Pure Mathematics 理论数学, 2026, 16(6), 36-43
Published Online June 2026 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2026.166154

Hans汉斯

基于有限域上多项式的存在特权集的门限签名研究

陈超粤

成都理工大学数学科学学院，四川 成都

收稿日期：2026年4月16日；录用日期：2026年5月14日；发布日期：2026年6月24日

摘　要

针对存在特权集的门限签名中传统双重秘密共享机制存在的密钥分发复杂及安全短板问题，本文提出了一种基于有限域上相似多项式的改进方案。该方案利用Schnorr签名体制，构建了一个仅在常数项上存在差异的主多项式与辅助多项式。通过这种构造，将特权成员与普通成员绑定在同一数学框架下，既实现了特权集成员对签名过程的强制参与，又消除了两组防护水平不一致带来的安全隐患。安全性分析表明，该方案满足信息论安全，优化了密钥分发与管理的复杂度，且能有效抵抗合谋攻击。

关键词

门限签名，特权集，相似多项式

Research on Threshold Signature Scheme with Privilege Set Based on Polynomials over Finite Fields

Chaoyue Chen

School of Mathematical Sciences, Chengdu University of Technology, Chengdu Sichuan

Received: April 16, 2026; accepted: May 14, 2026; published: June 24, 2026

Abstract

To address the issues of complex key distribution and the "security short-board effect" inherent in the traditional dual secret sharing mechanism within privilege set threshold signatures, this paper proposes an improved scheme based on similar polynomials over a finite field. Leveraging the Schnorr signature scheme, the proposed method constructs a primary polynomial and an auxiliary

文章引用: 陈超粤. 基于有限域上多项式的存在特权集的门限签名研究[J]. 理论数学, 2026, 16(6): 36-43.
DOI: 10.12677/pm.2026.166154

polynomial that differ solely in their constant terms. By binding privileged members and ordinary members within a unified mathematical framework, this construction not only enforces the mandatory participation of the privileged set in the signing process but also eliminates the security vulnerabilities arising from inconsistent protection levels between the two groups. Security analysis demonstrates that the proposed scheme achieves information-theoretic security, optimizes the complexity of key distribution and management, and effectively resists collusion attacks.

Keywords

Threshold Signatures, Privileged Set, Similar Polynomials

1. 引言

在现代密码学中，数字签名技术作为保障数据完整性与身份认证的核心机制，正面临着从单一主体向多主体协同演进的挑战。特别是在企业级联盟链、多方安全计算、以及关键基础设施的访问控制等场景下，参与实体往往呈现出明显的层级化特征[1]。这种层级化不仅体现在物理节点的分布上，更体现在逻辑权限的差异上，即系统中存在一个或多个特权成员，其决策权重或法律地位高于普通成员。为了在密码学层面严谨地刻画这种非对称的信任关系，存在特权集的门限签名方案成为了学术界与工业界共同关注的焦点。

传统的门限签名方案，如基于 Shamir 秘密共享的(t,n)体制[2]，虽然在均衡参与模型中表现出色，但其隐含的“参与者地位平等”假设在特权场景下显得捉襟见肘。为此，研究者引入了双重秘密共享机制，试图通过为特权集与普通集分别构建独立的秘密多项式来实现权限的解耦。然而，这种解耦并非没有代价。现有双重共享方案普遍面临着一个结构性的安全脆弱性：两组秘密多项式的独立性导致系统的整体安全性取决于防护能力较弱的那一侧，同时，密钥分发中心需要维护两套独立的参数体系，这不仅增加了计算与通信的开销，更在理论上引入了额外的攻击面。针对上述结构性缺陷，本文提出了一种基于有限域相似多项式的创新性构造。本文的核心洞察在于，特权成员与普通成员并非必须依赖完全独立的秘密空间，而是可以通过数学上的“相似性”进行关联。具体而言，我们设计了一个辅助多项式来模拟普通成员的份额分布，该多项式与特权成员的主多项式仅在常数项(即秘密本身)上存在差异，而在高次项系数上完全共享。这种构造巧妙地将两组成员绑定在同一数学框架下，既保证了特权成员在签名生成中的主导地位，又消除了双重共享机制所带来的独立性安全隐患。

