中国科学 : 信息科学 2026 年 第 56 卷 第 8 期: 2180–2198
SCIENTIA SINICA Informationis
进展

门限签名系统研究进展

李增鹏[1,2,3], 邓旭东[1,2], 王梅[1,2,3*], 魏普文[1,2,3], 王书超[1,2], 耿春秋[1,2]

1. 山东大学网络空间安全学院, 青岛 266237
2. 山东大学密码与数字经济安全全国重点实验室, 青岛 266237
3. 泉城实验室, 济南 100190
* 通信作者. E-mail: wangmeiz@sdu.edu.cn

收稿日期: 2025–07–31; 修回日期: 2025–10–31; 接受日期: 2026–01–06; 网络出版日期: 2026–08–07

国家重点研发计划 (批准号: 2022YFB2701700)、国家自然科学基金 (批准号: 62472255, 62302271)、山东省高等学校青创科技支持计划 (批准号: 2024KJH79)、山东省自然科学基金 (批准号: ZR2023MF045, ZR2023QF088)、青岛市自然科学基金 (批准号: 23-2-1-152-zyyd-jch) 和 CCF – 腾讯犀牛鸟基金 (批准号: CCF-Tencent RAGR20250129) 资助项目

摘要 分布式安全计算的应用研究始终处于数字安全技术创新的核心位置, 其核心价值在数字政务、金融科技、物联网等关键领域持续凸显. 作为分布式数字身份与密钥管理体系的基石, 门限签名技术通过将密钥生成、存储进行分布式管理, 有效解决了传统中心化密钥管理系统存在的单点故障问题, 其抗合谋攻击、高容错性、动态节点管理等特性为构建新一代可信数字基础设施提供了理论基础. 近年来, 美国国家标准技术研究院 (NIST) 和互联网工程任务组 (IETF) 正在积极推动门限签名方案的标准化工作, 特别是对现有国际标准算法 ECDSA, Schnorr/EdDSA 以及具有后量子安全性的签名算法征集高效的门限化构造. 本文分别针对分布式密钥生成 (distributed key generation, DKG)、门限 ECDSA/SM2、门限 Schnorr/EdDSA 和门限格密码签名 4 个方面, 从优化通讯开销、降低交互轮次、增强鲁棒性、实现主动安全等角度, 对国内外相关研究成果进行分析和总结.

关键词 门限签名, 分布式密钥生成, 秘密共享, 后量子安全

1 研究背景及意义

随着数字化进程的加速, 中心化密钥管理模式逐渐暴露出单点故障、密钥托管风险等局限性, 可抵御 “单点故障” 的分布式系统需求日益增长. 传统数字签名依赖于单一私钥的管理与使用, 一旦私钥泄露或持有者失效, 系统将面临严重的安全威胁. 门限签名技术作为分布式安全计算的核心支撑, 因其独特的分布式密钥管理机制、抗单点故障能力及高容错性, 成为学术界和产业界的研究热点 [1,2]. 近来, 美国国家标准技术研究院 (NIST) 和互联网工程任务组 (IETF) 正在积极推动门限签名方案的标准化工作, 特别是对现有国际标准算法 ECDSA, Schnorr/EdDSA 以及具有后量子安全性的签名算法征集高效的门限化构造, 并将具有鲁棒性与自适应安全的门限签名构造列为目标之一 [3,4]. 具有鲁棒性和自适应安全的门限签名能够在有外部干扰甚至部分参与方掉线的情形下, 依旧可靠有效地生成签名, 从而提高参与方间协作效率, 降低协作成本. NIST 和 IETF 所定的标准化目标这一趋势表明, 门限签名技术正从理论研究向实际应用快速过渡, 是未来密码学标准化与产业应用的重要方向. 其研究意义不仅在于优化算法性能与安全性, 更在于为数字经济、Web3.0 等新兴领域的安全升级奠定基础.

引用格式: 李增鹏, 邓旭东, 王梅, 等. 门限签名系统研究进展. 中国科学: 信息科学, 2026, 56: 2180–2198, doi: 10.1360/SSI-2025-0340
Li Z P, Deng X D, Wang M, et al. Recent developments in threshold signature scheme. Sci Sin Inform, 2026, 56: 2180–2198, doi: 10.1360/SSI-2025-0340

门限签名本质是通过将私钥拆分为多个份额, 要求至少达到阈值数量的参与者协作才能生成有效签名, 从根本上规避了单点失效风险, 同时降低了密钥托管带来的信任成本. 因此, 门限签名密码系统被广泛应用于分布式身份/密钥管理、分布式密码学钱包管理以及分布式身份认证等领域. 然而, 门限签名在实际的工业使用中仍面临诸多挑战. 首先, 分布式密钥生成 (distributed key generation, DKG) 协议的效率与安全性直接影响整体方案的可行性, 低交互、高鲁棒性的 DKG 设计亟待突破. 其次, 现有方案在通讯开销、交互轮次及计算复杂度方面存在瓶颈, 难以满足大规模分布式系统的实时性需求. 此外, 随着量子计算的发展, 基于传统数论假设的签名方案面临威胁, 如何设计后量子安全的门限签名也已成为紧迫课题. 随着国内《数据安全法》《个人信息保护法》《网络安全法》及其配套法规体系的日臻完善, 科研机构和企业在推进数据合规实践的同时, 不仅需聚焦安全合规的顶层应用, 更应深入研究制约数据要素安全的底层密码学机制与隐私增强技术 [5], 其中门限签名是构建可信分布式系统中不可或缺的关键技术之一.

因此, 本文着重围绕各类代表性门限签名, 从通讯开销、交互轮次优化、鲁棒性与主动安全实现等角度, 对国内外相关研究成果进行分析和总结. 期望总结现有门限签名机制的理论和技术, 为分布式安全计算和应用的隐私保护问题提供系统的理论依据和技术参考.

2　基本概念与相关性质

2.1　符号和简写

记 λ 为安全参数. 对于一个有限集合 S, 用 $|S|$ 表示该集合的大小. 对于整数 $a \in \mathbb{N}$, 用 $[a]$ 表示有序集合 $\{1,\dots,a\}$. 若未作特殊说明, 所有算法均为概率多项式时间算法 (probabilistic polynomial-time, PPT), 即其在多项式时间内运行并可能使用随机性.

2.2　门限签名的基本定义

定义1 ([6])　(t,n) 门限签名方案由一组 $n \geqslant 1$ 个参与方执行, 其中任何大于等于 t 个参与方都能够完成签名, 而任何少于 t 个参与方则无法完成签名或获得与签名相关的任何秘密信息. 对于消息空间 $\mathcal{M}$, 一个 (t,n) 门限签名方案由 4 个 PPT 算法 $\mathsf{TS}=(\mathsf{Setup},\mathsf{KeyGen},\mathsf{TSign},\mathsf{Verify})$ 组成, 定义如下.

- $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$: 初始化算法输入安全参数 λ, 输出公开参数 pp.
- $(\mathsf{vk},(\mathsf{sk}_i,\mathsf{pk}_i)_{i\in[n]}) \leftarrow \mathsf{KeyGen}(\mathsf{pp},t,n)$: 密钥生成算法的输入有公开参数 pp, 重建门限 t, 签名者数量 n, 其中 $1 \leqslant t \leqslant n$, 输出公钥 vk, 私钥份额集合 $\{\mathsf{sk}_1,\dots,\mathsf{sk}_n\}$ 和公钥份额集合 $\{\mathsf{pk}_1,\dots,\mathsf{pk}_n\}$. 每个签名者 $i \in [n]$ 持有 $(\mathsf{vk},\mathsf{sk}_i,\mathsf{pk}_i)$.
- $\mathsf{sig} \leftarrow \mathsf{TSign}(\{\mathsf{pk}_1,\mathsf{sk}_1\},\dots,\{\mathsf{pk}_{t'},\mathsf{sk}_{t'}\},\mathsf{msg})$: 对于消息 $\mathsf{msg} \in \mathcal{M}$, 任意签名者集合 t' ($|t'| \geqslant |t|$) 中的每个签名者分别运行签名算法, 输入公私钥份额 $(\mathsf{pk}_j,\mathsf{sk}_j)$, 得到对消息 msg 的签名份额 sig_j. 最终聚合所有的签名份额 $\{\mathsf{sig}_j\}_{j\in[t']}$, 输出对消息 msg 的签名 sig.
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{vk},\mathsf{msg},\mathsf{sig})$: 验证算法输入公钥 vk, 消息 msg, 以及签名 sig, 如果 sig 是有效的签名, 则算法返回 1, 反之则返回 0.

2.3　门限签名的性质

定义2 (正确性 (correctness))　给定 (t,n) 门限签名方案 TS, 对于安全参数 λ, 消息 $\mathsf{msg} \in \mathcal{M}$, 签名参与方集合 $\mathsf{act} \subseteq [n]$ ($|\mathsf{act}| \geqslant t$), 若存在可忽略函数 $\mathsf{negl}(\cdot)$ 使得以下条件满足则正确性成立:

$$\Pr[\mathsf{Game}^{\mathsf{ts\text{-}cor}}_{\mathsf{TS}}(\lambda,n,t,\mathsf{msg},\mathsf{act})=1] \geqslant 1-\mathsf{negl}(\lambda).$$

正确性游戏 $\mathsf{Game}^{\mathsf{ts\text{-}cor}}_{\mathsf{TS}}(\lambda,n,t)$**.** 挑战者运行 $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$ 和 $(\mathsf{vk},(\mathsf{sk}_i,\mathsf{pk}_i)_{i\in[n]}) \leftarrow \mathsf{KeyGen}(\mathsf{pp},t,n)$. 对任意消息 msg, 由 act 中各参与方执行签名算法 $\mathsf{sig} \leftarrow \mathsf{TSign}(\{(\mathsf{pk}_j,\mathsf{sk}_j)\}_{j\in\mathsf{act}},\mathsf{msg})$, 挑战者最终输出对签名 sig 的验证 $\mathsf{Verify}(\mathsf{vk},\mathsf{msg},\mathsf{sig})$.

定义3 (不可伪造性 (unforgeability))　给定 (t,n) 门限签名方案 TS 与 PPT 敌手 $\mathcal{A}$, 对于安全参数 λ, 消息 $\mathsf{msg}\in\mathcal{M}$, 签名参与方集合 $\mathsf{act}\subseteq[n]$ ($|\mathsf{act}|\geqslant t$), 定义 $\mathcal{A}$ 的优势为

$$\mathsf{Adv}^{\mathsf{ts\text{-}uf}}_{\mathcal{A},\mathsf{TS}}(\lambda,n,t):=\Pr\big[\mathsf{Game}^{\mathsf{ts\text{-}uf}}_{\mathcal{A},\mathsf{TS}}(\lambda,n,t)=1\big],$$

若对任意 $\mathcal{A}$ 都有 $\mathsf{Adv}^{\mathsf{ts\text{-}uf}}_{\mathcal{A},\mathsf{TS}}(\lambda,n,t)\leqslant\mathsf{negl}(\lambda)$, 则称 TS 满足 (门限) 不可伪造性.

不可伪造性游戏 $\mathsf{Game}^{\mathsf{ts\text{-}uf}}_{\mathcal{A},\mathsf{TS}}(\lambda,n,t)$**.** 挑战者运行 $\mathsf{pp}\leftarrow\mathsf{Setup}(\lambda)$ 和 $(\mathsf{vk},(\mathsf{sk}_i,\mathsf{pk}_i)_{i\in[n]})\leftarrow\mathsf{KeyGen}(\mathsf{pp},t,n)$, 公开 $(\mathsf{pp},\mathsf{vk})$. 设腐化集合 $\mathsf{Corr}\leftarrow\varnothing$, 并初始化查询消息集合 $\mathcal{M}\leftarrow\varnothing$. 敌手 $\mathcal{A}$ 可自适应访问以下两个预言机.

- **签名预言机** $\mathcal{O}_{\mathsf{sign}}(\mathsf{msg},\mathsf{act})$: 对于任意消息 msg, 预言机计算 $\mathsf{sig}\leftarrow\mathsf{TSign}(\{(\mathsf{pk}_j,\mathsf{sk}_j)\}_{j\in\mathsf{act}},\mathsf{msg})$, 并返回 sig 给敌手, 同时将 msg 加入 $\mathcal{M}$.
- **腐化预言机** $\mathcal{O}_{\mathsf{corr}}(i)$: 若 $|\mathsf{Corr}|<t$ 且 $i\notin\mathsf{Corr}$, 则返回 sk_i 并令 $\mathsf{Cor}\leftarrow\mathsf{Cor}\cup\{i\}$; 否则终止游戏.

最终敌手输出一个伪造签名 $(\mathsf{msg}^\star,\mathsf{sig}^\star)$. 若此时满足 $\mathsf{msg}^\star\notin\mathcal{M}$ 且 $|\mathsf{Corr}|<t$, 挑战者最终输出对签名 $\mathsf{sig}^\star$ 的验证 $\mathsf{Verify}(\mathsf{vk},\mathsf{msg}^\star,\mathsf{sig}^\star)$.

