

DOI:10.3969/j.issn.1671-0673. 2026. 01. 014

融合对称矩阵的双重可验证高维秘密共享方案设计

王北平, 潘思明, 唐婷婷

(武警警官学院, 四川 成都 610000)

摘要:为解决传统秘密共享方案中权限划分不清、安全性与可验证性不足的问题,设计了一种融合对称矩阵的双重可验证高维秘密共享方案。该方案按职位等级划分参与者,基于有限域构建多项式编码主密钥,通过对称矩阵特征值与特征向量生成子密钥,结合正交矩阵实现安全分发;引入双重验证机制确保子密钥真实与参与者诚实;恢复阶段利用满足门限的子密钥特征值,通过多项式插值与范德蒙行列式特性求解主密钥。理论推导证明了方案正确性,对称矩阵特性与双重验证可抵御篡改、窃听等攻击,满足信息论安全要求。以部队军械库管理为例,验证其可实现“1名干部+2名军械员”的分级授权并成功恢复密钥。该方案实现分级权限管控,兼具高安全性、可验证性与实用性,适用于需分级授权的秘密管理场景。

关键词: 门限秘密共享方案; 对称矩阵; 秘密分割; 秘密恢复

中图分类号: TP309.7

文献标识码: A

文章编号: 1671-0673(2026)01-0105-07

Design of Dual-Verifiable High-Dimensional Secret Sharing Scheme Integrating Symmetric Matrices

WANG Beiping, PAN Siming, TANG Tingting

(Officers College of PAP, Chengdu 610000, China)

Abstract: To address unclear permissions, weak security and poor verifiability in traditional secret sharing, a dual-verifiable high-dimensional secret sharing scheme integrating symmetric matrices is designed. Participants are grouped by job levels. The polynomial master key is encoded based on finite-field polynomials. Sub-keys, generated from symmetric matrix eigenvalues and eigenvectors, are securely distributed using orthogonal matrices. A dual verification mechanism is used to ensure sub-key authenticity and participant's honesty. The master key is derived from polynomial interpolation and Vandermonde determinant properties using threshold sub-key eigenvalue in the recovery stage. Theoretically proven correct, tampering and eavesdropping are resisted through symmetric matrix properties and dual verification, meeting the requirements of information-theoretic security. Validated in military ordnance management, it enables “1 cadre + 2 ordnance man” hierarchical authorization and key recovery. This scheme achieves hierarchical permission control with high security, verifiability and practicality, suitable for graded authorization scenarios.

Key words: threshold secret sharing scheme; symmetric matrix; secret splitting; secret recovery

随着数字化进程飞速推进,信息安全已成为所有行业不可忽视的核心焦点。作为守护信息安全的关键技术,秘密共享方案在过去几十年里,不

仅得到学术界的深度探索与广泛研究,更成功渗透到多个领域,实现了从理论到实际应用的落地。其中,1979年Shamir^[1]提出的经典方案颇具里程碑

收稿日期: 2025-09-25; 修回日期: 2025-11-20

作者简介: 王北平(1988—),女,讲师,硕士,主要研究方向为随机分析、大学数学教学。E-mail: 575139341@qq.com

意义,该方案以拉格朗日插值公式为理论基础,开启了秘密共享技术发展的重要篇章。Blakley^[2]基于射影几何的方案问世以来,该领域不断发展,众多学者投入研究。1999年, Hillery等^[3]创新性地将量子力学原理融入秘密共享领域,成功构建出首个量子秘密共享(Quantum Secret Sharing, QSS)协议,在该领域具有划时代的意义。文献[4-6]均在推动量子秘密共享方案计算速度优化进程中,发挥了重要的作用。2005年, Yan等^[7]凭借独到的设计理念,成功搭建起多方之间秘密共享的桥梁。2011年, Wang等^[8]引入了量子秘密共享模型,针对各类潜在攻击在该模型框架内构建坚固的安全方案。2013年, Hsu等^[9]基于EPR对(Einstein Podolsky Rosen pairs)提出了纠缠变换这一概念。2017年, Qin等^[10]运用高维GHZ(Greenberger-Horne-Zeilinger)态构建出一款灵活度更高的DQSS(Dynamic Quantum Secret Sharing)协议,此协议允许在同一更新周期内对多个参与者进行动态的增加或删除操作,极大地拓展了协议的应用弹性。然而,2020年, Yang等^[11]指出,文献[10]的协议在复杂多变的实际应用场景中依旧未能找到彻底杜绝参与者不诚实行为的有效办法。为此, Qin等^[12]依托高维纠缠态构建起HQSS(Hierarchical Quantum Secret Sharing)协议,该协议在参与者管理上采用层级化设计。然而,不足的是,该协议无法实现参与者数量的动态增减。2024年,陈克勤等^[13]提出了一项基于高维GHZ态的创新方案——动态分层量子秘密共享协议,该协议将每个参与者合理分配至相应层级,可以实现多个参与者的动态增加或删除。与此同时, Ma等^[14]提出了首个保护秘密重构过程的量子秘密重构协议,该协议不仅实现了所有份额的信息理论安全,而且由于减少了分配和计算成本,效率也更高。