2. 门限签名方案设计

本章以 Schnorr 门限签名为例[3]，给出具体的$(t,n+d)$门限签名方案设计。

1) 系统初始化阶段：D 为秘密分发人，为 n 个普通群成员，$\mathrm{U}_1,\mathrm{U}_2,\cdots,\mathrm{U}_d$ 为 d 个拥有特权的群成员，t 为门限值，$d<t<n$，秘密 $a_0\in\mathbf{F}_q^*$，q 为素数，m 为待签名的消息。秘密分发人 D 取循环群 $\mathbf{F}_q^*$ 的生成元 g 并将其公布，设置域 $\mathbf{F}_q^*$ 上秘密多项式

$$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0\mathrm{P}_1,\mathrm{P}_2,\cdots,\mathrm{P}_n$$

和辅助多项式

$$y(x)=f(x)-a_0=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x.$$

秘密分发人随机选取 $n+1$ 个非零元素 $x_0,x_1,\cdots,x_n\in\mathbf{F}_q$，计算 $y_i=y(x_i)$，$i=0,1,\cdots,n$，将 (x_0,y_0) 发送给所有特权群成员，将后 n 个形如 (x_i,y_i) 的普通私钥份额对分别发送给 n 个普通群成员 $\mathrm{P}_1,\mathrm{P}_2,\cdots,\mathrm{P}_n$；再随机选取 d 个不同于以上 $n+1$ 个元素的非零元素 $u_1,u_2,\cdots,u_d\in\mathbf{F}_q$，计算 $f_i=f(u_i)$，$i=0,1,2,\cdots,d$，将形如 (u_i,f_i) 的特权私钥份额对分别发送给 d 个特权群成员 $\mathrm{U}_1,\mathrm{U}_2,\cdots,\mathrm{U}_d$；秘密分发人 D 计算并公布公钥 $Q=g^{a_0}\bmod q$，最后销毁所有秘密参数与内部状态。

2) 签名生成阶段：不妨设参与签名生成的 t 个群成员为 $\mathrm{P}_1,\mathrm{P}_2,\cdots,\mathrm{P}_{t-1},\mathrm{U}_1$。为了规范符号的使用，之后本文用 P_0 指代 U_1。不妨设子集 T: $\mathrm{P}_1,\mathrm{P}_2,\cdots,\mathrm{P}_{t-1},\mathrm{P}_0$。T 集的每个成员选择随机数 $k_i\in\mathbf{N}^+$，计算 $r_i=g^{k_i}\bmod q$，向 T 集的其他成员公布 r_i，每个 T 集的成员利用 t 个 r_i 计算 $r=\prod_{i=0}^{t-1}r_i\bmod q$，公布哈希值 $c=Hash(m\|r)$。

群成员 $\mathrm{P}_i\,(i=0,1,\cdots,t-1)$ 计算

$$\Delta_i=\prod_{\substack{P_j\in T\\ x_j\neq x_i}}\frac{u_1-x_j}{x_i-x_j},$$

然后利用选择的随机数 $k_i\in\mathbf{N}^+$，计算出签名份额 $s_i=(cy_i\Delta_i+k_i)\bmod(q-1)$，之后将 s_i 公布给其他 T 集的成员。最后，群成员 P_0 利用特权私钥份额 f_1 和收集的 t 个签名份额计算

$$s=\left(cf_1-\sum_{i=0}^{t-1}s_i\right)\bmod(q-1),$$

形成签名

$$\sigma=(c,s).$$

3) 签名验证阶段：验证方收到消息 m 和 $\sigma=(c,s)$ 后，计算 $r_0=\left(g^sQ^{-c}\right)^{-1}\bmod q$，若 $r_0\neq r$ 则拒绝签名，否则，进行下一步；计算 $c_0=Hash(m\|r_0)$，比较 c 和 c_0，相等则接受签名，否则拒绝签名。