定义4 (鲁棒性 (robustness) 与弱鲁棒性 (weak robustness))　鲁棒性指一个系统在受到外部干扰或部分组件异常时, 仍能维持其预期的功能与稳定性. 在多方计算协议中, 鲁棒性要求即使存在恶意参与方, 也不能阻止诚实参与方获得协议输出. 即协议应保证诚实方能最终完成计算并获得正确结果, 这一性质又被称为有保证输出交付性 (guaranteed output delivery). 弱鲁棒性要求协议在遭遇恶意行为时, 虽然可能无法立即完成输出, 但至少能够识别出导致协议中止的恶意参与方, 并在重启或替换后继续执行. 在门限签名中, 这一性质通常被称为可识别中止性 (identifiable abort).

2.4　门限签名的敌手假设

在对安全性的非正式定义中往往会忽略一个问题, 即攻击协议执行的敌手的能力, 通常情况下会假设敌手可以控制协议中部分参与方. 在此, 我们总结了敌手的腐化策略, 允许的敌手行为, 以及假定敌手具有什么样的复杂度. 本文将描述已被考虑的主要敌手类型.

(1) **腐化策略**: 腐化策略处理的是参与方何时以及如何被腐化的问题. 腐化模型分为以下两种.

- 静态腐化模型: 在该模型中, 敌手控制一组固定的参与方. 诚实的参与方始终保持诚实, 腐化的参与方始终处于腐化状态.
- 自适应腐化模型: 与静态腐化模型不同, 自适应敌手能够在计算过程中腐化参与方. 敌手可以任意决定何时以及腐化哪些参与方, 并且这种选择可能取决于其在执行过程中观察到的内容 (因此称为 “自适应”). 这种策略模拟了外部 “黑客” 在执行过程中入侵机器的行为. 在这种模型中, 一旦某个参与方被腐化, 从那时起该参与方将始终处于腐化状态.

(2) **敌手行为**: 允许的敌手行为与被腐化的参与方可以采取的行为有关, 主要有两种类型的敌手.

- 半诚实 (semi-honest) 敌手: 在半诚实敌手模型中, 模拟了诚实参与方在无意中泄露信息的情境. 尽管某些参与方可能会被腐化, 但它们仍会正确遵循协议规范. 然而, 敌手能够获取所有被腐化参与方的内部状态, 包括其接收到的所有消息记录, 并尝试利用这些信息推测本应保密的数据. 故半诚实敌手也被视为被动 (passive) 攻击者, 因为它们只能通过观察协议执行过程中收到的信息来试图获取秘密, 而无法采取其他攻击手段. 半诚实敌手通常也被称为诚实但好奇 (honest-but-curious) 攻击者, 例如当参与方之间基本上互相信任, 但希望确保除了输出之外不会泄露其他信息时. 此外, 该模型也适用于能够强制执行 “正确” 软件以确保协议准确执行的环境.
- 恶意 (malicious) 敌手: 恶意敌手又称主动 (active) 攻击者. 方案通常优先考虑在恶意敌手存在情况下的安全性, 因为它确保任何敌手攻击都不会成功. 然而, 能够实现这种安全级别的协议通常效率较低. 在这种敌手模型中, 恶意敌手可以在协议执行期间采取任意行动, 被腐化的参与方需根据敌手的指示任意偏离协议规范.

除上述经典的敌手模型, 还存在一种中间的敌手模型. 原因在于, 半诚实敌手模型通常过于薄弱, 而能够在面对恶意敌手时提供安全性的协议可能效率太低. 一种中间的敌手模型是隐蔽 (covert) 敌手模型. 简单来讲, 这

种敌手也可能会表现出恶意行为, 然而在隐蔽敌手模型中, 敌手的恶意行为会以某种给定的概率被诚实的参与方发现.

(3) **复杂度**: 考虑两类敌手的假定计算复杂度.

- 概率多项式时间 (PPT) 敌手: 此类敌手被限制在 (期望) 多项式时间内运行, 并可使用随机性. 根据建模方式的不同, 敌手可以是一致的 (即由概率多项式时间图灵机表示), 或非一致的 (即由多项式规模的电路族表示).
- 计算上不受限制 (computationally unbounded) 的敌手: 敌手没有任何计算限制.

3　国内外研究现状

门限签名方案受到各国政界、学界和业界的关注. 近 5 年, 在如 CRYPTO, CCS 和 NDSS 等密码与安全会议中, 分布式签名及其应用研究的工作占据了相当大的比重. 本文分别针对分布式密钥生成 DKG、门限 ECDSA/SM2、门限 Schnorr/EdDSA 和格密码门限签名 4 个方面, 从优化通讯开销、降低交互轮次、优化鲁棒性、实现主动安全等角度, 对国内外相关研究成果进行分析和总结.

3.1　基于秘密共享的分布式密钥生成研究现状

秘密共享 (secret sharing, SS) 及其衍生技术主要通过将秘密进行分割的方式实现秘密去中心化, 如高安全鲁棒性的前摄性秘密共享 (proactive SS, PSS)、可验证秘密共享 (verifiable SS, VSS) 和公开可验证秘密共享 (public VSS, PVSS) 等 [7], 能够有效防止单点故障, 规避密钥托管失控的潜在风险, 提高分布式系统的容错性. 同时, 该类技术是实现门限密码学和分布式密钥生成等技术的主要手段, 在门限签名中有重要应用 [1,8], 可为各签名参与方提供联合公钥 (验证密钥) 和签名私钥. 此外, 密码学协议通常需假定初始设置可信, 并通过可信第三方为所有的参与方生成密钥, 其安全性取决于第三方是否有保护这些密钥安全的意愿和能力. 然而, 现有密钥生成方案多依靠单一可信机构, 存在单点失败的潜在风险. 为摆脱中心化可信初始设置的束缚, 秘密共享协议和基于秘密共享的 DKG 协议已成为去中心化的关键技术手段, 并逐步在安全多方计算和分布式签名中得到广泛应用 [9~11]. 依据初始设置的不同, 将分布式协议分为可信初始设置和透明式初始设置 (transparent setup) 两类, 其中, 可信初始设置包括依赖于可信第三方或基于 DKG 协议的分布式初始设置, 生成含有秘密陷门 (如私钥) 的公共参数 (如公钥); 透明式初始设置通过提供一个不包含任何秘密或陷门信息的公共参数实现去可信化, 如通用字符串 (common reference string, CRS) [11]. 透明式初始设置具备可重用友好等优点, 每当参与方新加入协议或被替换时, 无需重新执行可信初始设置生成相应的参数, 可减少计算与通讯资源浪费. 此外, DKG 协议的属性可细分为可识别中止性、鲁棒性、自适应安全性等. Katz [12] 提出了轮次最优的鲁棒 DKG 协议, 包括在随机预言机模型 (random oracle model, ROM) 下 1 轮预处理外加 2 轮在线交互, 以及在 CRS 模型下 2 轮预处理外加 1 轮在线交互. Zhang 等人 [13] 讨论了异步网络模型下的 DKG 方案. 此外, 基于格上密码的 DKG 方案 [14,15] 以及结合应用于门限签名的方案也相继提出 [11,16,17]. 几种典型 DKG 协议的对比如表 1 [9~11,18] 所示. 其中, κ 为安全参数, n 为参与方数, t 为最多容忍失败方参与数, Δ 表示同/异步网络通信轮次. VUF 为可验证不可预测函数 (verifiable unpredictable function), DL 为离散对数假设 (discrete logarithm assumption), SXDH 为对称外部 Diffie-Hellman 假设 (symmetric external Diffie-Hellman assumption), BDH 为双线性 Diffie-Hellman 假设 (bilinear Diffie-Hellman assumption).

3.2　门限 ECDSA 签名方案研究现状

Gennaro 等人 [19] 提出了对 DSS (digital signature standard) 的门限化方案, 同样地, 门限 ECDSA 签名的本质是多方协同计算 $\pi = k^{-1} \cdot (H(\mathsf{msg}) + r \cdot x) \bmod p$, 其中 $r = g^k \bmod p$ 为随机挑战, 随机数 k 与私钥 x 由多个参与方份额聚合而成. 其研究可溯源到 MacKenzie 和 Reiter [20] 构造的两方 ECDSA 签名方案, 各参与方为了隐私地计算本地私钥 sk 与对方随机数 k (或本地随机数与对方私钥) 的乘法运算, 除秘密共享外, 还需要利用同态加密技术执行隐私乘法或乘法转加法 (multiplicative-to-additive, MtA) 运算, 导致交互轮次高和通讯开销大的

表 1　分布式密钥生成协议对比.

Table 1　Comparison of distributed key generation protocols.

Scheme	Trusted setup	Network	Resilience	Communication	Latency	Assumption	Primitives
Gennaro et al. [10]	No	Sync	$\frac{1}{2}$	$\mathcal{O}(\kappa \cdot n)$	$\mathcal{O}(t\Delta)$	DL	VSS
Gurkan et al. [11]	No	Sync	$\log n$	$\mathcal{O}(\kappa \cdot n^3 \log n)$	$\mathcal{O}(t\Delta)$	SXDH+BDH	PVSS+VUF
Shrestha et al. [18]	No	Sync	$\frac{1}{2}$	$\mathcal{O}(\kappa \cdot n^3)$	$\mathcal{O}(t) - \mathcal{O}(t\Delta)$	DL	VSS
Kokoris-Kogias et al. [9]	No	Async	$\frac{1}{3}$	$\mathcal{O}(t)$	$\mathcal{O}(t)$	DL	VSS

问题. 此外, 门限 ECDSA 签名的证据 π 需依赖随机数的逆 (即 k^{-1}, $\pi = k^{-1} \cdot (H(\mathsf{msg}) + r \cdot x) \bmod p$) 来计算, 一旦给定密钥 k 的份额 k_1 和 k_2, 计算 k_1' 和 k_2' 满足 $k_1' + k_2' = k^{-1} \bmod q$ 是困难的. 值得说明的是, SM2 [21] 和 ECDSA 等国际标准签名算法受限于底层的非线性结构, 在门限化构造过程中, 同样存在着求逆和求乘积的困难. 因此, 克服门限 ECDSA 和 SM2 签名中计算随机数逆的困难和优化计算/通讯开销是推动门限 ECDSA 和 SM2 应用的关键.

3.2.1　低交互开销的门限 ECDSA 签名

Gennaro 等人 [22] 基于 MacKenzie-Reiter 方案 [20] 的思想, 在半诚实模型下给出基于 Paillier 同态加密的 6 轮次 n 选 t 门限 ECDSA 签名. 为抵抗恶意敌手并降低通讯开销, Gennaro 和 Goldfeder [23] 在密钥生成阶段, 遵循 CDN (Cramer-Damgård-Nielsen) 范式 [24] 通过 Feldman-VSS 技术实现无可信中心 (透明化初始设置) 的多秘密共享分发; 在签名阶段, 借鉴 SPDZ 范式 [25] 和 Beaver-Triple 技术实现安全多方计算的方法, 将两方计算的乘法秘密份额转变为同一秘密的加法份额, 并将其拓展到多方的 ECDSA 签名. 然而, 由于 ECDSA 签名是在模 q 空间完成, 而 Paillier 同态加密是在模 N^2 ($N = p \cdot q$) 空间, 因此, 需借助范围证明来限制敌手的行为以避免密钥提取等攻击, 但范围证明则进一步增大通讯开销. 为降低通讯开销并减少交互轮次, 通常从优化 MtA 协议或隐私乘法运算入手, 通过减少其使用频率或避免使用范围证明的方式来控制开销, 可概括为以下 3 条技术思路: 思路一是通过 Diffie-Hellman 密钥交换技术协商随机数以减少隐私乘法数量 [26]; 思路二是遴选支持在模 q 上的同态运算以替换 Paillier 同态加密, 如, Lindell [27] 选用的指数 ElGamal 加密、Castagnos 等人用于两方 [28] 和多方场景 [29] 的 Castagnos-Laguillaumie 加密以及 Xue 等人 [30] 选用的 Joye-Libert 加密; 思路三是将签名阶段细分为离线预处理和在线签名两个阶段, 在离线预处理阶段, 预先处理开销负载大的计算, 从而减少在线阶段的交互轮次和开销, 如, Doerner 等人 [31] 和 Xue 等人 [32] 使用的不经意传输 (oblivious transfer)、Doerner 等人 [33] 使用的不经意线性计算 (oblivious linear evaluation, OLE) 以及伪随机关联生成器 (pseudorandom correlation generator, PCG) 等. 此外, 为降低计算开销, 在两方协作的 SM2 签名中, 文献 [34~36] 均围绕减少交互轮次和优化协作签名效率等方面进行了有效的优化提升. 在最新的工作中, 利用类群上 CL 加密方案的证明友好结构, 门限 ECDSA 的方案的交互轮次已经降低到两轮 [37,38]. 上述方案的对比具体如表 2 [6,22,23,29,33,37~41] 所示. 其中, P2P 代表点到点信道; BC 代表广播信道; t 为门限值, n 为参与方数量. sRSA 为强 RSA 假设 (strong RSA assumption), DCR 为合数剩余判定假设 (decisional composite residuosity assumption), DDH 为判定型 Diffie-Hellman 假设 (decisional Diffie-Hellman assumption), CDH 为计算型 Diffie-Hellman 假设 (computational Diffie-Hellman assumption), SR 为强根假设 (strong root assumption), LO 为低阶元素假设 (low order assumption), HSM 为困难子群假设 (hard subgroup membership assumption), ARSA 为自适应根子群假设 (adaptive root subgroup assumption).