另一方面,张艳硕等^[15]在2018年的研究中,率先探索了对称矩阵特征值与门限秘密共享方案的结合,但并没有充分利用实对称矩阵的特殊性质。之后该团队^[16-17]利用矩阵特征值的特性提出了无可信中心的秘密共享方案,但缺少验证环节,容易发生参与者欺诈行为。2020年,方案得到进一步优化,提出了基于特征值的可验证无可信中心的门限方案^[18],其中虽然对参与者划分了集合,但各集合所持子密钥的份额固定为2份,很难满足参与者具有权限等级的情况,而且同一个集合中的所有参与者的子密钥对应同一个特征值,在验证过

程中只是验证参与者的子密钥线性无关,安全性相对薄弱。同时,这3篇文献^[16-18]秘密恢复阶段每个集合的参与者至少1人,但现实场景中存在某个集合需要多名参与者才能恢复秘密的情况,比如,某次军事行动的指挥控制涉及高度机密和重大责任,不同级别军官负责不同层面指挥任务。若将军官按职位等级分为基层指挥官、中层指挥官和高层指挥官。对于重要军事行动的指挥密钥,可能要求至少2名高层指挥官和3名中层指挥官共同参与,才能恢复密钥下达指令,确保军事行动的严肃性和安全性,防止误操作或恶意指令。

文献[16-18]方案设计中只对参与者的身份进行了单一的验证,没有对系统的安全性进行验证,而且没有体现出现实中的高维需求以及参与者身份会发生变化的灵活性需求。受到以上文献的启发,考虑到对称矩阵的特殊性质(特征值都是实数,且不同特征值对应的特征向量一定正交,避免复数运算带来的密钥不一致问题,提出一种融合对称矩阵的双重可验证高级秘密共享方案)。首先,通过职位等级划分参与者集合,实现“高权限者多拿子密钥、低权限者少拿子密钥”的差异化分配,且在秘密恢复阶段,每个集合参与恢复秘密的人数不都是至少1个人,不同集合参与秘密恢复的人数按照职位等级是有差别的;其次引入“不同参与者间子密钥正交性验证”与“同一参与者线性无关性验证”的双重机制,既能确保子密钥传输的完整性,又能识别欺诈参与者,形成全流程安全防护;最后利用多项式插值与范德蒙行列式的唯一性,保障秘密恢复的准确性。

为验证方案的实用性,以部队军械库安全管理为例,设定“1名军械干部+2名军械员”的门限恢复规则,通过参数选取、秘密分割、子密钥分发与秘密恢复的全流程模拟,证明方案在满足权限分级需求的同时,具备高安全性与高可靠性。该方案不仅为军事、政务等对权限管控要求严格的领域提供了新的技术路径,也为秘密共享技术的维度拓展与安全升级提供了理论参考。

1 基础知识

1.1 线性代数相关知识

定义1^[19] 设 A 是 n 阶矩阵,如果数 λ 和 n 维非零列向量 p 使关系式成立:

$$Ap = \lambda p \quad (1)$$

那么这样的数 λ 称为矩阵 A 的特征值,非零向量 p

称为 A 的对应于特征值 λ 的特征向量。

定义2^[19] 设 A 、 B 为 n 阶矩阵,若存在可逆矩阵 P 使 $P^{-1}AP = B$,则 A 与 B 相似。 $P^{-1}AP$ 称为对 A 进行相似变换,可逆矩阵 P 称为把 A 变成 B 的相似变换矩阵。

定义3^[19] 设 $x = (x_1, x_2, \dots, x_n)^T$, $y = (y_1, y_2, \dots, y_n)^T$, 若向量 x 与 y 的内积 $[x, y] = 0$,则称向量 x 与向量 y 正交。

定义4^[19] 给定向量组 $A: (a_1, a_2, \dots, a_m)$, 当且仅当实数 $(k_1, k_2, \dots, k_m)$ 全为零时,有:

$$k_1 a_1 + k_2 a_2 + \dots + k_m a_m = 0 \quad (2)$$

则称向量组 $A: (a_1, a_2, \dots, a_m)$ 是线性无关。

定理1^[19] 若 n 阶矩阵 A 与 B 相似,则 A 与 B 的特征多项式相同,从而 A 与 B 的特征值相同。

推论1^[19] 若 n 阶矩阵 A 与对角阵 $\Lambda = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ 相似,则 $(\lambda_1, \lambda_2, \dots, \lambda_n)$ 就是 A 的 n 个特征值。