3. 门限签名方案分析

3.1. 正确性分析

因为签名份额 $s_0=(cy_0\Delta_0+k_0)\bmod(q-1)$，所以可设 $s_0=(cy_0\Delta_0+k_0)+(q-1)w_0$，$w_0\in\mathbf{Z}$；同理，可设 $s_i=(cy_i\Delta_i+k_i)+(q-1)w_i$，$w_i\in\mathbf{Z}$，$i=1,\cdots,t-1$；$s=\left(cf_1-\sum_{i=0}^{t-1}s_i\right)+(q-1)w_t$，$w_t\in\mathbf{Z}$。

此时，有

$$s=cf_1-\sum_{i=0}^{t-1}\left[cy_i\Delta_i+k_i+(q-1)w_i\right]+(q-1)w_t,$$

将其代入 g^s，得

$$g^s=g^{cf_1}g^{-c\sum_{i=0}^{t-1}y_i\Delta_i}g^{-\sum_{i=0}^{t-1}k_i}g^{-\sum_{i=0}^{t-1}(q-1)w_i}g^{(q-1)w_t}.$$

针对 $g^{(q-1)w_t}$ 和 $g^{-\sum_{i=0}^{t-1}(q-1)w_i}$，有

$$g^{(q-1)w_t}\equiv 1\bmod q,$$

和

$$g^{-\sum_{i=0}^{t-1}(q-1)w_i}\equiv 1\bmod q,$$

所以

$$g^s\equiv g^{cf_1}g^{-c\sum_{i=0}^{t-1}y_i\Delta_i}g^{-\sum_{i=0}^{t-1}k_i}\bmod q.$$

根据拉格朗日插值法，有

$$a_0 = f(u_1) - y(u_1) = f_1 - \sum_{i=0}^{t-1} y_i \Delta_i,$$

所以

$$g^s \equiv g^{ca_0} g^{-\sum_{i=0}^{t-1} k_i} \bmod q.$$

将 g^s 和 $Q = g^{a_0} \bmod q$ 代入 $r_0 = \left(g^s Q^{-c}\right)^{-1} \bmod q$，得

$$r_0 \equiv Q^c \left(g^s\right)^{-1} \equiv g^{ca_0} g^{\sum_{i=0}^{t-1} k_i} g^{-ca_0} \bmod q \equiv g^{\sum_{i=0}^{t-1} k_i} \bmod q.$$

因为

$$r = \prod_{i=0}^{t-1} r_i \bmod q \equiv \prod_{i=0}^{t-1} g^{k_i} \bmod q \equiv g^{\sum_{i=0}^{t-1} k_i} \bmod q$$

所以必有

$$r = r_0.$$

根据以上分析，有 $c_0 = Hash(m \| r_0) = Hash(m \| r) = c$，与常规 Schnorr 签名算法一致[4]。

3.2. 安全性分析

3.2.1. 不可伪造性的归约证明

安全模型定义：本节在随机预言模型下，基于有限域 $\mathbf{F}_q$ 上的离散对数问题的困难性，对存在特权集的门限签名方案进行形式化安全证明。我们采用标准的 EUF-CMA 安全模型[5]。该模型涉及两个参与者：一个概率多项式时间敌手 $\mathcal{A}$ 和一个挑战者 $\mathcal{C}$。

系统参数：设 λ 为安全参数，g 为循环群 $\mathbf{F}_q^*$ 的生成元，q 为大素数。

模型建立：

1、初始化：挑战者 $\mathcal{C}$ 运行系统初始化算法，生成公钥 PK 和对应的主私钥份额分发机制(包含多项式 $f(x)$ 和 $y(x)$ 的构造逻辑)，并将 PK 发送给敌手 $\mathcal{A}$。

2、查询：敌手 $\mathcal{A}$ 可以自适应地进行多项式有界的询问：

哈希查询：$\mathcal{A}$ 询问哈希预言机 $H(\cdot)$，$\mathcal{C}$ 返回随机值。

签名查询：$\mathcal{A}$ 提交消息 m，$\mathcal{C}$ 模拟 t 个成员(包含至少一个特权成员)的签名协议，返回合法签名 $\sigma = (c, s)$。

3、伪造：最终，$\mathcal{A}$ 输出一个新消息–签名对 (m^*, σ^*)，其中 m^* 从未被提交过签名查询。

4、胜利条件：若 $\mathcal{A}$ 输出的 σ^* 能通过验证算法 $Verify(PK, m^*, \sigma^*) = Accept$，且 m^* 是新的，则 $\mathcal{A}$ 获胜。