3.2.2　具有鲁棒性的门限 ECDSA 签名

复杂网络环境中恶意攻击的日益猖獗, 具有可识别中止性的安全多方计算方案已无法满足应用需求, 如何构造可抵抗恶意干扰并具有鲁棒性的门限 ECDSA 签名愈发受到关注. 具有鲁棒性的门限签名其基本要求之一便是无论是否存在作弊行为, 诚实参与方总能最终生成签名. 鲁棒性通常可以通过在签名失败后引入新的参与

表 2　门限 ECDSA 签名对比.

Table 2　Comparison of threshold ECDSA signature.

Scheme	Channel	Identifiable abort	Threshold	Rounds	Communication	Computation	Assumption
Gennaro et al. [22]	BC	No	$t<n$	6	$\mathcal{O}(n)$	$\mathcal{O}(n)$	sRSA, DCR
Boneh et al. [39]	BC	No	$t<n$	4	$\mathcal{O}(n)$	$\mathcal{O}(n)$	sRSA
Gennaro et al. [23]	P2P&BC	No	$t<n$	8	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	sRSA, DCR, DDH
Doerner et al. [40]	P2P&BC	No	$t<n$	$\lceil\log t\rceil+6$	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	CDH
Canetti et al. [41]	P2P	Yes	$t<n$	4 or 7	$\mathcal{O}(n^3)$	$\mathcal{O}(n^3)$	sRSA, DCR, DDH
Castagnos et al. [29]	P2P	No	$t<n$	8	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	SR, LO, HSM, DDH
Doerner et al. [33]	P2P	No	$t<n$	3	$\mathcal{O}(n^2)$	$\mathcal{O}(n^2)$	CDH
Wong et al. [6]	P2P	Yes	$t<n$	5	$\mathcal{O}(n^2)$	$\mathcal{O}(n)$	SR, LO, HSM, DDH
Dahari-Garbian et al. [37]	BC	Yes	$t<n$	2	$\mathcal{O}(n)$	$\mathcal{O}(n)$	HSM, ARSA
Lyu et al. [38]	P2P	No	$t<n$	2	$\mathcal{O}(n)$	$\mathcal{O}(n)$	SR, LO, HSM

方来替换已识别的恶意参与方并重启协议来实现. 此外, 各类具有新型态鲁棒性的门限签名方案也逐步受到关注, 如具备可自愈性 (self-healing) 的方案 [6] 中, 在部分密钥份额丢失后, 诚实参与方可使用其密钥份额和公开信息来合作恢复该部分密钥, 而不需要重置密钥的生成与分配.

此外, 抵抗恶意敌手的主动 (active) 安全门限方案是 NIST 征集的主要目标之一. 主动安全意味着敌手可以主动地收买并完全控制被收买的参与方, 主动安全的敌手可以是静态的、移动的和自适应的, 主动且静态的敌手通常指恶意敌手, 主动且自适应的敌手简称为自适应敌手, 在参与方动态变化的环境下, 自适应敌手称为移动敌手. 为实现主动安全, Dalskov 等人 [42] 和 Smart 等人 [43] 利用 SPDZ-MAC 等信息论安全工具讨论了其可行性. 为抵抗移动敌手收买, Canetti 等人 [41] 和 Castagnos 等人 [29] 分别讨论了保持秘密不变而支持秘密份额定期刷新的前摄性自适应安全方案. 显然, 如何提升鲁棒性与安全性也是门限签名方案所关注的焦点问题.

3.3　门限 Schnorr 签名方案研究现状

参考 NIST 针对门限 Schnorr 方案的征集需求, 优化交互轮次、降低在线通讯开销并实现自适应安全是门限签名研究的主要目标. Schnorr 签名来源于 Schnorr 识别协议, 因其私钥 x 和随机数 k 是以线性等式 (如 $\pi=k-e\cdot x \bmod p$) 的方式使用, 容易以分布式方式实现. 门限 Schnorr 签名通常遵循 3 轮次构造范式 [10], 首先参与方对同一随机数达成共识, 随后各自在本地计算并生成签名的份额. EdDSA 签名是 Schnorr 方案的变种, 通常归类讨论 [44,45]. 自 NIST 和 IETF 推进门限 Schnorr/EdDSA 签名的标准化工作以来 [3,4], 低延迟的 FROST [46] 和 FROST2 [47]、异步环境下的 ROAST [48] 和 SPRINT [49] 以及高鲁棒性的 OLAF [50] 等方案相继提出. 在最新的工作中, Bacho 等人提出了标准假设下自适应安全的门限 Schnorr 方案 Glacius [51] 及其轮次优化的版本 Gargos [52], Cho 等人 [53] 也首次给出了 Schnorr 签名在 ROM 下的紧安全性证明. 上述方案的具体对比如表 3 [46,47,51~57] 所示. 其中, t 为门限值, n 为参与方数量. PRF 为伪随机生成函数 (pseudorandom function), OT 为不经意传输 (oblivious transfer), OMDL 为多一离散对数假设 (one-more discrete logarithm assumption), AOMDL 为代数型多一离散对数假设 (algebraic OMDL assumption), CDL 为循环离散对数假设 (circular discrete logarithm assumption).

3.3.1　具有鲁棒性的低交互门限 Schnorr 签名

围绕实现低交互门限 Schnorr 签名的目标, 当前工作聚焦于将交互轮次由 3 轮次降为 2 轮次并提高通讯吞吐量, 同时将签名过程细分为离线和在线两个阶段, 离线阶段用于高开销高延迟的预签名, 在线阶段用于低开销低延迟的签名生成. 为约减交互轮次, Chen 等人 [58] 较早讨论了离线和在线设置的门限签名. Komlo 和 Goldberg [46] 提出名为 FROST 的门限 Schnorr 签名, 包括一个交互式方案和一个非交互式方案, 其中非交互式 FROST 签名支持签名者以异步的方式完成签名, 包括 1 轮次预处理阶段和 1 轮次签名阶段. 与此同时, Bellare 等人 [47] 在

表 3　门限 Schnorr 签名对比.

Table 3　Comparison of threshold Schnorr signature.

Scheme	Rounds	Threshold	Security	Identifiable abort	Assumption
Komlo et al. [46]	2	$t < n$	Semi-honest	No	OMDL
Bellare et al. [47]	2	$t < n$	Malicious	No	OMDL
Crites et al. [54]	3	$t < n$	Malicious	Yes	DL
Crites et al. [54]	3	$\frac{t}{2} < n$	Malicious (adaptive)	Yes	AOMDL, DL
Lindell et al. [55]	3	$t < n$	Malicious	Yes	RO
Garillot et al. [56]	3	$t = 1, n = 2$	Malicious	No	RO, PRF
Kondi et al. [57]	2	$t = 1, n = 2$	Covert	No	OT, PRF
Kondi et al. [57]	2	$t = 1, n = 2$	Malicious	No	RO, DCR, sRSA
Bacho et al. [51]	5	$t < n$	Malicious (adaptive)	Yes	DL, DDH
Bacho et al. [52]	3	$t < n$	Malicious (adaptive)	Yes	DL, DDH
Cho et al. [53]	2	$t = 1, n = 2$	Malicious	No	CDL

CRYPTO'22 上整合 FROST2-CKM 和 FROST2-BTZ 两个方案, 分别基于 OMDL 假设给出具有强不可伪造性的 2 轮次门限 Schnorr 方案, 以及在可编程随机预言机 (programmable random oracle model, PROM) 模型下基于离散对数假设的 3 轮次门限 Schnorr 签名 (SimpleTSig). 为降低通讯开销, FROST2-CKM 方案更是将签名阶段的标量乘法运算从线性复杂度降低到了仅 1 个标量乘法. FROST 能够识别恶意签名者并中止协议 (可识别中止性), 但无法阻止被收买的参与方任意生成签名, 即无法提供鲁棒性. 现有工作多通过替换被识别的恶意参与方并重启协议的方式来实现鲁棒性, 但需要在同步网络环境下重复执行 FROST. 为了在异步通讯网络环境下实现鲁棒性, Ruffing 等人 [48] 提出的 ROAST (即 FROST3) 方案本质是在 FROST 方案基础上, 同步执行 C_t^n 个 FROST 会话, 并确保每个会话中超过阈值数目的签名者组成一个子集, 同时通过在协议广播前先聚合协议消息的方式来降低预处理阶段的通信开销, 但其安全性规约到 FROST2-BTZ 方案的不可伪造性, 则需要依赖代数群模型 (algebraic group model, AGM) 下的可信密钥生成, 但该工作未提供形式化证明和分析. 在异步网络环境下, 为同时兼顾门限签名方案的安全性和鲁棒性, SPRINT 方案 [49] 在 FROST 的基础上引入批量随机数提取技术来优化预签名协议, 从而提高吞吐量. OLAF 方案 [50] 则在 ROAST 方案基础上, 绕过理想化密钥生成, 引入优化后 Pedersen-DKG, 提供对秘密份额的持有性证明, 从而在 ROM 模型下实现不可伪造性, 且不再依赖 AGM 模型.

3.3.2　自适应安全门限 Schnorr/EdDSA 签名

FROST 和 ROAST 等先期工作仅考虑单机或静态敌手模型下的鲁棒性, 对更高层级安全性 (如, 安全模型、自适应安全性和可组合安全性) 的讨论则浅尝辄止. Lindell [55] 提出一个在 PROM 模型下基于离散对数假设的 3 轮次门限 Schnorr 签名, 并在通用可组合模型下对静态敌手和并发敌手进行讨论, 但该方案需依赖 Fischlin 转换. SimpleTSig [47] 则通过引入具有秘密份额持有性证明的 Pedersen DKG 来绕开 Fischlin 证明转换技术. Crites 等人 [54] 在 CRYPTO'23 会议上提出的门限 Schnorr 签名方案 Sparkle, 不需要在线可提取零知识证明技术, 有效简化了方案设计并提升方案效率, 并以此讨论了 3 种情形: 在 ROM 模型下基于离散对数假设实现静态安全、在 ROM 模型下基于弱 OMDL 假设实现自适应安全以及在 AGM 模型下基于弱 OMDL 假设实现门限为 t 的完全自适应安全. Makriyannis [59] 则证明了 3 轮次的分布式 Schnorr 签名可实现完全自适应的通用可组合安全并具备紧致安全性.

3.4　格密码门限签名方案研究现状

随着 NIST 后量子密码标准算法的公布及战略部署, 基于格密码假设开展后量子签名的研究如火如荼, 主要集中在基于格的签名以及门限签名、盲签名、门限盲签名等应用性较强的特种签名. 目前, 基于格密码假设的签名构造路线有两种: 一种是遵循 Hash-and-Sign 范式, 采用 Micciancio 和 Peikert 提出的格上原像采样技术来生

成签名; 另一种则是采用 Lyubashevsky 提出的基于格上 Schnorr 协议和 Fiat-Shamir 转换技术来生成签名. 遵循第一条技术路线, Bendlin 等人 [15] 构造分布式格签名, 为 Micciancio-Peikert 方案设计了相应的 DKG 协议和分布式签名协议, 但仍需引入一个可信领导者来负责秘密的分发与聚合. 此外, 该方案的 DKG 协议采用 Shamir 的秘密共享技术, 其通讯开销和参数过大以至于最终的签名规模较大. 因此, 遵循第 2 种技术路线的分布式格签名是当前学界主要研究方向. 其中, 代表性的工作之一是 Boneh 等人 [14] 将全同态加密方案 [60] 优化设计成一个通用门限工具, 用于 Lyubashevsky 签名方案得到一个 1 轮次门限签名方案. 随后, 优化签名大小的方案相继提出 [61], 但上述方案是以增加通讯轮次或通讯开销为代价, 而实际应用中带宽的费用往往高于计算费用. del Pino 等人 [62] 提出一个实用的门限格基签名 TRaccoon, 但仅实现了被动安全, 不具有鲁棒性与可识别中止性等属性. 针对签名授权电子交易的场景, 为避免托管密钥服务器单点故障, Dutta 等人 [63] 委托多服务器执行门限签名, 并与客户端通过低熵口令建立会话密钥以确保私钥份额传输的机密性, 再利用全同态加密构造口令认证密钥交换, 并应用于口令保护门限签名方案, 但并未给出具体实例化构造. 而在最新的研究中, Pino 等人 [64] 提出了一种基于拒绝采样的紧凑型格门限签名方案, 成功实现了在无需多方安全计算或全同态加密的情况下构造高效的 t-out-of-n 格门限签名. 该方案引入了复制秘密共享 (replicated secret sharing) 机制来分发密钥, 与传统的 Shamir 秘密共享不同, 其生成的私钥份额具有较小的范数, 能够直接在每个签名份额上执行拒绝采样, 从而显著减少签名尺寸和通信开销. 然而, 由于其设计在计算与参数规模上针对小规模协作者进行了优化, 目前该方案主要适用于参与方数量较少的门限设置.