特别的,如果 n 阶矩阵 A 与对角阵 $\Lambda = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ 相似,有:

$$A = P^{-1} \Lambda P \quad (3)$$

式中: A 是的特征值; P 是由特征值对应的特征向量 $p_1, p_2, \dots, p_n$ 构成的矩阵。

性质1^[19] 设 λ_1, λ_2 是实对称阵 A 的两个特征值, p_1, p_2 是对应的特征向量,若 $\lambda_1 \neq \lambda_2$,则 p_1 与 p_2 正交。

性质2^[19] A 为 n 阶对称阵, λ 是 A 的特征方程的 k 重根,则 $R(A - \lambda E) = n - k$,从而对应于 λ 的线性无关的特征向量有 k 个。

定理2^[19] 设 A 为 n 阶对称阵,则必有正交阵 P ,使得:

$$P^{-1}AP = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix} \quad (4)$$

式中, $(\lambda_1, \lambda_2, \dots, \lambda_n)$ 为 A 的特征值。

1.2 (k, n) 门限秘密共享方案的基本概念

在密码学技术谱系中, (k, n) 门限秘密共享方案占据关键地位,其核心思想是将一个秘密值 S 分割成 n 个份额(Share),并分发给 n 个参与者。该方案满足以下两点特性。

1) 重构条件:任意至少 k 个参与者的份额组合,可通过特定算法准确恢复出原始秘密 S 。

2) 安全性:任意少于 k 个参与者的份额组合,无法获取关于秘密 S 的任何有效信息(信息论安全

或计算安全)。

1.3 基于多项式插值的 (t, n) 门限秘密共享方案

基于多项式的拉格朗日插值公式,Shamir^[11]构建了一种门限方案。由于其独特的设计思路与广泛应用,该方案被命名为Shamir门限方案,同时因核心技术依赖拉格朗日插值,也常被称作拉格朗日插值法门限方案。方案详细说明如下。

1) 参数选取。设共享秘密 K ,选择一个素数 $p \in Z_p(p)$,该方案包含 n 名参与者,要实现共享秘密的重构,核心条件是参与操作的人数需达到 t 人及以上。

2) 秘密分割。第1步:随机地选定 $(t-1)$ 个互不相同的数,记为 $(a_1, a_2, \dots, a_{t-1}) \in Z_p$,得到多项式

$$s(x) = K + a_1 x + \dots + a_{t-1} x^{t-1} \pmod{p} \quad (5)$$

该多项式满足 $s(0) = K \pmod{p}$ 。

第2步:选定 n 个不同的整数 $(x_1, x_2, \dots, x_n) \in Z_p$,对于每个整数分别计算数对 (x_i, y_i) ,其中 $i = 1, 2, \dots, n; y_i \equiv s(x_i) \pmod{p}$ 。

第3步:将 n 个数对 (x_i, y_i) 分别秘密传送给 n 个成员,多项式 $s(x)$ 则是保密的,可以销毁。

3) 秘密恢复。假设 t 个人一起准备恢复秘密 K ,不妨设他们的数对为 $(x_1, y_1), (x_2, y_2), \dots, (x_t, y_t)$ 。

首先, t 个人计算多项式 $s(x)$ 为

$$s(x) = \sum_{k=1}^t y_k \prod_{\substack{j=1, \\ j \neq k}}^t \frac{x - x_j}{x_k - x_j} \pmod{p} \quad (6)$$

其次,取多项式 $s(x)$ 的常数项 $s(0)$,即为所求的秘密 K 。

2 (m, n) 门限秘密共享方案

2.1 (m, n) 门限秘密共享方案的定义

在文献[15-18]提出方案的基础上,本文提出一种多维秘密共享方案。以某部队的军械库安全管理为例,设定一个中队配有2名军械干部和3名军械员共同掌管军械库密钥系统,按照职位等级的不同将这些人员分为两个集合,其中:2名军械干部归为一个集合,因其职位等级较高,在保险库开启权限方面也更高,他们所持有子密钥的份额相对较多;另外3名军械员归为另一个集合,他们所持有子密钥的份额相对少。在秘密恢复阶段,考虑到职位等级与开启军械库所需人数的关系,通常职位等级高的所需人数较少。为有效避免诸如职员监守自盗、遗忘密钥,或者因职员缺席而导致

军械库无法开启等一系列问题,制定了严格的开启规则:开启军械库时,至少需要1名军械干部和2名军械员同时在场。根据组合原理进行计算,此时开启军械库的决定方式共有 $(2+1) \times (3+1) = 12$ 种决定方式。由此定义了一种 (m,n) 门限秘密共享方案。

