群签名及其应用场景

刘 丹[1] 胡桃英[1]
LIU Dan HU Taoying

摘 要 针对实际多方协作场景中隐私保护与行为追溯的双重核心需求，群签名技术因兼具匿名性与可追踪性的独特优势，成为信息安全领域的研究热点。基于此，文章首先系统梳理群签名的定义与分类，明确其安全性要求并完成安全模型的形式化描述；其次，结合电子投票、区块链隐私保护、物联网设备认证及车载网安全通信等典型场景，分析群签名的实际应用价值；最后，阐述群签名技术的国内外研究现状，并展望其未来发展趋向，以期为信息安全领域的相关研究与应用提供参考，为群签名技术的工程化应用提供实践借鉴。

关键词 群签名；静态群签名；动态群签名；安全模型；应用研究

doi：10.3969/j.issn.1672-9528.2026.02.031

0 引言

在信息技术高速发展的背景下，数字签名技术已成为信息安全的重要基石。然而，面对商业联盟决策、医疗数据共享等需要多方协作的场景，传统签名机制暴露出明显的局限性：一方面需要保障参与者的匿名性需求，另一方面又必须满足纠纷时的责任追溯要求。群签名技术通过创新性的设计解决了这一矛盾——允许群成员代表群体生成有效签名（验证者仅能确认签名者属于该群组而无法识别具体身份），同时赋予群管理员在必要时“打开”签名揭示真实身份的特权。这种兼具隐私保护与可追溯性的特性，使其成为平衡信息安全与隐私保障的理想技术方案。

1. 马鞍山师范高等专科学校 安徽马鞍山 243041
[基金项目] 2024 年安徽省一般教学研究项目（2024jyxm0988）；2024 年度安徽省自然科学基金项目（2024AH051773）

1 群签名的分类、定义和安全模型

1.1 分类

根据群组管理的动态特性，群签名可分为静态群签名和动态群签名两大类型。

静态群签名在群系统建立时即固定成员集合，无法在系统运行过程中进行成员变更。若需更换群成员，必须重新建立整个群体系统。在静态群签名方案中，群管理员的职责相对有限，主要负责群签名的追踪工作。静态群签名主要应用于短期项目合同签署、固定委员会决议等场景。

动态群签名则允许在群体系统建立后，由特权管理员动态管理成员资格。管理员既能追踪签名，又能通过颁发或撤销证书来增减成员，整个过程无需重建群体系统。动态群签名主要应用于企业 VPN 访问控制、联盟链节点管理等场景。

1.2 定义

静态群签名的定义基于固定的群成员集合，其核心算法

[4] 李亚晓，李青山，王璐，等 .AmazeMap: 基于多层次影响图的微服务故障定位方法 [J]. 软件学报，2024, 35(7): 3115-3140.
[5] 仇莹，曹刚，朱晞旸 . 电力数据通信网络阻塞故障节点快速辨识研究 [J]. 电子设计工程，2024,32(13):149-153.
[6] 唐婧壹，李强 . 基于无约束插值法的无线传感网络故障节点检测研究 [J]. 传感技术学报，2023,36(7):1143-1147.
[7] 牟小令 . 光纤通信网络中节点故障定位方法研究 [J]. 激光杂志，2023, 44(2):143-148.
[8] 石海杰，李京华，刘丽丽，等 . 基于贝叶斯估计的浅海声源被动定位方法 [J]. 兵工学报，2023,44(5):1394-1402.

【作者简介】
王玖苏（1990—），女，黑龙江哈尔滨人，本科，助理工程师，研究方向：信息工程。

（收稿日期：2025-05-18 修回日期：2026-01-26）

包括以下五个部分：

（1）Setup（系统初始化）：$\text{Setup}(1^{\lambda},1^{n})\rightarrow \text{params}$

输入系统安全参数 λ, $n\in N$ 是群成员的数量，输出公共参数 params。

（2）KeyGen（密钥生成）：$\text{KeyGen}(\text{params})\rightarrow(\text{gpk},\text{sk}_{\text{gm}},\{\text{usk}_i\})$