4　部分代表性门限签名的构造思路

当前, 门限签名的构造通常沿用基于门限密码的安全多方计算范式 (简称 CDN 范式), 结合分布式密钥生成 (DKG) 技术和椭圆曲线综合加密机制 (elliptic curve integrated encryption scheme, ECIES), 在原 ECDSA/SM2/Schnorr/EdDSA 等签名的基础上, 各参与方使用各自的私钥进行分布式的签名, 并最终借助拉格朗日插值多项式, 聚合生成最终的签名结果.

4.1　分布式密钥生成

Gennaro 等人 [10] 的方案基于 Pedersen-VSS 方案构造, 在承诺阶段使用信息论安全的可验证秘密共享方案来对多项式进行承诺, 这样秘密 x 的值就会被确定并且之后也不可被更改, 同时保证生成密钥的均匀分布. 如下分别给出私钥生成阶段和公钥生成两个阶段的描述.

(1) 私钥生成.

- 每个参与者 P_i 会作为分发者通过运行 Pedersen-VSS 来分发一个随机值 z_i.

– P_i 选择两个阶数为 t 的随机多项式 $f_i(z)$ 和 $f_i'(z)$: $f_i(z)=a_{i0}+a_{i1}z+\cdots+a_{it}z^t$, $f_i'(z)=b_{i0}+b_{i1}z+\cdots+b_{it}z^t$, 令 $z_i=a_{i0}=f_i(0)$, 计算并广播 $C_{ik}=g^{a_{ik}}h^{b_{ik}} \bmod p$, 其中 $k=0,\ldots,t$. 然后计算 $s_{ij}=f_i(j), s_{ij}'=f_i'(j) \bmod q$, 其中 $j=1,\ldots,n$. 最后将 $s_{ij}=f_i(j)$ 和 $s_{ij}'=f_i'(j)$ 发送给 P_j.

– 每个参与者 P_j 验证从其他参与者 $P_{i,i\neq j}$ 接收到的份额, 检查等式 (1) 是否成立

$$g^{s_{ij}}h^{s_{ij}'}=\prod_{k=0}^{t}(C_{ik})^{j^k} \bmod p. \tag{1}$$

若某个索引 i 对应的验证不通过, 那么 P_j 广播对 P_i 投诉.

– 作为分发者的参与者 P_i 接收到 P_j 的投诉后, 广播满足等式 (1) 的值 s_{ij} 和 s_{ij}'. 如果收到超过 t 个投诉, 或在回答投诉的值 s_{ij} 和 s_{ij}' 不满足等式 (1), 则各方将该参与者标记为不合格.

- 每个参与者构建合格参与者的集合 QUAL, 并且所有诚实的参与方构建相同的集合.
- 分布式的秘密值 x 不会由任何一方显式的计算, 但是它满足 $x=\Sigma_{i\in\mathrm{QUAL}}z_i \bmod q$, 每一个 P_i 将自己的秘密份额设置为 $x_i=\sum_{j\in\mathrm{QUAL}}s_{ji} \bmod q$ 和 $x_i'=\sum_{j\in\mathrm{QUAL}}s_{ji}' \bmod q$.

(2) 公钥生成 $y = g^x \bmod q$.

- 每个属于 QUAL 的参与者 P_i 通过 Feldman-VSS 打开 $y_i = g^{z_i} \bmod q$.
  - 每个属于 QUAL 的参与者 P_i 计算并广播 $A_{ik} = g^{a_{ik}} \bmod p$, 其中 $k = 0, \ldots, t$.
  - 每个参与者 P_j 验证其他参与者 $P_{i,i\neq j}$ 广播的值, 检查等式 (2) 是否成立

$$g^{s_{ij}} = \prod_{k=0}^{t} (A_{ik})^{j^k} \bmod p. \tag{2}$$

若某个索引 i 的验证失败, P_j 通过广播满足等式 (1) 但不满足等式 (2) 的值 s_{ij} 和 s'_{ij} 来投诉 P_i.

– 对于收到至少一个有效投诉的 P_i, 其他各方运行 Pedersen-VSS 的重建阶段来计算 $z_i, f_i(z)$ 和 A_{ik}, 其中 $k = 0, \ldots, t$. QUAL 中的每个参与者令 $y_i = A_{i0} = g^{z_i} \bmod q$, 然后计算 $y = \prod_{i\in \mathrm{QUAL}} y_i \bmod p$.

4.2　门限 ECDSA 签名

本小节通过 1996 年的 Gennaro-Jarecki-Krawczyk-Rabin (简称 GJKR) 和 2018 年的 Gennaro-Goldfeder 两个方案, 分别展示经典门限 ECDSA 签名构造过程中的技术思路.

GJKR 门限签名方案 (EUROCRYPT'96). Gennaro 等人 [19] 基于 DSA 或 DSS 构造了门限签名方案 (简称 GJKR 方案). 方案使用 DKG 方案来生成公私钥, 并通过计算随机数的逆来生成签名, 签名过程简述如下.

- 每个参与方 P_i 选择随机值 $u_i \in \mathbb{Z}_q$ 和一个 t 阶多项式运行 Joint-Uncond-Secure-RSS 得到秘密份额 k_i, 其中 $(k_1, \ldots, k_n) \xleftarrow{(t,n)} k \bmod q$, k 为聚合后的秘密值.

- 每个参与方 P_i 生成两个常数项为 0 阶为 $2t$ 的随机多项式, 然后运行两次 Joint-Zero-SS. 最终每个参与方 P_i 持有份额 (b_i, c_i).

- 每个参与方 P_i 选择随机值 $v_i \in \mathbb{Z}_q$ 和一个 t 阶多项式运行 Joint-Feldman-RSS 得到秘密份额 a_i, 计算并广播 $v_i = k_i \cdot a_i + b_i \bmod q$ 和 $w_i = g^{a_i}$. 如果参与方 P_j 未参与广播, 设置 v_j 值为 0. 每个参与方 P_i 对 $(v_i, \ldots, v_n)$ 进行插值得到中间值 $\mu = k \cdot a$. 对 $(w_i, \ldots, w_n)$ 在指数上进行插值得到中间值 g^a, 计算获得随机信标值 $r = (g^a)^{\mu^{-1}} \bmod q$.

- 每个参与方 P_i 计算并广播 $s_i = k_i(H(m) + x_i r) + c_i \bmod q$, 如果参与方 P_j 未参与广播, 设置 s_j 值为 0, 然后 P_i 对 $(s_1, \ldots, s_n)$ 进行插值得到 $s = k(H(m) + xr) \bmod q$, 输出 (r, s) 作为 m 的签名.

Gennaro-Goldfeder 门限签名方案 (CCS'18). 以 Gennaro 和 Goldfeder 两人的门限 ECDSA 签名方案 [23] 为例, 展示一种具有低交互开销的门限 ECDSA 签名方案的典型结构. 下面主要介绍密钥生成算法 KeyGen 和签名算法 TSign [23], 并简要说明其中使用的非交互零知识 (non-interactive zero-knowledge, NIZK) 证明机制. 为简化描述, 以下省略模运算的具体细节.

(1) 非交互零知识 (NIZK). 在 RO/CRS 模型下, NIZK 允许证明者在无需交互的情况下向验证者证明其拥有某个秘密 (knowledge of a witness), 且不泄露该秘密本身. 在本方案中, NIZK 主要用于: (i) 对承诺的离散对数给出知识证明 (如证明 $\Gamma_i = g^{\gamma_i}$ 的正确性, Schnorr Σ 协议经 Fiat-Shamir 非交互化); (ii) 对 Paillier 密文给出明文知识证明与范围证明, 确保参与 MtA/MtAwc 的输入落在合法区间; (iii) 证明与 Paillier 公钥关联的模数为无平方因子 RSA 模. 上述论证共同保证密钥生成与签名阶段中承诺与响应值的一致性与合规性, 从而防止 "流氓密钥" 与由越界输入引发的伪造/操纵风险.

(2) 密钥生成算法 KeyGen.

- 每个参与方 P_i 随机选取 $u_i \in_R \mathbb{Z}_q$, 计算并广播一个对 g^{u_i} 的承诺, 同时广播其 Paillier 加密的公钥 E_i.

- 每个参与方 P_i 广播打开对 g^{u_i} 的承诺, 令 $y_i = g^{u_i}$, 可计算出签名的公钥为 $y = \prod_i y_i$. 然后 P_i 对其 u_i 执行 (t, n) Feldman-VSS 协议, 计算得到自己的秘密份额 x_i,x_i 是密钥 $x = \Sigma_i u_i$ 的 (t, n) Shamir 秘密共享份额. 最后公开 $X_i = g^{x_i}$.

- 令 $N_i = p_i q_i$ 作为与 E_i 相关的 RSA 模值, P_i 使用 Schnorr-Sigma 协议 [65] 证明它知道 x_i, 使用 Gennaro 等人 [66] 的方式证明 N_i 是一个无平方因子数.

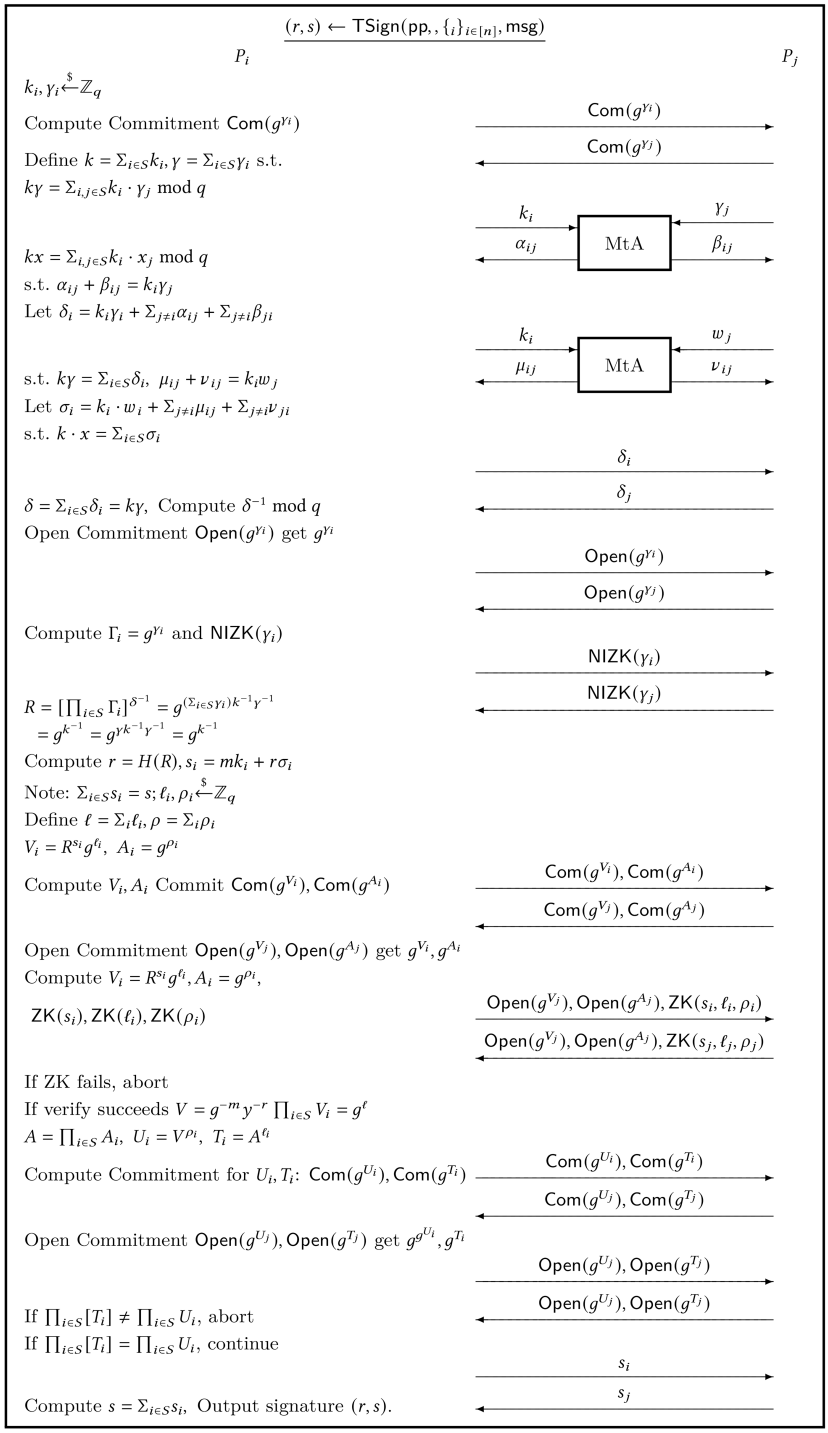

图 1　门限 ECDSA 分布式签名阶段.