定义5 设 $(B_1, B_2, \dots, B_t)$ 是 t 个参与者的集合,任意2个集合的交集是空集,即 $B_f \cap B_g = \Phi (1 \leq f \leq t, 1 \leq g \leq t, f \neq g)$; $|B_1| = n_1, |B_2| = n_2, \dots, |B_t| = n_t$, 且 $n_1 + n_2 + \dots + n_t = n$, 第 i 个集合每人分得 k_i 个子密钥。主密钥恢复阶段,每一等级参与者数都有严格的门限要求,最高等级集合最少只需 m_1 个人参与,下一等级集合最少需 m_2 个人参与,依次类推,第 t 个集合最少需要 m_t 人参与,其中 $m_i \geq 1$ 且 $m_1 + m_2 + \dots + m_t = m$, 唯有满足上述条件,秘密 K 才能被恢复,一旦这 m 个参与者中有任何一个缺失,都无恢复秘密 K ,这样的秘密共享方案即称为 (m,n) 门限秘密共享方案。

2.2 黑盒

2.2.1 黑盒的定义

以文献[20]中“黑盒”的定义为基础,说明该概念在本文方案中的具体界定与内涵。

定义6 黑盒的内部组成与结构,只有参与设计的人员能够掌握,除此之外的任何个体或群体,均无法了解其内部详情。另外,为了防止黑盒被恶意控制直接破坏方案安全性,嵌入异常行为追溯与熔断机制,会自动记录黑盒操作日志,包括子密钥输入、验证过程、特征值输出的时间戳和数据摘要,日志不可篡改且多节点备份,并设定异常阈值,若黑盒输出的特征值分布、验证通过率与历史数据偏差过大,自动触发熔断,暂停流程,需重新分发密钥并排查黑盒问题。在子密钥的生成阶段,密钥分发者的核心操作之一是向黑盒提供待分发的秘密 K 、参与者集合的个数 t 、各集合的人数 $n_i (1 \leq i \leq t)$ 以及各集合中参与者所持有子密钥份额数 k_i ,黑盒随即输出 $\sum_{i=1}^t n_i k_i$ 个子密钥 $p_{ij} (1 \leq i \leq t, 1 \leq j \leq n_i, 1 \leq h \leq k_i)$ 。参与者集合是按参与者的职位等级划分的,职位等级高的集合中参与者权限也高,所持有的子密钥的份额相对多,反之亦然。参与者拿到子密钥可以自行验证自己的子密钥是否满足线性无关且 $\lambda_{ij1} = \lambda_{ij2} = \dots = \lambda_{ijk_i} = \lambda_{ij}$,若不满足则有可能系统已被攻击。在秘密恢复时,参与恢复秘密的参与者持有的子密钥必须满

足:1)同一个参与者的子密钥 $p_{ij1}, p_{ij2}, \dots, p_{ijk_i}$ 线性无关且 $\lambda_{ij1} = \lambda_{ij2} = \dots = \lambda_{ijk_i} = \lambda_{ij}$;2)不同的参与者的子密钥正交。若满足以上两个条件,则输出与之对应的特征值 λ_{ij} ,进而实现秘密 K 的恢复;反之,若不满足条件,则无法恢复秘密 K 。

2.2.2 黑盒的原理

依据定理2完成子密钥生成阶段的设计。在该阶段内,密钥分发者根据参与者集合的个数 t 、各集合的人数 $n_i (1 \leq i \leq t)$ 、各集合中参与者所持有子密钥份额数 k_i ,计算矩阵阶数为 $\sum_{i=1}^t n_i k_i$,并以随机数为对角元素构建该阶对角矩阵 A 并将其输入黑盒,随后黑盒随机生成 $\sum_{i=1}^t n_i k_i$ 阶正交阵 Q ,根据式(1)可得到一个对称矩阵 A ,即 $A = QAQ^{-1}$ 。此时黑盒依次输出对称矩阵 A 的所有特征值对应的特征向量 p_{ij} ,密钥分发者将 p_{ij} 作为子密钥,按照份额分发给所有参与者。

依据性质1和性质2完成秘密恢复阶段。黑盒中存储着矩阵 A ,而该矩阵源自子密钥生成阶段。当参与者输入子密钥 p_{ij} ,若它能够同时满足两个条件,黑盒会输出该子密钥对应的特征值 λ_{ij} ;若子密钥无法满足这两项条件,则秘密恢复工作将无法成功进行。

3 方案设计

该方案共包含4个递进步骤,依次为系统描述、参数选取、秘密分割和秘密恢复。

1)系统描述。秘密共享系统的构成主体包括1名密钥分发者与 n 名参与秘密管理的参与者。 n 个秘密参与者构成集合 B ,集合 B 按照职位等级被划分为若干个不相交的集合 $B_1, B_2, \dots, B_t$,即 $B = \bigcup_{i=1}^t B_i$,其中 $|B_i| = n_i (i = 1, \dots, t; n_1 + \dots + n_t = n)$ 。