定义 1 (EUF-CMA 安全性)：一个特权集门限签名方案是 EUF-CMA 安全的，如果对于任意 PPT 敌手 A，其赢得上述流程的优势 $Adv_A(\lambda)$ 是关于 λ 的可忽略函数。

我们将证明：如果存在一个能以不可忽略优势破解本文方案的敌手 $\mathcal{A}$，那么我们就能构造一个算法 $\mathcal{B}$，利用 $\mathcal{A}$ 来解决 $\mathbf{F}_q$ 上的离散对数问题。

定理 1：在随机预言模型下，若有限域 $\mathbf{F}_q$ 上的离散对数问题是难解的，则本文提出的基于相似多项式的特权集门限签名方案满足 EUF-CMA 安全性。

假设存在一个敌手 $\mathcal{A}$ 能以优势 ϵ 破解本文方案，即 $\mathcal{A}$ 能伪造一个有效签名。我们将构建一个模拟器 $\mathcal{B}$，其目标是求解给定的 DLP 实例：给定 (g, h)，其中 $h = g^x$，求 x。

1. 系统模拟：$\mathcal{B}$ 接收到挑战实例 (g, h)。$\mathcal{B}$ 将 h 设为系统的公钥 Q，即隐含地设定主私钥 $a_0 = x$ 这是 $\mathcal{B}$ 需要求解的秘密)。$\mathcal{B}$ 选择主多项式 $f(x)$ 的高次项系数 $\{a_{t-1}, \cdots, a_1\}$ 并公布。注意，$\mathcal{B}$ 不知道常数项 a_0

(即 x)。$\mathcal{B}$ 构造辅助多项式 $y(x)=f(x)-a_0$。由于 $\mathcal{B}$ 知道 $f(x)$ 的除了 a_0 之外的所有系数，它完全掌握 $y(x)$ 的结构。$\mathcal{B}$ 生成普通成员的份额 (x_i,y_i) 并发送给 $\mathcal{A}$。

2. 预言机模拟：

哈希预言机：$\mathcal{B}$ 维护列表记录 (m,r,c) 的映射，返回一致的哈希值。

签名预言机：当 $\mathcal{A}$ 请求签名时，$\mathcal{B}$ 模拟成员交互。对于普通成员 P_i，$\mathcal{B}$ 知道私钥份额 y_i，可计算 s_i。对于特权成员 U_j，$\mathcal{B}$ 无法直接计算 $f(u_j)$。这里利用 Schnorr 签名性质，$\mathcal{B}$ 直接生成满足 $g^s \equiv rQ^c \bmod q$ 的签名。

3. 伪造与提取：假设 $\mathcal{A}$ 输出针对新消息 m^* 的有效伪造签名 $\sigma^*=(c^*,s^*)$。根据验证等式：

$$g^{s^*} \equiv r^* Q^{c^*} \bmod q,$$

代入 $Q=g^{a_0}$，得

$$g^{s^*} \equiv r^* g^{a_0 c^*} \bmod q,$$

整理得

$$g^{s^*-a_0 c^*} \equiv r^* \bmod q.$$

归约结论：由于 $\mathcal{A}$ 是在不知道 a_0 的情况下生成了 s^* 和 r^*，且满足上述等式。如果 $\mathcal{A}$ 没有询问过 m^* 的签名，那么 $\mathcal{A}$ 必须直接解出 a_0 才能构造出满足该等式的 s^*。如果 $\mathcal{A}$ 能以优势 ϵ 伪造签名，那么 $\mathcal{B}$ 即可通过分析 $\mathcal{A}$ 的输出，以至少 ϵ' 的优势计算出 $a_0=\log_g Q$。这与有限域 $\mathbf{F}_q$ 上离散对数问题的困难性假设矛盾。