Figure 1　The distributed signing phase of threshold ECDSA.

(3) 签名算法 TSign. 签名阶段交互过程的如图 1 所示, 其中使用了 MtA 操作, 该操作允许分别拥有秘密 $a_i \in \mathbb{Z}_q$ 和 $b_i \in \mathbb{Z}_q$ (满足 $x = a_i \cdot b_j$) 的参与方 P_i 和 P_j, 在不暴露各自输入的前提下, 将 x 的乘法份额 a_i 和 b_i 转换为加法份额 α_i 和 β_j, 使得 $x = \alpha_i + \beta_j$. Gennaro 和 Goldfeder 方案对上述协议引入可验证性, 称之为 MtAwc (MtA with check), 它与 MtA 协议的区别仅在于: 如果 $B_j = g^{b_j}$ 是一个公开值 (其中 g 是一个素数 q 阶循环群的生成元), 则参与方 P_j 在零知识中额外证明 b_j 是 B_j 的离散对数. 此外, 为不失一般性, 用 $m = \mathsf{H}(\mathsf{msg})$ 表示

对消息 msg 进行哈希, 并令参与签名算法的参与方集合 S 大小为 t, 因此在签名算法中只需要使用 (t,t) 秘密共享方案, 而不用使用 (t,n) 形式的构造, 签名过程中的参与方均来自集合 S. 使用合适的拉格朗日系数 $\lambda_{i,S}$, 每个参与签名的参与方可以在本地将秘密 x 的 (t,n) 形式的秘密共享份额 x_i 转换为 x 的 (t,t) 形式的秘密共享份额, 表示为 $w_i=(\lambda_{i,S})(x_i)$, 满足 $x=\Sigma_{i\in S}w_i$. 因为 $X_i=g^{x_i}$ 和 $\lambda_{i,S}$ 是公开值, 所以每个参与方都能够计算 $W_i=g^{w_i}=X_i^{\lambda_{i,S}}$.

• 每个参与方 P_i 选取 $k_i,\gamma_i\in_R\mathbb{Z}_q$, 计算并广播 g^{γ_i} 的承诺. 令 $k=\Sigma_{i\in S}k_i,\gamma=\Sigma_{i\in S}\gamma_i$, 其值满足 $k\gamma=\Sigma_{i,j\in S}k_i\gamma_j$, $kx=\Sigma_{i,j\in S}k_ix_j$.

• 所有参与方两两之间执行 MtA 和 MtAwc 子协议. 参与方 P_i 与 P_j 执行如下: (1) 分别使用 k_i 和 γ_j 运行 MtA 子协议分别得到 α_{ij} 和 β_{ij}; (2) 分别使用 k_i 和 w_j 运行 MtAwc 子协议分别得到 μ_{ij} 和 ν_{ij}, 其值满足 $k_i\gamma_j=\alpha_{ij}+\beta_{ij}$, $k_iw_j=\mu_{ij}+\nu_{ij}$. 在与其他所有参与方的子协议交互都完成后, P_i 计算得到 $\delta_i=k_i\gamma_i+\Sigma_{j\neq i}\alpha_{ij}+\Sigma_{j\neq i}\beta_{ji}$, $\sigma_i=k_iw_i+\Sigma_{j\neq i}\mu_{ij}+\Sigma_{j\neq i}\nu_{ji}$, 其值满足 $k\gamma=\Sigma_{i\in S}\delta_i$, $kx=\Sigma_{i\in S}\sigma_i$.

• 每个参与方 P_i 广播 δ_i, 然后可计算得到 $\delta=\Sigma_{i\in S}\delta_i=k\gamma$ 和 δ^{-1}.

• 每个参与方 P_i 广播打开对 g^{γ_i} 的承诺, 令 $\Gamma_i=g^{\gamma_i}$, 同时使用 Schnorr-Sigma 协议 [65] 证明它知道满足 $\Gamma_i=g^{\gamma_i}$ 的 γ_i. 然后 P_i 计算 $R=[\prod_{i\in S}\Gamma_i]^{\delta^{-1}}=g^{(\Sigma_{i\in S}\gamma_i)k^{-1}\gamma^{-1}}=g^{k^{-1}}$ 和 $r=\mathsf{H}(R)$.

• 每个参与方 P_i 计算 $s_i=mk_i+r\sigma_i$, 其值满足 $s=\Sigma_{i\in S}s_i$. 然后 P_i 选取 $\ell_i,\rho_i\in_R\mathbb{Z}_q$, 令 $\ell=\Sigma_i\ell_i$, $\rho=\Sigma_i\rho_i$, 计算 $V_i=R^{s_i}g^{\ell_i}$, $A_i=g^{\rho_i}$, 计算并广播对 (V_i,A_i) 的承诺.

• 每个参与方 P_i 广播打开对 (V_i,A_i) 的承诺, 并使用零知识证明他知道满足 $V_i=R^{s_i}g^{\ell_i}$ 和 $A_i=g^{\rho_i}$ 的 s_i,ℓ_i,ρ_i. 如果零知识证明验证失败, 则协议中止, 否则令 $V=g^{-m}y^{-r}\prod_{i\in S}V_i=g^{\ell}$, $A=\prod_{i\in S}A_i$.

• 每个参与方 P_i 计算 $U_i=V^{\rho_i}$, $T_i=A^{\ell_i}$. 计算并广播对 (U_i,T_i) 的承诺.

• 每个参与方 P_i 广播打开对 (U_i,T_i) 的承诺, 若 $\prod_{i\in S}[T_i]\neq\prod_{i\in S}U_i$ 则协议中止.

• 每个参与方 P_i 广播 s_i, 计算 $s=\Sigma_{i\in S}s_i$. 若 (r,s) 不是一个有效的签名, 则中止协议, 否则接受签名并结束协议.

4.3　门限 Schnorr 签名

FROST 方案. 本小节着重通过 FROST 签名方案来展示门限 Schnorr 的构造思路, 并指出在构造过程中的难点与痛点. 作为经典的门限 Schnorr 签名构造方案, 其主要由 3 个算法 KeyGen, Preprocess(π) 和 Sign(m) 组成. 密钥生成算法 KeyGen 是 Pedersen-DKG 方案的变体, 该方案主要目的是生成一个阶为 $t-1$ 的随机多项式 $f(x)\in\mathbb{Z}_q[x]$ 和随机值 $s\in\mathbb{Z}_q$, 令 $f(0)=s$. 每个签名者 P_i 持有 s 的秘密份额 $s_i=f(i)$ 及对应的公钥 $Y_i=g^{s_i}$. 每当检测到错误结点时, FROST 协议会终止从而避免 rogue key 攻击 [67]. 在 KeyGen 算法中, 与 Pedersen-DKG 的不同之处在于会对 $a_{i0}=f_i(0)$ 进行知识的零知识证明. 由于此变动, 使得门限 t 的上界由 $\frac{n}{2}$ 提升到 n. KeyGen 算法完成后, 运行 Preprocess(π) 算法, 进入预处理阶段. 每个签名者 P_i 创建并发布 π 对承诺 $(D_{ij},E_{ij})=(g^{d_{ij}},g^{e_{ij}})$, 其中 $d_{ij},e_{ij}\in\mathbb{Z}_q^*$. 每次签名会调用一个承诺, 并将其从承诺列表中删除. 如果签名者需要签名一个新的消息但是没有可用的承诺值, 则重新运行该算法.

签名算法 Sign(m). m 表示待签名消息, 令 SA 表示签名聚合者 (其自身也可以是签名参与方之一), S 表示由 α ($t\leqslant\alpha\leqslant n$) 个被 SA 选中进行签名操作的参与者的集合, H_1 和 H_2 是输出值在 $\mathbb{Z}_q^*$ 中的哈希函数, $B=\langle(i,D_i,E_i)\rangle_{i\in S}$ 表示每个参与者 P_i 对应的参与方索引构成的有序列表, 其中 s_i 为 P_i 的秘密份额, L_i 是预处理阶段 P_i 发布的承诺值列表. 签名协议如下.

• SA 首先从 L_i 中获取每个参与方 $P_i\in S$ 的下一个可用承诺并构造有序列表 B, 然后将元组 (m,B) 发送给 $P_i\in S$.

• P_i 在接收到 (m,B) 后, 验证 m 和 B 中每个承诺的有效性, 如果存在无效值则终止协议.

• P_i 计算绑定值集合 $\rho_l=H_1(l,m,B)$, $l\in S$, 然后派生群体承诺 $R=\prod_{l\in S}D_l\cdot(E_l)^{\rho_l}$, 并计算挑战值 $c=H_2(R,Y,m)$. 随后, P_i 用其秘密份额 s_i 计算返回值 $z_i=d_i+(e_i\cdot\rho_i)+\lambda_i\cdot s_i\cdot c$, 用集合 S 确定对应拉格朗日系数 λ_i. P_i 从本地存储中安全的删除 $((d_i,D_i),(e_i,E_i))$, 并返回 z_i 给 SA.

• SA 完成以下步骤. (i) 计算 $\rho_i = H_1(i, m, B)$ 和 $R_i = D_{ij} \cdot (E_{ij})^{\rho_i}$, 随后计算 $R = \prod_{i \in S} R_i$ 和 $c = H_2(R, Y, m)$. (ii) 通过检查 $g^{z_i} \stackrel{?}{=} R_i \cdot Y_i^{c \cdot \lambda_i}$ 来验证返回值的有效性. 若等式不成立, 则识别并报告恶意行为的参与方, 终止协议. (iii) 计算群体返回值 $z = \Sigma z_i$ 并发布消息 m 及其签名值 $\sigma = (R, z)$.

4.4　门限 BLS 签名与可验证随机函数

门限 BLS 签名. BLS (Boneh-Lynn-Shacham) 门限签名是由 Boldyreva [68] 在 Boneh 等人 [69] 研究基础上提出的重要方案, 现已成为主流选择. 该方案的优势包括: 验证过程与非门限 BLS 签名完全一致、签名过程无需交互、签名结果唯一且体积小 (仅需单个椭圆曲线群元素), 同时在计算与通信效率方面表现优异. 这些特性使得 Boldyreva 的 BLS 门限签名方案在去中心化场景中得到了实际应用 [70,71]. 门限 BLS 签名依赖于 BLS 签名方案, 使用双线性配对 $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_{\mathrm{T}}$, 其中 $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_{\mathrm{T}}$ 是阶为素数 q 的循环群, g_0, g_1 分别是循环群 $\mathbb{G}_0, \mathbb{G}_1$ 是生成元, 使用一个哈希函数 H 将有限集合 $\mathcal{M}$ 的值映射到 $\mathbb{G}_0$ 中的元素. 不同的是, 门限 BLS 签名方案引入 Shamir 秘密分享 $(G_{\mathrm{sh}}, C_{\mathrm{sh}})$ 来进行签名密钥分割和部分签名生成, 其中签名生成过程并不需要单点重建私钥. 令 $\mathcal{S}$ 表示大小为 t 的签名者的集合, BLS 门限签名方案 $S_{\mathrm{thBLS}} = (\mathrm{KGen}, \mathsf{Sign}, \mathrm{Comb}, \mathrm{Vrfy})$ 计算如下.

• $\mathrm{KGen}(1^\lambda, n, t) \to (\mathsf{pk}, \mathsf{pkc}, \mathsf{sk}_1, \ldots, \mathsf{sk}_n)$:

– 密钥生成中心选择随机数 $\alpha \xleftarrow{R} \mathbb{Z}_q$ 并计算 $\mathsf{pk} \leftarrow g^\alpha$, 构造一个 $t-1$ 阶多项式 $\omega \in \mathbb{Z}_q[x]$, 令 $\omega(0) = \alpha$, 计算获得 n 个份额 $(\alpha_1, \ldots, \alpha_n) \xleftarrow{(t,n)} \alpha \pmod q$, 其中 $\omega(i) = \alpha_i$, $i = 1, \ldots, n$;

– 计算 $u_i \leftarrow g^{\alpha_i}$, 令 $\mathsf{sk}_i := \alpha_i$, $\mathsf{pk}_i := u_i$, $\mathsf{pkc} := \{\mathsf{pk}_1, \ldots, \mathsf{pk}_n\}$;

– 输出 $(\mathsf{pk}, \mathsf{pkc}, \mathsf{sk}_1, \ldots, \mathsf{sk}_n)$.

• $\mathsf{Sign}(\mathsf{sk}_i, m) \to \sigma_i'$: item 参与方 P_i 计算并广播签名份额 $\sigma_i' \leftarrow H(m)^{\mathsf{sk}_i}$.

• $\mathrm{Comb}(\mathsf{pkc}, m, \mathcal{S}, \{\sigma_j'\}_{j \in \mathcal{S}}) \to \sigma$:

– 参与方 P_i 首先验证其他 $t-1$ 个签名份额是否有效, 如果存在无效签名, 输出无效签名集合并终止协议;

– 然后计算签名 $\sigma \leftarrow \prod_{j \in \mathcal{S}} (\sigma_j')^{\lambda_j}$, 其中 λ_j 是参与方 P_j 对应的拉格朗日系数.