2)参数选取。选取系统参数的目的是为后续操作流程奠定基础。设有限域为 $GF(p)$ (p 为素数,且 $p > n$),密钥分发者从中独立随机地选 $(m-1)$ 个元素 $(a_1, a_2, \dots, a_{m-1}) \in GF(p)$,依次构建多项式 $f(x) = K + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} \pmod{p}$,其中 K 是共享秘密。

3)秘密分割。第1步:密钥分发者需挑选 n 个非零的、互不相同的整数 $(x_{11}, x_{12}, \dots, x_{1n_1}, x_{21}, x_{22}, \dots, x_{2n_2}, \dots, x_{t1}, x_{t2}, \dots, x_{tn_t}) \in Z_p$,分别计算 $\lambda_{ij} = f(x_{ij}) \pmod{p}$,

($1 \leq i \leq t, 1 \leq j \leq n_i$), 得到 $\sum_{i=1}^t n_i k_i$ 阶对角阵, 其对角阵元素为 $\lambda_{11}, \dots, \lambda_{11}, \dots, \lambda_{1n_1}, \dots, \lambda_{1n_1}, \dots, \lambda_{t1}, \dots, \lambda_{t1}, \dots, \lambda_{tn_t}, \dots, \lambda_{tn_t}$

其中: $(\lambda_{11}, \lambda_{12}, \dots, \lambda_{1n_1}, \lambda_{21}, \lambda_{22}, \dots, \lambda_{2n_2}, \dots, \lambda_{t1}, \lambda_{t2}, \dots, \lambda_{tn_t}) \in \text{GF}(p)$ 是特征方程 $|A - \lambda E| = 0$ 的特征根, 并且 $(\lambda_{11}, \lambda_{12}, \dots, \lambda_{1n_1})$ 都是 k_1 重根, $(\lambda_{21}, \lambda_{22}, \dots, \lambda_{2n_2})$ 都是 k_2 重根, $\dots, (\lambda_{t1}, \lambda_{t2}, \dots, \lambda_{tn_t})$ 都是 k_t 重根。

第2步: 密钥分发者以随机的方式, 生成一个 $\sum_{i=1}^t n_i k_i$ 阶的正交矩阵 Q , 进而得到矩阵 A 为

$$A = QAQ^{-1} \quad (7)$$

则矩阵 A 是对称矩阵且与 Λ 相似, 因此它们有相同的特征值 $\lambda_{11}, \lambda_{12}, \dots, \lambda_{1n_1}, \lambda_{21}, \lambda_{22}, \dots, \lambda_{2n_2}, \dots, \lambda_{t1}$ 。再由性质2可知, 特征值 $\lambda_{11}, \lambda_{12}, \dots, \lambda_{1n_1}$ 都有 k_1 个线性无关的特征向量; $\lambda_{21}, \lambda_{22}, \dots, \lambda_{2n_2}$ 都有 k_2 个线性无关的特征向量; 依次类推, $\lambda_{t1}, \lambda_{t2}, \dots, \lambda_{tn_t}$ 都有 k_t 个线性无关的特征向量。设 λ_{11} 对应的线性无关的特征向量为 $p_{111}, p_{112}, \dots, p_{11k_1}$; λ_{21} 对应的线性无关的特征向量 $p_{211}, p_{212}, \dots, p_{21k_2}$; λ_{t1} 对应的线性无关的特征向量 $p_{t11}, p_{t12}, \dots, p_{t1k_t}$ 。

随后, 密钥分发者会将子密钥 $(x_{ij}, p_{ijh}) (1 \leq i \leq t, 1 \leq j \leq n_i, 1 \leq h \leq k_i)$ 分发给第 t 个集合中的参与者, 每位参与者将获得 k_i 份, 其中 x_{ij} 是公开的。

第3步: 当秘密参与者拿到子密钥时, 需先确认此子密钥是否真实有效, 这是必不可少的环节。根据式(1)判断自己的子密钥 $p_{ij1}, p_{ij2}, \dots, p_{ijk_i}$ 是否线性无关且 $\lambda_{ij1} = \lambda_{ij2} = \dots = \lambda_{ijk_i} = \lambda_{ij}$, 若满足该条件, 则表明参与者获取的子密钥无误, 因而系统没有被攻击; 否则, 说明系统可能出现问题或被攻击, 在此情况下, 需先开展系统维护工作, 再重新向参与者分发子密钥, 直至该条件满足为止。此过程可检验系统的可靠性。