因此，假设不成立。在随机预言模型下，本文方案是 EUF-CMA 安全的。

3.2.2. 特权集特定安全属性分析

本节给出对特权集的具体安全性分析。

特权集强制参与性：t 个普通成员联合，能计算出 $\sum s_i$，甚至能恢复辅助多项式 $y(x)$，但是无法从 $y(x)$ 中推导出包含秘密信息的 f_1，按照签名公式 $s=\left(cf_1-\sum_{i=0}^{t-1}s_i\right)\bmod(q-1)$。普通成员无法生成合法签名。这一特点保证了若没有特权群成员参与，则无法生成签名，满足了特权集的强制参与性[6]。

抗合谋攻击：

普通组合谋：普通成员持有由辅助多项式 $y(x)$ 生成的份额。由于 $y(x)=f(x)-a_0$，$y(x)$ 不包含秘密信息，所以即使 t 个普通成员合谋，也不能获得主密钥 a_0。

特权组合谋：特权成员各自持有特权私钥份额对 (u_i,f_i)，共同持有普通私钥份额对 (x_0,y_0)，由于 $d<t$，即使所有特权成员合谋，他们虽然知道秘密多项式 $f(x)$ 的部分信息，但是无法进行有效的拉格朗日插值来恢复 $f(x)$ 的全部系数，更无法获得主密钥 a_0。

消除安全短板问题：在解决安全短板问题，传统的双重秘密共享体制需要独立维护两个秘密，攻击者只需要攻破防护较弱的那一组即可获得部分密钥。本文方案中，普通组的辅助多项式 $y(x)$ 不包含主密钥 a_0，即使攻击者获得 $y(x)$，因为没有特权私钥份额对，无法求出 $f(x)$，所以本方案的安全性取决于重构主多项式 $f(x)$ 的整体难度。

3.2.3. 其他安全性分析

针对恶意分发者的安全性分析：在本方案的初始设定中，我们假设秘密分发人是诚实的。然而，在某些高安全需求的场景中，若秘密分发人是恶意的，他可能不按照规定的分布生成多项式系数，或者不将份额分发给所有成员，从而破坏系统的正确性或安全性。本方案的数学结构天然兼容可验证秘密共享

(VSS)机制。虽然基础方案未显式包含承诺步骤，但生成的主多项式 $f(x)$ 和辅助多项式 $y(x)$ 的系数是公开验证的。具体而言，秘密分发人广播 Petersen 承诺 $C_j = g^{a_j} h^{b_j}$，其中 a_j 是多项式系数，b_j 是盲化因子，成员可以通过验证接收到的份额是否符合广播的承诺来验证秘密分发人的诚实性。

前向安全性分析：本方案基于 Schnorr 签名机制，在签名生成阶段，每个参与者均独立选取随机数 k_i 作为临时私钥，并计算 $r_i = g^{k_i} \bmod q$。最终的签名依赖于聚合的随机数和挑战值。根据 Schnorr 签名的安全性质，只要临时私钥 k_i 在每次签名后被安全销毁且不重复使用，即使长期私钥 a_0 泄露，攻击者也无法根据公开的签名值推导出临时私钥。

3.3. 性能与效率分析

本节在六组不同参数配置下，对比本文方案与传统的基于双重秘密共享的门限签名方案的综合性能，传统方案的门限签名设计思路来源于文献[7]。具体参数配置涵盖了普通成员数量 n、特权成员数量 d 及门限值 t 的变化，分别为 20:6:12、20:6:13、20:7:12、20:7:13、21:6:12 以及 22:6:12，测试结果如图 1~3 所示。