• $\mathrm{Vrfy}(\mathsf{pk}, m, \sigma)$: 输出 $\mathrm{Vrfy}_{\mathrm{BLS}}(\mathsf{pk}, m, \sigma)$.

门限 VRF. BLS 签名是一种特殊可验证随机函数 (verifiable random function, VRF). 下文将简述 Galindo 等人基于配对的 DVRF (简称 GLOW) 方案 [72], 该方案能同时实现强伪随机性与紧致的证明. 设 $(e, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, h_1, h_2)$ 为双线性配对, 其中 g_1, g_2 分别为 $\mathbb{G}_1, \mathbb{G}_2$ 的生成元 (h_1, h_2 同理). 定义哈希函数 $H_1 : \{0,1\}^* \mapsto \mathbb{G}_1$, $H_2 : \mathbb{G}_1 \mapsto \{0,1\}^{b(\lambda)}$ 及 $H_3 : \{0,1\}^* \mapsto \mathbb{Z}_q$. 令 $\mathrm{GLOW\text{-}DVRF} = (\mathrm{DistKG}, \mathrm{PEval}, \mathrm{Comb}, \mathrm{Vrfy})$ 为伪随机函数的分布式可验证方案, QUAL 表示有效节点的集合, 其构造如下.

• 密钥生成算法 $\mathrm{DistKG}(1^\lambda, t, \ell)$:

– 在生成阶段, 每个节点 P_i ($i \in \mathrm{QUAL}$) 通过 Feldman-VSS 协议计算并广播 $A_{i,k} = g_1^{a_{i,k}}$ $(0 \leqslant k \leqslant t)$ 及 $B_{i,0} = g_2^{a_{i,0}}$, $a_{i,k}$ 为 Feldman-VSS 中的多项式系数;

– 对于每个 $i \in \mathrm{QUAL}$, 节点 N_j 需验证等式 $g_1^{s_{i,j}} = \prod_{k=0}^{t} (A_{i,k})^{j^k}$ 和 $e(A_{i,0}, g_2) = e(g_1, B_{i,0})$ 是否成立, 并设置全局公钥为 $\mathsf{pk} = \prod_{i \in \mathrm{QUAL}} B_{i,0}$.

• 部分求值算法 $\mathrm{PEval}(x, \mathsf{sk}_i, \mathsf{vk}_i)$: 计算 $v_i = H_1(x)^{\mathsf{sk}_i}$ 及 $\pi_i \leftarrow \text{EQ-DL}_{H_3}(g, \mathsf{vk}_i, H_1(x), v_i; r)$, 其中 $r \in \mathbb{Z}_q$ 为随机数, 最终输出份额 $s_x^i = (i, v_i, \pi_i)$.

• 合并算法 $\mathrm{Combine}(\mathsf{pk}, \mathcal{VK}, x, \mathcal{E})$ 需要先解析候选集合 $\mathcal{E} = \{s_x^{j_1}, \ldots, s_x^{j_{|\mathcal{E}|}}\}$ (需满足 $|\mathcal{E}| \geqslant t+1$ 且来自不同节点), 并获取验证密钥 $\mathsf{vk}_{j_1}, \ldots, \mathsf{vk}_{j_{|\mathcal{E}|}}$, 随后执行:

– 选取一个索引子集 $I = \{i_1, \ldots, i_{t+1}\}$, 满足对于每个 $i \in I$, 都有 $\text{VfyEQ-DL}_{H_3}(g, \mathsf{vk}_i, H_1(x), v_i, \pi_i) = 1$, 其中 $(i, v_i, \pi_i) \leftarrow s_x^i$. 若不存在此类子集, 输出 $\perp$;

– 计算 $\pi \leftarrow \prod_{j \in I} v_j^{\lambda_{0,j,I}}$ 及 $v = H_2(\pi)$, 输出 (v, π).

• 验证算法 $\mathrm{Vfy}(\mathsf{pk}, x, v, \pi)$: 判断等式 $e(\pi, g_2) = e(H_1(x), \mathsf{pk})$ 和 $v = H_2(\pi)$ 是否成立, 若成立则输出 1, 否则输出 0.

综上, GLOW-DVRF 的 DistKG 算法在 $\mathbb{G}_1$ 中生成验证密钥 vk_i, 而在 $\mathbb{G}_2$ 中生成全局公钥 pk. 其函数求值份额通过 NIZK 验证, 重构后的伪随机值 v 的正确性则通过配对方程验证, 从而实现紧致证明.

4.5　门限格密码系统

门限 Raccoon 方案在 NIST 后量子密码标准化项目中, 格基签名方案 (如 Falcon, Dilithium) 占据主导地位. 为了使这些签名方案适用于高安全性和分布式场景, 研究者开始关注其门限变体的构建与实现, 以满足密钥分散管理和系统容错性的实际需求. TRaccoon 门限签名由 del Pino 等人 [62] 提出, 可以视为 Raccoon 签名的 (t,n) 门限化版本. 在密钥生成阶段, 系统生成包含向量 $\mathbf{s}$ 的私钥 sk、公钥 $\mathsf{vk} := (\mathbf{A}, \lfloor \mathbf{As}+\mathbf{e} \rceil_{\nu_\mathbf{t}})$ 以及每一方的私钥份额 sk_i, 其中 $\mathbf{A}$ 为随机矩阵, $\mathbf{s},\mathbf{e}$ 为随机向量. sk_i 包含 3 部分: 私钥 $\mathbf{s}$ 的 Shamir 秘密共享份额 $\mathbf{s}_i$、每一方的标准签名密钥对 $((\mathsf{vk}_{\mathsf{sig},i})_{i\in[n]}, \mathsf{sk}_{\mathsf{sig},i})$、成对的共享种子集合 $(\mathsf{seed}_{i,j}, \mathsf{seed}_{j,i})_{j\in[n]}$, 种子用在伪随机函数生成掩码. 令 $\mathcal{S}$ 表示参与签名的参与方集合, msg 表示待签名消息, sid 为参与方的会话 id, PRF 为伪随机生成函数, $\mathsf{H}_{\mathsf{com}}$, H_{c} 分别为两个不同的哈希函数, $\nu_\mathbf{t}$ 和 $\nu_\mathbf{w}$ 分别为公钥和承诺丢弃的比特位数. 分布式签名环节如图 2 所示, 签名者通过三轮交互最终生成签名 $\widehat{\mathsf{sig}} = (c, \mathbf{z}, \mathbf{z}')$, 具体如下.

- 每个参与方 P_i 采样随机短向量 $\mathbf{r}_i$ 和噪声 $\mathbf{e}'_i$, 计算承诺 $\mathbf{w}_i = \mathbf{A}\cdot\mathbf{r}_i + \mathbf{e}'_i$ 及其哈希值 $\mathsf{cmt}_i = \mathsf{H}_{\mathsf{com}}(\mathsf{sid}, \mathcal{S}, \mathsf{msg}, \mathbf{w}_i)$, 然后计算行掩码 $\mathbf{m}_i = \sum_{j\in\mathcal{S}} \mathsf{PRF}(\mathsf{seed}_{i,j}, \mathsf{sid})$, 输出 $\mathsf{contrib}_{1,i} = (\mathsf{cmt}_i, \mathbf{m}_i)$.
- 每个参与方 P_i 拿到 $(\mathsf{contrib}_{1,j})_{j\in\mathcal{S}\setminus\{i\}}$ 后, 使用标准 Raccoon 签名算法 (但噪声使用离散高斯采样) 签名得到 $\sigma_i \xleftarrow{\$} \mathsf{Sign}(\mathsf{sk}_i, \mathsf{sid}||\mathcal{S}||\mathsf{msg}||(\mathsf{contrib}_{1,j})_{j\in\mathcal{S}})$, 然后打开承诺 $\mathbf{w}_i$, 输出签名 σ_i.
- 每个参与方 P_i 对所有 $j\in\mathcal{S}$ 验证签名 σ_j 及等式 $\mathsf{cmt}_j = \mathsf{H}_{\mathsf{com}}(\mathsf{sid}, \mathcal{S}, \mathsf{msg}, \mathbf{w}_j)$ 是否成立. 如果验证通过, 计算聚合承诺 $\mathbf{w} = \lfloor \Sigma_{i\in\mathcal{S}} \mathbf{w}_i \rceil_{\nu_\mathbf{w}}$. 然后计算挑战值 $c = \mathsf{H}_{\mathsf{c}}(\mathsf{vk}, \mathsf{msg}, \mathbf{w})$ 和列掩码 $\mathbf{m}_i^* = \Sigma_{j\in\mathcal{S}}\mathsf{PRF}(\mathsf{seed}_{j,i}, \mathsf{sid})$, 计算并输出掩码的响应 $\mathbf{z}_i = c\cdot\lambda_{\mathcal{S},i}\cdot\mathbf{s}_i + \mathbf{r}_i + \mathbf{m}_i^*$, 其中 $\lambda_{\mathcal{S},i}$ 为 $\mathbf{s}_i$ 对应拉格朗日参数.
- 待所有参与方交互完成后, 任意一方可调用签名聚合算法输入 $((\mathsf{cmt}_i, \mathbf{m}_i), (\mathbf{w}_i, \sigma_i), \mathbf{z}_i)_{i\in\mathcal{S}}$, 计算 $\mathbf{z} = \Sigma_{i\in\mathcal{S}}(\mathbf{z}_i - \mathbf{m}_i)$ 和 $\mathbf{z}' = \mathbf{w} - \lfloor \mathbf{A}\cdot\mathbf{z} - 2^{\nu_\mathbf{t}}\cdot c\cdot\mathbf{t} \rceil_{\nu_\mathbf{w}}$, 其中 $\mathbf{t} = \lfloor \mathbf{As}+\mathbf{e} \rceil_{\nu_\mathbf{t}}$, 输出聚合签名 $\widehat{\mathsf{sig}} = (c, \mathbf{z}, \mathbf{z}')$.

5　国内外研究现状总结 —— 存在问题及发展趋势

通过上述文献工作可知, 门限签名的研究已经取得了部分进展, 但仍有以下 4 点问题亟待解决.

门限签名友好的分布式密钥生成机制设计. DKG 作为密钥初始化设置, 不仅提升了密钥的公平性和无偏性, 也能有效解决中心化密钥生成机制潜在的单点故障和密钥托管问题. 具有鲁棒性的低交互 DKG 协议有助于更有效地耦合门限签名协议. 通过多秘密同步共享的方式, 摊销通讯与计算开销; 通过透明化初始设置, 支持参与方的动态出入以及秘密的定期刷新, 提高协议的可延展性. 然而, 当前门限签名和 DKG 的研究相对孤立, 对门限签名友好的 DKG 协议研究尚在起步阶段. 在构造门限签名时, 对于可提供公平无偏置密钥的 DKG 讨论多停留在假设阶段, 对门限签名应用落地的前景存疑. 因此, 讨论 DKG 自身鲁棒性和安全性以及对门限签名友好性是一个迫切问题.

门限签名的高 (通讯/交互) 开销. 分布式密钥生成和签名, 通常需要参与方之间频繁交互, 造成带宽占用和资源损耗. 同时, 分布式计算强调结果的正确性, 即可识别中止性或有保证输出交付性等 [73]. 实现有保证输出交付性的标准技术需依赖广播信道 [18], 但广播信道在同步网络模型下将引发高通讯复杂度, 更无法应用于半同步网络模型. 此外, 实际应用部署中存在参与方动态进出、秘密份额定期刷新以及支持网络延迟的半同步和异步网络等现实需求, 然而参与方的动态性与秘密份额的前摄性将增加交互轮次与通讯开销. 显然, 在同时保证鲁棒性与安全性的前提下, 构造低通讯开销的 DKG 和门限签名是一个公开问题.