4) 秘密恢复。第1步: 为确保参与秘密恢复的所有成员所提供子密钥的真实性, 在正式启动秘密恢复流程前, 需由每位参与秘密恢复的成员将自身持有的子密钥 p_{ijh} 放入黑盒中完成验证, 只要他们所持有的子密钥同时满足条件1和条件2(条件1: 同一个参与者的子密钥 $p_{ij1}, p_{ij2}, \dots, p_{ijk_i}$ 线性无关且 $\lambda_{ij1} = \lambda_{ij2} = \dots = \lambda_{ijk_i} = \lambda_{ij}$; 条件2: 不同的参与者的子密钥正交), 方可进入下一步操作; 反之, 需立即终止密钥恢复工作。此过程可检验参与秘密

恢复的成员是否诚实, 若满足以上两个条件, 可确认参与秘密恢复的成员是诚实可信的; 若未能满足条件, 则表明参与秘密恢复的成员可能存在欺诈行为, 可按照规定对其追究责任。

第2步: 当确定成员的可信性后, 便可以正式实施秘密恢复。以恢复秘密时参与者最少(即每个集合出1个人, 此时 $m = t$) 为例进行说明。假设成员 B_{11} 是来自集合 B_1 中参与密钥恢复的成员, 其持有子密钥 $(x_{11}, p_{111}), (x_{11}, p_{112}), \dots, (x_{11}, p_{11k_1})$; 成员 B_{21} 是来自集合 B_2 中参与密钥恢复的成员, 持有子密钥 $(x_{21}, p_{211}), (x_{21}, p_{212}), \dots, (x_{21}, p_{21k_2})$; 依次类推, 成员 B_{t1} 是来自集合 B_t 中参与密钥恢复的成员, 持有子密钥 $(x_{t1}, p_{t11}), (x_{t1}, p_{t12}), \dots, (x_{t1}, p_{t1k_t})$ 。成员 $B_{11}, B_{21}, \dots, B_{t1}$ 在黑盒中分别输入自己持有的子密钥, 进而获取与该子密钥项对应的特征值 λ_{ij} 。

第3步: 将 $(x_{11}, \lambda_{11}), (x_{21}, \lambda_{21}), \dots, (x_{t1}, \lambda_{t1})$ 代入多项式 $f(x) = K + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1} \pmod{p}$, 得到方程:

$$\begin{cases} f(x_{11}) = K + a_1 x_{11} + a_2 x_{11}^2 + \dots + a_{t-1} x_{11}^{t-1} \pmod{p} = \lambda_{11}; \\ f(x_{21}) = K + a_1 x_{21} + a_2 x_{21}^2 + \dots + a_{t-1} x_{21}^{t-1} \pmod{p} = \lambda_{21}; \\ \vdots \\ f(x_{t1}) = K + a_1 x_{t1} + a_2 x_{t1}^2 + \dots + a_{t-1} x_{t1}^{t-1} \pmod{p} = \lambda_{t1}. \end{cases} \quad (8)$$

由于 $f(x)$ 是 $(t-1)$ 次曲线, 如果知道 t 个点 (x_{ij}, λ_{ij}) , 曲线就可以表达出来, 而共享密钥 $K \equiv f(0) \pmod{p}$ 。而次线性方程组的系数矩阵为

$$C = \begin{bmatrix} 1 & x_{11} & \dots & x_{11}^{t-1} \\ 1 & x_{21} & \dots & x_{21}^{t-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_{t1} & \dots & x_{t1}^{t-1} \end{bmatrix} \quad (9)$$

因此系数行列式为范德蒙行列式^[17], 因为 $x_{11}, x_{21}, \dots, x_{t1}$ 是互不相等的 t 个数, 所以 $\det C \neq 0$, 由克莱姆法则可知, 方程组有唯一解, 从而可求出 $f(x)$, 即可得到 K 。这恰恰说明了此方案的正确性。

4 具体方案应用

通过部队的军械库安全管理案例, 阐释了一种分角色协同授权机制。

设定一个中队配有2名军械干部和3名军械员共同掌管军械库密钥系统, 按职位等级分为两个集合 $B_1 = \{B_{11}, B_{12}\}$, $B_2 = \{B_{21}, B_{22}, B_{23}\}$, 且所拿子密钥份额按职位等级进行分配, 具体分配如表1所示。

表1 子密钥份额分配

参与者	职位	子密钥份额
B_{11}	军械干部	2
B_{12}		
B_{21}	军械员	1
B_{22}		
B_{23}		

为防范内部舞弊、密钥遗失或人员缺勤等风险,部队规定至少1名军械干部和至少2名军械员在场才能开启军械库。现为所有参与者分配密钥,随后对秘密 K 的重构过程进行分析与梳理。

1)参数选取。设共享秘密 $K=5$,密钥分发者以随机的方式选取素数 $p=7$ 、 $a_1=2$ 、 $a_2=3$,得到多项式 $f(x)=5+2x+3x^2(\bmod 7)$ 。