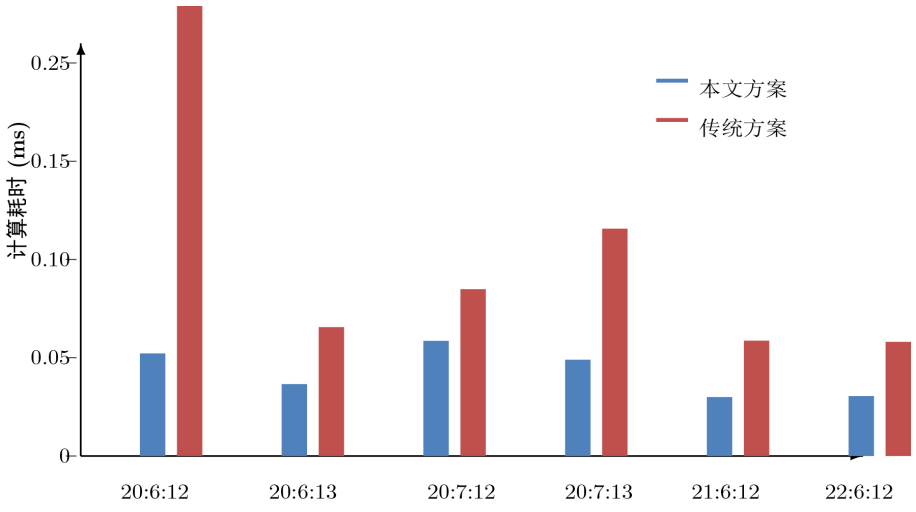

Figure 1. Comparison of key generation time
图 1. 密钥生成阶段计算耗时对比

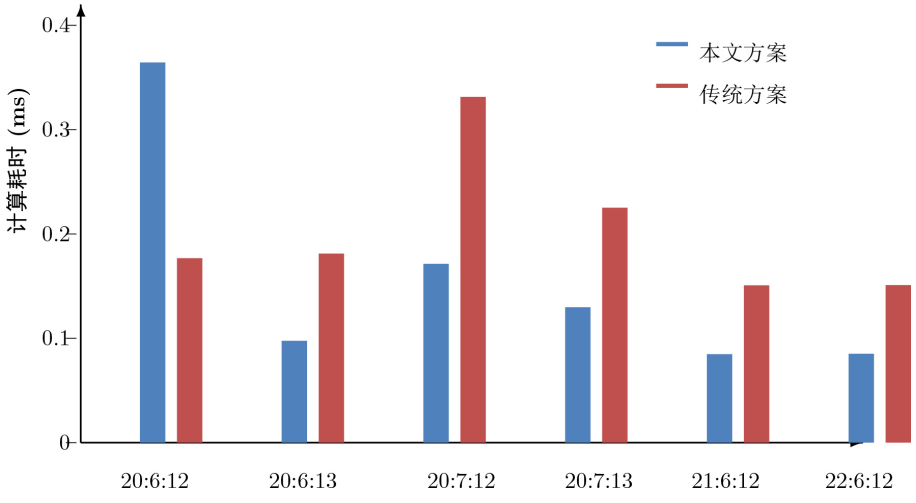

Figure 2. Comparison of signature generation time
图 2. 签名生成阶段计算耗时对比

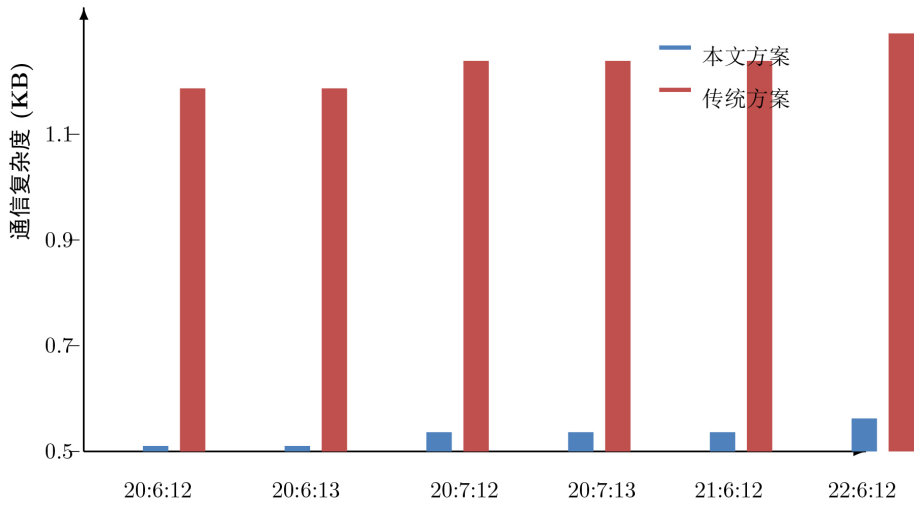

Figure 3. Comparison of communication complexity
图 3. 通信复杂度对比

根据以上统计图，本文方案与传统方案在不同性能维度上呈现出差异化优势：在密钥生成阶段，本文方案的计算耗时(蓝色柱形)始终低于传统方案(红色柱形)，尤其在参数规模较大时，效率优势更为突出；签名生成阶段则呈现复杂特征——在部分参数组合下本文方案耗时略高，但在多数场景中仍能保持较低的计算开销，整体表现与传统方案基本持平；通信复杂度方面，本文方案展现出优势，其通信开销(蓝色柱形)在所有测试场景中均低于传统方案，且在参数规模扩大时差距进一步拉大。综合来看，本文方案通过优化密钥生成和通信效率，在保障安全性的同时实现了更优的系统性能，尤其在资源受限的网络环境中更具应用价值。

4. 结束语

针对现有的存在特权集的门限签名方案中双重秘密共享机制带来的密钥分发复杂度高与安全短板问题，本文提出了一种基于有限域相似多项式的改进方案。该方案通过构造包含秘密项与不包含秘密项的两个关联多项式，巧妙地实现了特权集成员与普通成员的差异化权限管理。最大的改进在于安全性层面：理论分析与实验表明，该方案确保了特权集与普通集在安全防护水平上的一致性，有效规避了传统双重秘密共享中因两组防护水平不一致导致的安全短板问题，即攻击者无法通过攻破防护较弱的普通组来间接威胁主密钥安全。然而，本文方案也有局限性。正如性能测试所示，在签名生成阶段，本方案并未体现出显著的效率优势，其计算开销与传统方案基本相当，甚至在部分高并发场景下可能略高，这是因为签名过程中的核心密码学运算并未因多项式构造的改变而减少。

另外本文对前向安全性的讨论有限，主要因为严格的前向安全性通常需要结合密钥更新协议，这超出了本文静态门限签名的研究范畴。未来的工作将致力于在保持两组安全防护水平一致这一核心优势的前提下，进一步优化签名算法的计算复杂度[8] [9]，探索更高效的聚合签名策略，以及更复杂的模型和动态密钥更新场景。

参考文献

[1] 智勇. 一种混合数据加密方案在企业管理系统中的应用[J]. 网络安全技术与应用, 2019(4): 30-33.

[2] Abdel Hakeem, S.A. and Kim, H. (2022) Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication. *Sensors*, **22**, Article 331. https://doi.org/10.3390/s22010331