输入公共参数，输出群公钥 gpk，群管理员私钥 sk_{gm} 和群成员私钥 $\{\text{usk}_i\}_{i=1}^{n}$。

（3）Sign（签名生成）：$\text{Sign}(\text{gpk},\text{usk}_i,M)\rightarrow\sigma$

群成员 i 使用其成员私钥 gsk_i，对消息 M 生成签名 σ。

（4）Verify（签名验证）：$\text{Verify}(\text{gpk},M,\sigma)\rightarrow\{0,1\}$

验证者使用群公钥 gpk，验证签名 σ 的有效性。如果签名有效，返回 1；否则，返回 0。

（5）Open（签名打开）：$\text{Open}(\text{gpk},\text{sk}_{\text{gm}},M,\sigma)\rightarrow i$

群管理员使用私钥 sk_{gm}，打开签名 σ 以确认签名者身份 $i\in\{1,2,...,n\}$。这一步确保签名者的身份可以被唯一追踪，但对验证者不可见。

动态群签名允许成员动态加入或退出群组，其核心算法在静态群签名基础上增加了 Jion 协议，并可能包含 Revocation 机制。

（1）Setup（系统初始化）：$\text{Setup}(1^{\lambda},1^{n})\rightarrow \text{params}$

输入系统安全参数 λ, $n\in N$ 是群成员的数量，输出公共参数 params。

（2）KeyGen（密钥生成）分为两部分：

$\text{KeyGen}_{\text{gm}}(\text{params})\rightarrow((\text{pk}_{\text{gm}},\text{sk}_{\text{gm}}),(\text{pk}_t,\text{sk}_t))$

输入公共参数，输出群管理员的主密钥对 (pk_{gm}, sk_{gm})，和后续追踪密钥对 (pk_t, sk_t)。

$\text{KeyGen}_{\text{user}}(\text{params})\rightarrow(\text{upk}_i,\text{usk}_i)$

输入公共参数，输出群成员 U_i 密钥对 (upk_i, usk_i)，最后群公钥为 $\text{gpk}=(\text{pk}_{\text{gm}},\text{pk}_t,\{\text{upk}_i\})$

（3）Join（成员加入协议）：Join(params, gpk, sk_{gm})$\rightarrow(\text{cert}_i,\tau_i)$

用户与群管理员通过交互协议加入群组，输入公共参数 params，主私钥 sk_{gm}，群公钥 gpk，输出群成员的证书 cert_i 和撤销追踪标记 τ_i。

（4）Sign（签名生成）：$\text{Sign}(\text{gpk},\text{usk}_i,\text{cert}_i,M)\rightarrow\sigma$

群成员 U_i 使用其成员私钥 usk_i，群公钥 gpk，成员证书 cert_i，对消息 M 生成签名 σ。

（5）Revoke（成员撤销）：$\text{Revoke}(\text{RL},\tau_i)\rightarrow\text{RL}'$

群管理员将 τ_i 加入到撤销列表 RL 中，并更新和发布 RL'。撤销检查 $\text{CheckRL}(\text{RL},\sigma)\rightarrow\{0,1\}$，验证 $\tau_i\notin\text{RL}$。

（6）Verify（签名验证）：$\text{Verify}(\text{gpk},M,\sigma,\text{RL})\rightarrow\{0,1\}$

验证者使用群公钥 gpk，可判断该签名的签名者的撤销状态，若未被撤销可验证签名 σ 的有效性。如果签名有效，返回 1；否则，返回 0。

（7）Open（签名打开）：$\text{Open}(\text{gpk},\text{sk}_t,M,\sigma)\rightarrow i$

群管理员使用群公钥 gpk，追踪私钥 sk_t，打开签名 σ 以确认签名者身份 $i\in\{1,2,...,n\}$。

1.3 安全属性及安全模型形式化描述

设静态群签名方案包含算法组 $\prod_{\text{static}}$ = (Setup, KeyGen, Sign, Verify, Open)，动态群签方案包含算法组 $\prod_{\text{dyn}}$ = (Setup, KeyGen, Join, Sign, Revoke, Verify, Open)，安全属性需满足以下形式化要求。