2)秘密分割。第1步:密钥分发者随机取 $x_{11}=0$ 、 $x_{12}=1$ 、 $x_{21}=2$ 、 $x_{22}=4$ 、 $x_{23}=5$,则 $\lambda_{11}=f(0)=2$ 、 $\lambda_{12}=f(1)=3$ 、 $\lambda_{21}=f(2)=0$ 、 $\lambda_{22}=f(4)=5$ 、 $\lambda_{23}=f(5)=6$,得到7阶对角矩阵:

$$A = \begin{bmatrix} 2 & & & & & & \\ & 2 & & & & & \\ & & 3 & & & & \\ & & & 3 & & & \\ & & & & 0 & & \\ & & & & & 5 & \\ & & & & & & 6 \end{bmatrix}$$

随后黑盒随机生成7阶正交阵 Q :

$$Q = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

就可以得到对称阵 A (保留3位小数): $A=QAQ^{-1}=$

$$\begin{bmatrix} 2 & -2.029 \times 10^{-17} & 0 & 0 & 0 & 0 & 0 \\ -2.029 \times 10^{-17} & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 \end{bmatrix}$$

此时黑盒输出 A 的特征值 $\lambda_{11}=2$ 对应的2个线性无关的特征向量 $p_{111}=(0,1,0,0,0,0)^T$ 、 $p_{112}=(0,0,1,0,0,0)^T$; $\lambda_{12}=3$ 对应的2个线性无关的特

征向量 $p_{121}=(0,0,0,-1/\sqrt{2},1/\sqrt{2},0,0)^T$ 、 $p_{122}=(1,0,0,0,0,0)^T$; $\lambda_{21}=0$ 对应的1个特征向量 $p_{211}=(0,0,0,-1/\sqrt{2},-1/\sqrt{2},0,0)^T$; $\lambda_{22}=5$ 对应的1个特征向量 $p_{221}=(0,0,0,0,0,1,0)^T$; $\lambda_{23}=6$ 对应的1个特征向量 $p_{231}=(0,0,0,0,0,0,1)^T$ 。可得子密钥为 $(x_{11}, p_{111}), (x_{11}, p_{112}), (x_{12}, p_{121}), (x_{12}, p_{122}), (x_{21}, p_{211}), (x_{22}, p_{221}), (x_{23}, p_{231})$ 。

第2步:密钥分发者根据参与者所需子密钥份额将子密钥分发给所有参与者,即把 $k_{11}=(x_{11}, p_{111}) \cup (x_{11}, p_{112})$ 、 $k_{12}=(x_{12}, p_{121}) \cup (x_{12}, p_{122})$ 、 $k_{21}=(x_{21}, p_{211})$ 、 $k_{22}=(x_{22}, p_{221})$ 、 $k_{23}=(x_{23}, p_{231})$ 分别给 B_{11} 、 B_{12} 、 B_{21} 、 B_{22} 、 B_{23} ,其中 x_{ij} 只有参与者自己知道。

第3步:所有参与者获取子密钥后,首要任务是对所持子密钥的真实性进行验证。将 p_{ij} 输入到黑盒中,判断是否满足下列条件:自己所持子密钥 p_{ij1} 、 p_{ij2} 、 $\dots$ 、 p_{ijk} 线性无关且 $\lambda_{ij1}=\lambda_{ij2}=\dots=\lambda_{ijk}=\lambda_{ij}$ 。若满足该条件,则表明参与者获取的子密钥无误,因而系统没有被攻击;否则说明系统可能出现问题或被攻击,在此情况下,需先开展系统维护工作,再重新向参与者分发子密钥,直至该条件满足为止。

3)秘密恢复。假设有1人 B_{11} 来自集合 B_1 ,2人 B_{21} 和 B_{22} 来自集合 B_2 ,则此3人输入的子密钥满足以下两个条件:a) B_{11} 的子密钥 p_{111} 和 p_{112} 线性无关且 $\lambda_{111}=\lambda_{112}=\lambda_{11}$ 、 $\lambda_{211}=\lambda_{21}$ 、 $\lambda_{221}=\lambda_{22}$;b)成员 B_{11} 的子密钥 p_{111} 和 p_{112} 都与成员 B_{21} 的子密钥 p_{211} 正交,且都与成员 B_{22} 的子密钥 p_{221} 正交。此过程可检验参与秘密恢复的成员是否诚实,若未能满足条件,则表明参与秘密恢复的成员可能存在欺诈行为,可按照规定对其追究责任。若满足,则说明参与秘密恢复的成员可信,此时输出所对应的特征值 λ_{ij} ,即输出 $\lambda_{11}=2$ 、 $\lambda_{21}=0$ 、 $\lambda_{22}=5$ 。接下来恢复秘密 K ,构造方程组:

$$\begin{cases} f(x_{11}) = K + 2x_{11} + 3x_{11}^2 (\bmod 7) = \lambda_{11}; \\ f(x_{21}) = K + 2x_{21} + 3x_{21}^2 (\bmod 7) = \lambda_{21}; \\ f(x_{22}) = K + 2x_{22} + 3x_{22}^2 (\bmod 7) = \lambda_{22}. \end{cases}$$