[3] Cimatti, A., De Sclavis, F., Galano, G., Giammusso, S., Iezzi, M., Muci, A., *et al*. (2025) Dynamic-FROST: Schnorr Threshold Signatures with a Flexible Committee. *Journal of Mathematical Cryptology*, **19**, Article 20240045. https://doi.org/10.1515/jmc-2024-0045

[4] Ji, Y., Zhang, R., Tao, Y. and Gao, B. (2024) Designated Confirmer Threshold Signature and Its Applications in Blockchains. *Cybersecurity*, **7**, Article No. 67. https://doi.org/10.1186/s42400-024-00256-2

[5] 汪玉. 一种无证书环签名方案及应用研究[D]: [硕士学位论文]. 武汉: 湖北民族大学, 2025.

[6] 陈道伟, 施荣华, 樊翔宇. 一种存在特权集的门限群代理多重签名方案[J]. 小型微型计算机系统, 2012, 33(11): 2514-2517.

[7] 王天芹. 存在特权集的门限代理群签名方案[J]. 计算机应用研究, 2008(7): 2146-2147+2151.

[8] Jia, X., Wang, L., Cheng, K., Jing, P. and Song, X. (2025) A Blockchain-Based Privacy-Preserving and Collusion-Resistant Scheme (PPCR) for Double Auctions. *Digital Communications and Networks*, **11**, 116-125. https://doi.org/10.1016/j.dcan.2023.05.002

[9] Li, F., Zhao, Y., Zhang, K., Xu, H., Wang, Y. and Wang, D. (2025) Blockchain-Based Lightweight Trusted Data Interaction Scheme for Cross-Domain IIoT. *Digital Communications and Networks*, **11**, 1192-1204. https://doi.org/10.1016/j.dcan.2024.11.018