门限签名的弱鲁棒性. 由于在门限签名的场景中完全实现鲁棒性通常代价较高, 因此现有门限签名方案对鲁棒性的讨论较少, 许多方案仅实现弱鲁棒性 (可识别中止性), 即若协议执行过程中因恶意方干扰而中止, 系统可以明确定位并识别出这些导致中止的参与方. 在可识别中止方案基础上, 可通过引入新的参与方来替换已识别的恶意参与方, 并重启协议来实现鲁棒性. 此外, 鲁棒性的具体含义在不同应用场景中有所扩展, 包括:

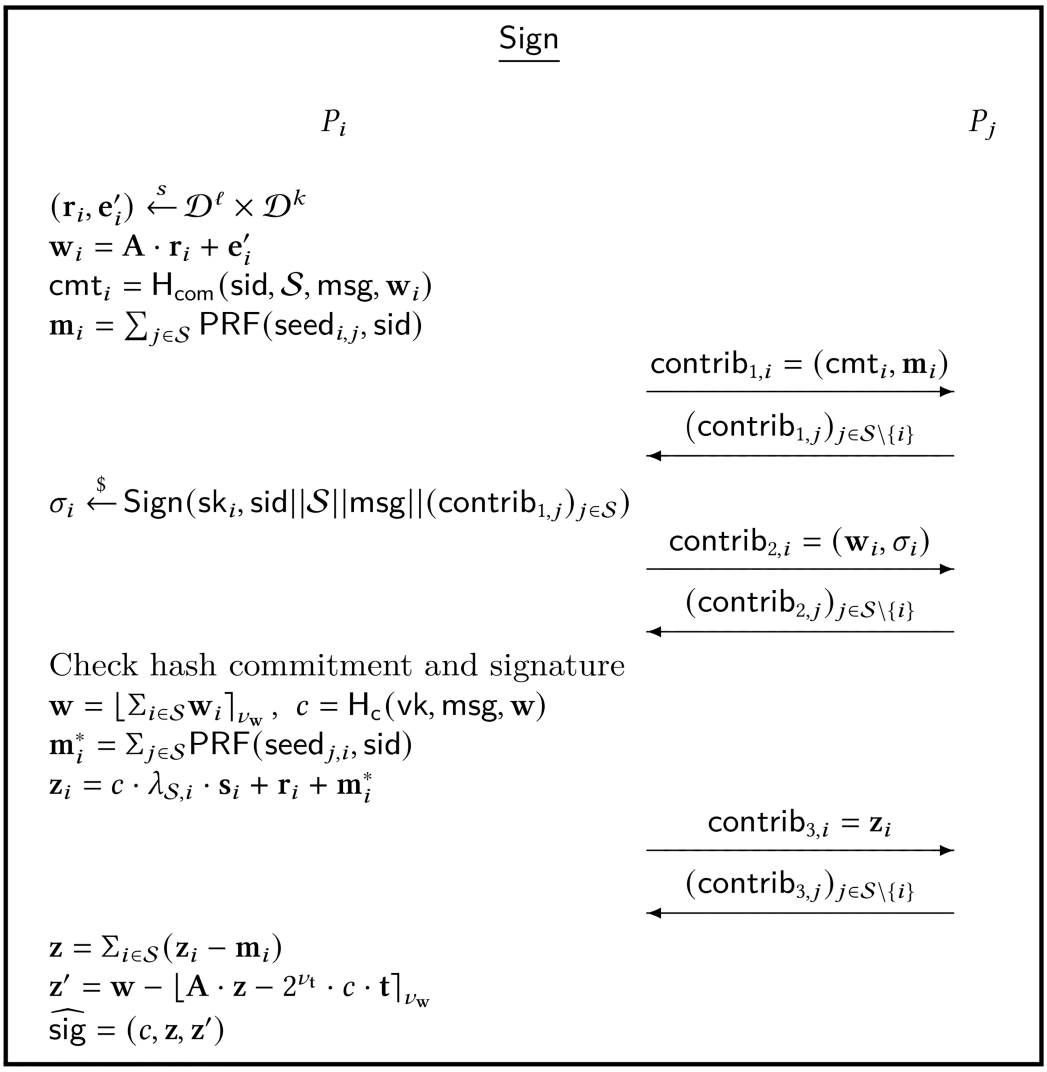

图 2　TRaccoon 分布式签名阶段.

Figure 2　The distributed signing phase of TRaccoon.

(i) 可问责性 (accountability) [74], 即第三方可以审计签名与签名成员合法性并问责作弊参与方; (ii) 可自愈性 [6], 若部分密钥份额丢失, 其他诚实参与方可修复其密钥份额并输出正确结果, 而无需中断协议; (iii) 口令保护性 (password-protected) [63], 将密钥进行秘密分享并利用口令加密保护. 因此, 构造实用门限签名方案不能仅局限于可识别中止性, 而应结合实际需求讨论具有更强鲁棒性的门限签名方案.

门限签名的自适应安全及后量子安全方案构造少. 近年来, 关于参与方动态出入和秘密份额可刷新的安全多方计算新范式研究逐渐引起学术界重视, 包括 Fluid-MPC (multiparty computing) [75] 和 YOSO (you only speak once) [76] 等. 该类范式中定义的前摄性 (proactive) 安全是指在移动敌手模型下, 敌手在不同时间单元中可自适应地收买小于阈值数量的参与方, 同时保证秘密不变而秘密份额可随时间单元定期刷新. 然而, 现有对于前摄性自适应安全门限签名的研究工作屈指可数. 此外, NIST 后量子密码标准算法的公布和近期对门限签名的征集活动表明, 研究具有后量子安全性的自适应安全门限签名已迫在眉睫. 由于将 NIST 候选格签名 (如 Dilithium 等) 直接扩展到分布式门限场景存在诸多实现困难, 相关研究仍然稀少. 值得注意的是, Pino 等人 [64] 近期提出的基于拒绝采样的紧凑型格门限签名方案为这一方向提供了新的思路, 但目前仍主要适用于小规模参与方的情形. 因此, 构造兼具高效性与可扩展性的后量子安全门限签名仍是亟待突破的研究课题.

6　典型应用讨论

6.1　分布式密钥管理与密码学钱包

门限签名算法在分布式密钥管理与密码学钱包中的应用体现了其在提升安全性与灵活性方面的核心价值. 传统的加密货币钱包常面临单点失效或密钥泄露风险, 而门限签名通过将私钥分割为多个份额, 并要求至少阈值数量的份额协作才能生成有效签名, 有效解决了这一问题. 密码学钱包领域, 门限签名技术从多方签名向隐私增强型托管服务演进. Alkadri 等人 [77] 研究了后量子安全的确定性门限钱包, 旨在解决当前主要加密货币所使用的数字签名方案容易受到量子攻击的问题. 作者提出了首个确定性门限钱包的形式化模型, 并展示了一种通用的后量子安全构造方法, 该方法基于任何具有可重随机化密钥的后量子安全门限签名方案. Yin 等人 [78] 提出了一种支持隐形地址的分层确定性钱包 (hierarchical deterministic wallet supporting stealth address, HDWSA), 旨在结合分层确定性钱包和隐形地址的优点, 以提高加密货币用户的隐私和安全性. Das 等人 [79] 提出了密码认证确定性钱包 (password-authenticated deterministic wallets, PADW), 这是一种新型且高效的共享托管钱包解决方案, 旨在解决当前共享托管钱包存在的隐私问题. PADW 方案通过将用户的秘密密钥在用户和服务提供商之间共享, 确保了即使在一方被攻击的情况下, 也能保持安全性. 作者同时基于两方盲 Schnorr 签名给出了一个实例. 当前挑战集中于算法标准化与跨链兼容性, 未来方向包括融合零知识证明构建隐私增强型门限签名、异构密码混合阈值方案, 以及适配 Web3.0 资产的合规化托管框架. 这些进展推动门限签名从理论突破向规模化应用扩展, 为分布式金融与物联网提供底层安全保障.

6.2　分布式匿名代币与匿名凭证

门限签名算法是实现匿名代币与匿名凭证系统的关键技术. 传统方案因颁发者集中持有密钥存在单点失效风险 (密钥泄露可用来任意伪造凭证且难以撤销), 而采用阈值 t/n 机制将密钥分片至多服务器后, 攻击者需攻陷至少 t 个节点才能伪造凭证, 从根本上消除单点信任漏洞, 显著提升系统抗密钥泄露攻击的能力. 得益于签名协议的可组合性, 现有匿名凭证方案无需重新验证属性即可直接替换底层签名机制. 其中, BBS+ 签名方案因支持可组合阈值化实现而广泛应用. 该方案由 Au 等人 [80] 提出, 其名称源于 Boneh 等人 [81] 的群签名方案. BBS+ 可对消息向量进行一次性签名, 其签名尺寸仅取决于安全参数, 与消息数量无关. Goldfeder 等人 [82] 较早探索了门限 BBS+ 签名方案, 其基于 Bar-Ilan-Beaver 反演协议, 采用 Paillier 加密硬编码乘法策略, 为完全盲签名扩展以及阈值无感知 VRF 问题打开了大门. Sonnino 等人 [83] 提出的 Coconut 方案则基于 Pointcheval-Sanders (PS) 签名, 其安全性依赖类 LRSW 的交互假设, 需要较大的公钥尺寸, 导致存储与验证开销显著增加. 相比之下, Doernert 等人 [84] 提出的门限 BBS+ 签名方案在密码学效率方面实现了重要突破, 其核心创新在于采用极简的公钥结构 (仅含 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 两个群元素) 和通用的群兼容性设计, 同时通过单轮 OT 乘法器技术将协议交互流程优化至最简模式: 客户端只需发起单次请求, 签名方经过两轮交互计算即可生成最终签名, 这种设计显著降低了通信开销, 实现了工程部署的实用性. 门限 BBS+ 签名协议因依赖 OT 扩展和乘法协议导致计算和通信开销较大, 其中双线性群运算成为主要性能瓶颈. 未来研究需重点优化效率, 改进乘法协议设计并简化交互流程, 同时探索标准模型下的安全性证明. 此外, 还需扩展协议功能以支持通用阈值和动态管理, 并推动标准化与实际应用落地.

7　总结与展望

随着区块链以及去中心化应用的不断发展, 门限签名算法正从理论研究逐渐向实际应用发展. 本文详细总结了国内外现有门限签名方案的研究成果和目前已有文献中存在的问题和需要解决的焦点问题, 现有的门限签名问题进一步凸显了门限签名中存在的 “高开销”“弱鲁棒” 和 “低安全强度” 等弊端. 在分布式计算需求日益增长的形势下, 高安全强度的门限签名不但可以抵抗恶意敌手的攻击, 同时有助于提升系统安全性与可靠性. 因此, 研究低开销与鲁棒性兼具的自适应安全门限签名的构造方法, 有助于分布式数字身份管理和密钥管理的落地应

用. 需要注意的是, 虽然门限签名的标准化工作正在逐步推进, 但工业化应用依然较少, 这主要源于技术实现复杂度高以及工业界对去中心化安全机制认知不足等原因. 相信随着区块链技术与物联网的深度融合, 门限签名在金融、政务等领域的应用潜力有望被加速释放.

参考文献

1 Tu B B, Chen Y. A survey of threshold cryptography. J Cryptol Res, 2020, 7: 1–14 [涂彬彬, 陈宇. 门限密码系统综述. 密码学报, 2020, 7: 1–14]
2 Jing J W, Zhang S C, Wang P J. Threshold cryptography technology and standardization process. J Cryptol Res, 2024, 11: 227–254 [荆继武, 张世聪, 王平建. 门限密码技术及其标准化进展. 密码学报, 2024, 11: 227–254]
3 Brandão L T A N, Davidson M. Notes on Threshold EdDSA/Schnorr Threshold Schemes. NIST IR 8214B ipd, 2022
4 Brandão L T A N, Peralta R. Nist First Call for Multi-Party Threshold Schemes. NIST IR 8214C ipd, 2023
5 Li Z P, Wang S Y, Wang M. Research of privacy-preserving proximity test. Netinfo Secur, 2024, 24: 817–830 [李增鹏, 王思旸, 王梅. 隐私保护近邻检测研究. 信息网络安全, 2024, 24: 817–830]
6 Wong H W H, Ma J P K, Yin H H F, et al. Real threshold ECDSA. In: Proceedings of NDSS, 2023
7 Gentry C, Halevi S, Lyubashevsky V. Practical non-interactive publicly verifiable secret sharing with thousands of parties. In: Proceedings of EUROCRYPT, 2022. 458–487
8 Abraham I, Jovanovic P, Maller M, et al. Bingo: adaptivity and asynchrony in verifiable secret sharing and distributed key generation. In: Proceedings of CRYPTO, 2023. 39–70
9 Kokoris-Kogias E, Malkhi D, Spiegelman A. Asynchronous distributed key generation for computationally-secure randomness, consensus, and threshold signatures. In: Proceedings of ACM CCS, 2020. 1751–1767
10 Gennaro R, Jarecki S, Krawczyk H, et al. Secure distributed key generation for discrete-log based cryptosystems. J Cryptology, 2007, 20: 51–83
11 Gurkan K, Jovanovic P, Maller M, et al. Aggregatable distributed key generation. In: Proceedings of EUROCRYPT, 2021. 147–176
12 Katz J. Round optimal robust distributed key generation. 2023. https://iacr.steepath.eu/2023/1094-RoundOptimalRobustDistributedKeyGeneration.pdf
13 Zhang H, Duan S, Liu C, et al. Practical asynchronous distributed key generation: improved efficiency, weaker assumption, and standard model. In: Proceedings of DSN, 2023. 568–581
14 Boneh D, Gennaro R, Goldfeder S, et al. Threshold cryptosystems from threshold fully homomorphic encryption. In: Proceedings of CRYPTO, 2018. 565–596
15 Bendlin R, Krehbiel S, Peikert C. How to share a lattice trapdoor: threshold protocols for signatures and (H)IBE. In: Proceedings of ACNS, 2013. 218–236
16 Agrawal S, Stehlé D, Yadav A. Round-optimal lattice-based threshold signatures, revisited. In: Proceedings of ICALP, 2022
17 Tang G, Pang B, Chen L, et al. Efficient lattice-based threshold signatures with functional interchangeability. IEEE Trans Inform Forensic Secur, 2023, 18: 4173–4187
18 Shrestha N, Bhat A, Kate A, et al. Synchronous distributed key generation without broadcasts. 2021. https://eprint.iacr.org/2021/1635.pdf
19 Gennaro R, Jarecki S, Krawczyk H, et al. Robust threshold DSS signatures. In: Proceedings of EUROCRYPT, 1996. 354–371
20 MacKenzie P D, Reiter M K. Two-party generation of DSA signatures. In: Proceedings of CRYPTO, 2001. 137–154
21 国家密码管理局. SM2 椭圆曲线公钥密码算法. 2010. https://www.oscca.gov.cn/sca/xxgk/2010-12/17/content_1002386.shtml
22 Gennaro R, Goldfeder S, Narayanan A. Threshold-optimal DSA/ECDSA signatures and an application to bitcoin wallet security. In: Proceedings of ACNS, 2016. 156–174
23 Gennaro R, Goldfeder S. Fast multiparty threshold ECDSA with fast trustless setup. In: Proceedings of ACM CCS, 2018. 1179–1194
24 Cramer R, Damgård I, Nielsen J B. Multiparty computation from threshold homomorphic encryption. In: Proceedings of EUROCRYPT, 2001. 280–299
25 Damgård I, Pastro V, Smart N P, et al. Multiparty computation from somewhat homomorphic encryption. In: Proceedings of CRYPTO, 2012. 643–662
26 Lindell Y, Nof A. Fast secure multiparty ECDSA with practical distributed key generation and applications to cryptocurrency custody. In: Proceedings of ACM CCS, 2018. 1837–1854
27 Lindell Y. Fast secure two-party ECDSA signing. J Cryptol, 2021, 34: 44
28 Castagnos G, Catalano D, Laguillaumie F, et al. Two-party ECDSA from hash proof systems and efficient instantiations. In:

Proceedings of CRYPTO, 2019. 191–221
29 Castagnos G, Catalano D, Laguillaumie F, et al. Bandwidth-efficient threshold EC-DSA revisited: online/offline extensions, identifiable aborts proactive and adaptive security. Theor Comput Sci, 2023, 939: 78–104
30 Xue H, Au M H, Liu M, et al. Efficient multiplicative-to-additive function from joye-libert cryptosystem and its application to threshold ECDSA. In: Proceedings of ACM CCS, 2023. 2974–2988
31 Doerner J, Kondi Y, Lee E, et al. Secure two-party threshold ECDSA from ECDSA assumptions. In: Proceedings of IEEE S&P, 2018. 980–997
32 Xue H, Au M H, Xie X, et al. Efficient online-friendly two-party ECDSA signature. In: Proceedings of ACM CCS, 2021. 558–573
33 Doerner J, Kondi Y, Lee E, et al. Threshold ECDSA in three rounds. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2024
34 Hou H X, Yang B, Zhang L N, et al. Secure two-party SM2 signature algorithm. Acta Electron Sin, 2020, 48: 1–8 [侯红霞, 杨波, 张丽娜, 等. 安全的两方协作 SM2 签名算法. 电子学报, 2020, 48: 1–8]
35 Zhang Y, He D, Zhang M, et al. A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. Front Comput Sci, 2020, 14: 143803
36 Liu Z Y, Lin J Q. Framework of two-party threshold calculation scheme for SM2 digital signature algorithm. J Softw, 2025, 36: 2188–2211 [刘振亚, 林璟锵. SM2 数字签名算法的两方门限计算方案框架. 软件学报, 2025, 36: 2188–2211]
37 Dahari-Garbian H, Nof A, Parker L. Trout: two-round threshold ECDSA from class groups. In: Proceedings of ACM CCS, 2025. 380–393
38 Lyu Y, Li Z, Zhou H, et al. Threshold ECDSA in two rounds. In: Proceedings of ACM CCS, 2025. 2937–2950
39 Boneh D, Gennaro R, Goldfeder S. Using level-1 homomorphic encryption to improve threshold DSA signatures for bitcoin wallet security. In: Proceedings of LATINCRYPT, 2017. 352–377
40 Doerner J, Kondi Y, Lee E, et al. Threshold ECDSA from ECDSA assumptions: the multiparty case. In: Proceedings of IEEE S&P, 2019. 1051–1066
41 Canetti R, Gennaro R, Goldfeder S, et al. UC non-interactive, proactive, threshold ECDSA with identifiable aborts. In: Proceedings of ACM CCS, 2020. 1769–1787
42 Dalskov A P K, Orlandi C, Keller M, et al. Securing DNSSEC keys via threshold ECDSA from generic MPC. In: Proceedings of ESORICS, 2020. 654–673
43 Smart N P, Alaoui Y T. Distributing any elliptic curve based protocol. In: Proceedings of IMACC, 2019. 342–366
44 Feng Q, Yang K, Zhang K, et al. Stateless deterministic multi-party EdDSA signatures with low communication. 2024. https://eprint.iacr.org/2024/358.pdf
45 Chalkias K, Garillot F, Kondi Y, et al. Non-interactive half-aggregation of eddsa and variants of schnorr signatures. In: Proceedings of CT-RSA, 2021. 577–608
46 Komlo C, Goldberg I. FROST: flexible round-optimized schnorr threshold signatures. In: Proceedings of SAC, 2020. 34–65
47 Bellare M, Crites E C, Komlo C, et al. Better than advertised security for non-interactive threshold signatures. In: Proceedings of CRYPTO, 2022. 517–550
48 Ruffing T, Ronge V, Jin E, et al. ROAST: robust asynchronous schnorr threshold signatures. In: Proceedings of ACM CCS, 2022. 2551–2564
49 Benhamouda F, Halevi S, Krawczyk H, et al. SPRINT: high-throughput robust distributed schnorr signatures. In: Proceedings of EUROCRYPT, 2024. 62–91
50 Chu H, Gerhart P, Ruffing T, et al. Practical schnorr threshold signatures without the algebraic group model. In: Proceedings of CRYPTO, 2023. 743–773
51 Bacho R, Das S, Loss J, et al. Adaptively secure three-round threshold schnorr signatures from DDH. In: Proceedings of CRYPTO, 2025. 390–422
52 Bacho R, Das S, Loss J, et al. Glacius: threshold schnorr signatures from DDH with full adaptive security. In: Proceedings of EUROCRYPT, 2025. 304–334
53 Cho G, Fuchsbauer G, O'Neill A, et al. Schnorr signatures are tightly secure in the ROM under a non-interactive assumption. In: Proceedings of CRYPTO, 2025. 223–255
54 Crites E C, Komlo C, Maller M. Fully adaptive schnorr threshold signatures. In: Proceedings of CRYPTO, 2023. 678–709
55 Lindell Y. Simple three-round multiparty schnorr signing with full simulatability. 2022. https://eprint.iacr.org/2022/374.pdf
56 Garillot F, Kondi Y, Mohassel P, et al. Threshold schnorr with stateless deterministic signing from standard assumptions. In: Proceedings of CRYPTO, 2021. 127–156
57 Kondi Y, Orlandi C, Roy L. Two-round stateless deterministic two-party schnorr signatures from pseudorandom correlation functions. In: Proceedings of CRYPTO, 2023. 646–677
58 Chen X, Zhang F, Tian H, et al. Efficient generic on-line/off-line (threshold) signatures without key exposure. Inf Sci, 2008, 178:

4192–4203
59 Makriyannis N. On the classic protocol for MPC schnorr signatures (or classic schnorr checks all the boxes). 2022. https://eprint.iacr.org/2022/1332.pdf
60 Li Z P, Ma C G, Zhou H S. Overview on fully homomorphic encryption. J Cryptol Res, 2017, 4: 561–578 [李增鹏, 马春光, 周红生. 全同态加密研究. 密码学报, 2017, 4: 561–578]
61 Gür K D, Katz J, Silde T. Two-round threshold lattice signatures from threshold homomorphic encryption. 2023. https://eprint.iacr.org/2023/1318.pdf
62 del Pino R, Katsumata S, Maller M, et al. Threshold raccoon: practical threshold signatures from standard lattice assumptions. In: Proceedings of EUROCRYPT, 2024
63 Dutta S, Roy P S, Safavi-Naini R, et al. Password protected universal thresholdizer. 2024. https://eprint.iacr.org/2024/007.pdf
64 Pino R D, Niot G. Finally! A compact lattice-based threshold signature. In: Proceedings of PKC, 2025. 169–199
65 Schnorr C P. Efficient signature generation by smart cards. J Cryptology, 1991, 4: 161–174
66 Gennaro R, Micciancio D, Rabin T. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products. In: Proceedings of ACM CCS, 1998. 67–72
67 Bellare M, Boldyreva A, Staddon J. Randomness re-use in multi-recipient encryption schemeas. In: Proceedings of PKC, 2003. 85–99
68 Boldyreva A. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In: Proceedings of PKC, 2003. 31–46
69 Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Proceedings of ASIACRYPT, 2001. 514–532
70 Choi K, Manoj A, Bonneau J. SoK: distributed randomness beacons. In: Proceedings of IEEE S&P, 2023. 75–92
71 Internet Computer. Chain-key cryptography. 2023. https://internetcomputer.org/how-it-works/chain-key-technology/
72 Galindo D, Liu J, Ordean M, et al. Fully distributed verifiable random functions and their application to decentralised random beacons. In: Proceedings of EuroS&P, 2021. 88–102
73 Benhamouda F, Halevi S, Krawczyk H, et al. Threshold cryptography as a service (in the multiserver and YOSO models). In: Proceedings of ACM CCS, 2022. 323–336
74 Boneh D, Komlo C. Threshold signatures with private accountability. In: Proceedings of CRYPTO, 2022. 551–581
75 Choudhuri A R, Goel A, Green M, et al. Fluid MPC: secure multiparty computation with dynamic participants. In: Proceedings of CRYPTO, 2021. 94–123
76 Braun L, Damgård I, Orlandi C. Secure multiparty computation from threshold encryption based on class groups. In: Proceedings of CRYPTO, 2023. 613–645
77 Alkadri N A, Das P, Erwig A, et al. Deterministic wallets in a quantum world. In: Proceedings of ACM CCS, 2020. 1017–1031
78 Yin X, Liu Z, Yang G, et al. Secure hierarchical deterministic wallet supporting stealth address. In: Proceedings of ESORICS, 2022. 89–109
79 Das P, Erwig A, Faust S. Shared-custodial password-authenticated deterministic wallets. In: Proceedings of SCN, 2024. 338–359
80 Au M H, Susilo W, Mu Y. Constant-size dynamic k-TAA. 2008. https://eprint.iacr.org/2008/136.pdf
81 Boneh D, Boyen X, Shacham H. Short group signatures. In: Proceedings of CRYPTO, 2004. 41–55
82 Gennaro R, Goldfeder S, Ithurburn B. Fully distributed group signatures. 2019. https://www.orbs.com/assets/docs/white-papers/Crypto_Group_signatures-2.pdf
83 Sonnino A, Al-Bassam M, Bano S, et al. Coconut: threshold issuance selective disclosure credentials with applications to distributed ledgers. In: Proceedings of NDSS, 2019
84 Doerner J, Kondi Y, Lee E, et al. Threshold BBS+ signatures for distributed anonymous credential issuance. In: Proceedings of IEEE S&P, 2023. 773–789

Recent developments in threshold signature scheme

Zengpeng LI[1,2,3], Xudong DENG[1,2], Mei WANG[1,2,3*], Puwen WEI[1,2,3], Shuchao WANG[1,2] & Chunqiu GENG[1,2]

1. *School of Cyber Science and Technology, Shandong University, Qingdao 266237, China*
2. *State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, Qingdao 266237, China*
3. *Quan Cheng Laboratory, Jinan 100190, China*
* Corresponding author. E-mail: wangmeiz@sdu.edu.cn

Abstract Research on distributed secure computation is central to advancements in digital security technology, demonstrating significant value in critical sectors like digital government, fintech, and the Internet of Things. Threshold signature technology serves as a foundational element for distributed digital identity and key management systems. By distributing the processes of key generation and storage, it effectively overcomes the single-point-of-failure vulnerability associated with traditional centralized key management. Its inherent resistance to collusion attacks, high fault tolerance, and support for dynamic node management establish a theoretical basis for next-generation trusted digital infrastructures. Recently, standardization bodies such as NIST and IETF have been actively promoting the standardization of threshold signature schemes, particularly by soliciting efficient threshold constructions for existing standardized signature algorithms such as ECDSA, Schnorr/EdDSA, and post-quantum secure signature schemes. This paper analyzes and summarizes relevant international and domestic research in four areas: distributed key generation (DKG), threshold ECDSA/SM2, threshold Schnorr/EdDSA, and threshold lattice-based cryptography signatures, focusing on aspects like optimizing communication overhead, reducing interaction rounds, enhancing robustness, and achieving proactive security.

Keywords threshold signature, distributed key generation, secret sharing, post-quantum security