即

$$\begin{cases} f(0) = K (\bmod 7) = 2; \\ f(1) = K + a_1 + a_2 (\bmod 7) = 3; \\ f(2) = K + 2a_1 + 4a_2 (\bmod 7) = 0. \end{cases}$$

经计算得到 $K=5$,密码成功恢复。

5 结束语

提出的双重可验证多维秘密共享方案,以有限域多项式和阶对称矩阵为核心,通过系统描述、参数选取、秘密分割、秘密恢复等4步流程实现秘密安全管理,且经范德蒙行列式、克莱姆法则及信息论安全要求验证了正确性与安全性,在部队军械库管理中能满足精细化权限分配与协同授权需求。方案优点在于双重验证机制提升抗攻击能力、多维管理适配复杂秘密场景;缺点是存在一定中心化风险,多项式插值效率需优化。下一步计划引入分布式密钥生成削弱中心化依赖,探索轻量化插值算法,并拓展至跨域军事秘密管理场景进一步验证。

参考文献:

- [1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
- [2] BLAKLEY G R. Safeguarding cryptographic keys [C]// Proceedings of the 1979 International Workshop on Managing Requirements Knowledge. Piscataway, USA: IEEE, 1979: 313-318.
- [3] HILLERY M, BUŽEK V, BERTHIAUME A. Quantum secret sharing[J]. Physical Review A, 1999, 59(3): 1829-1834.
- [4] GUO G P, GUO G C. Quantum secret sharing without entanglement[J]. Physics Letters A, 2003, 310(4): 247-251.
- [5] BUFALO M, BUFALO D, ORLANDO G. A note on the computation of the modular inverse for cryptography[J]. Axioms, 2021, 10(2): No.116.
- [6] SHEN A, CAO X Y, WANG Y, et al. Experimental quantum secret sharing based on phase encoding of coherent states[J]. Science China Physics (Physics, Mechanics & Astronomy), 2023, 66(6): 139-147.
- [7] YAN F L, GAO T. Quantum secret sharing between multiparty and multiparty without entanglement[J]. Physical Review A, 2005, 72(1): No.012304.
- [8] WANG T Y, WEN Q Y. Security of a kind of quantum secret sharing with single photons[J]. Quantum Information and Computation, 2011, 11(5&6): 434-443.
- [9] HSU J L, CHONG S K, HWANG T, et al. Dynamic quantum secret sharing[J]. Quantum Information Processing, 2013, 12(1): 331-344.
- [10] QIN H W, DAI Y W. Dynamic quantum secret sharing by using d-dimensional GHZ state[J]. Quantum Information Processing, 2017, 16(3): No.64.
- [11] YANG C W, TSAI C W. Participant attack and improving dynamic quantum secret sharing using d-dimensional GHZ state[J]. Modern Physics Letters A, 2020, 35(6): No.2050024.
- [12] QIN H W, TANG W K S, TSO R. Hierarchical quantum secret sharing based on special high-dimensional entangled state[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2020, 26(3): No.6600106.
- [13] 陈克勤, 邹峥, 蔡彬彬, 等. 基于高维 GHZ 态的动态分层量子秘密共享协议[J]. 网络与信息安全学报, 2024, 10(5): 134-144.
- [14] MA R H, GAO F, CAI B B, et al. Quantum secret reconstruction[J]. Advanced Quantum Technologies, 2024, 7(2): No.2300273.
- [15] 张艳硕, 李文敬, 陈雷, 等. 基于特征值的可验证特殊门限秘密共享方案[J]. 通信学报, 2018, 39(8): 169-175.
- [16] 张艳硕, 李文敬, 赵耿, 等. 基于特征值的无可信中心的秘密共享方案研究[J]. 电子与信息学报, 2018, 40(11): 2752-2757.
- [17] 张艳硕, 李文敬, 史国振, 等. 基于特征值的黑盒子意义下的特殊门限秘密共享方案[J]. 计算机应用研究, 2019, 36(8): 2444-2448; 2463.
- [18] 张艳硕, 王泽豪, 杜耀刚, 等. 基于矩阵特征值的可验证无可信中心门限方案[J]. 武汉大学学报(理学版), 2020, 66(2): 135-140.
- [19] 同济大学数学科学学院. 线性代数习题册[M]. 3版. 上海: 同济大学出版社, 2024: 1-104.
- [20] 曹尔强, 张沂, 曹晔, 等. “软件黑盒子”文件加锁和加密的一个方法[J]. 长春邮电学院学报, 1991, 9(3): 11-14.

(编辑: 冯 春)