.

[8] 宋云, 李志慧, 李永明. 基于极小线性码上的秘密共享方案[J]. 电子学报, 2013, 41(2): 220-226.

[9] Tentu, A.N., Paul, P. and Venkaiah, V.C. (2013) Ideal and Perfect Hierarchical Secret Sharing Schemes Based on MDS Codes. IACR Cryptology ePrint Archive, Paper 2013/189. http://eprint.iacr.org/2013/189

[10] Alahmadi, A., Altassan, A., AlKenani, A., Çalkavur, S., Shoaib, H. and Solé, P. (2020) A Multisecret-Sharing Scheme Based on LCD Codes. *Mathematics*, **8**, Article 272. https://doi.org/10.3390/math8020272

[11] Ghosh, H., Bhowmick, S., Maurya, P.K. and Bagchi, S. (2021) Linear Complementary Dual Code-Based Multi-Secret Sharing Scheme. arXiv:2112.05469. https://doi.org/10.48550/arXiv.2112.05469

[12] 伍高飞, 张玉清. 基于循环码的秘密共享方案[J]. 密码学报, 2024, 11(4): 895-910.

[13] 郭玉娟, 李志慧, 赖红. 基于线性码上的动态可验证的秘密共享方案[J]. 陕西师范大学学报, 2010, 38(4): 7-12.

[14] 李富林, 刘杨, 王娅如. 一种基于 Hamming 码的门限多秘密共享方案[J]. 合肥工业大学学报(自然科学版), 2021, 44(5): 711-714, 720.

[15] Agrawal, D., Das, S. and Krishanaswamy, S. (2020) Secret Sharing Schemes Based on Nonlinear Codes. 2020 *IEEE International Symposium on Information Theory* (*ISIT*), Los Angeles, 21-26 June 2020, 864-867. https://doi.org/10.1109/isit44484.2020.9174044

[16] Agrawal, D. (2022) Nonlinear Secret Sharing Schemes Based on $Z_4$ Linear Codes. 2022 *IEEE Globecom Workshops* (*GC Wkshps*), Rio de Janeiro, 4-8 December 2022, 608-611. https://doi.org/10.1109/gcwkshps56602.2022.10008706

[17] Hossain, M.A. and Bandi, R. (2023) A Verifiable Multi-Secret Sharing Scheme Based on $\ell$-Intersection Pair of Cyclic Codes. *International Journal of Foundations of Computer Science*, 1-21. https://doi.org/10.1142/s0129054123500284

[18] 庞辽军, 裴庆祺, 李慧贤, 等. 秘密共享技术及其应用[J]. 通信学报, 2017, 38(3): 204.

[19] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting C-Odes. Elsevier.

[20] Çalkavur, S., Bonnecaze, A., Cruz, R.D. and Solé, P. (2021) Code Based Secret Sharing Schemes: Applied Combinatorial Coding Theory. World Scientific. https://doi.org/10.1142/12585