1.3.1 正确性

定义：合法签名必须能通过验证，且可被准确追踪签名者身份。

对于所有合法的签名生成与验证过程，给定安全参数 $\lambda\in N$，群规模 $n\in N$，消息 M，应满足：

$$\forall i\in[n],\Pr\left[\text{Verify}(\text{gpk},M,\sigma)=1\wedge\text{Open}(\text{sk}_{\text{gm}},\text{gpk},\sigma)=i\middle|\begin{array}{l}\text{Setup}(1^{\lambda})\rightarrow(\text{params}),\\ \text{KeyGen}(\text{params})\rightarrow(\text{gpk},\text{sk},\{\text{usk}_i\}),\\ \text{Sign}(\text{gpk},\text{usk}_i,M)\rightarrow\sigma\end{array}\right]=1 \quad (1)$$

式中：gpk 为群公钥；sk_{gm} 为群管理员的私钥；usk_i 为群成员 i 的私钥；σ 为签名。

1.3.2 匿名性

定义：即使敌手掌握群管理员密钥 sk_{gm}，也无法区分签名者身份。

实验框架 $\text{Exp}_A^{\text{anon}-b}(1^{\lambda})$，其中 $b\leftarrow\{0,1\}$

（1）初始化：生成密钥 $\text{KeyGen}(1^{\lambda})\rightarrow(\text{gpk},\text{sk}_{\text{gm}},\{\text{usk}_i\})$。

（2）敌手能力：敌手 A 获取群公钥 gpk 和群管理员的私钥 sk_{gm}，可以访问签名预言机 $O_{\text{sign}}(i, M)$，生成成员 i 对 M 的签名 $\text{Sign}(\text{gpk},\text{usk}_i,M)\rightarrow\sigma$；访问打开预言机 $O_{\text{open}}(\sigma)$，揭示签名的创建者 $\text{Open}(\text{sk}_{\text{gm}},\sigma)\rightarrow i$。

（3）挑战阶段：敌手 A 输出挑战 (M^{*},i_0,i_1)，其中 i_0, i_1 未被查询过，获得挑战签名 σ^{*}，$\text{Sign}(\text{gpk},\text{usk}_{i_b},M^{*})\rightarrow\sigma^{*}$。

（4）胜利条件：敌手 A 输出猜测 b'，若 $b'=b$ 则代表获胜。

安全性要求：

$$\left|\Pr[\text{Exp}_A^{\text{anon}-1}(1^{\lambda})=1]-\Pr[\text{Exp}_A^{\text{anon}-0}(1^{\lambda})=1]\right|\leq\text{negl}(\lambda) \quad (2)$$

式中：negl(λ) 表示一个关于安全参数 λ 的可忽略函数。

1.3.3 可追踪性

定义：敌手即使联合腐化 $n-1$ 个群成员，也无法生成一个能通过验证但无法被追踪到腐化集外成员的签名。

实验框架 $\text{Exp}_A^{\text{trace}}(1^{\lambda})$：

（1）初始化：生成系统参数和密钥，$\text{Setup}(1^{\lambda})\rightarrow(\text{params})$，$\text{KeyGen}(\text{params})\rightarrow(\text{gpk},\text{sk}_{\text{gm}},\{\text{usk}_i\})$。

（2）敌手腐化：敌手 A 选择腐化集合 $C\subset[n]$，获得其私钥 $\{\text{usk}_i\}_{i\in C}$。

（3）预言机访问：敌手 A 可以查询加入预言机 $O_{\text{join}}(i)$，

模拟新成员加入$\text{Jion}(\text{params}, i) \to \text{cert}_i$；查询签名预言机$O_{\text{sign}}(i, M)$，生成成员 i 对 M 的签名$\text{Sign}(\text{gpk}, \text{usk}_i, M) \to \sigma$；查询打开预言机 $O_{\text{open}}(\sigma)$，追踪签名来源$\text{Open}(\text{sk}_{\text{gm}}, \sigma) \to i$。

（4）伪造阶段：A 输出伪造的签名 (M^*, σ^*)。

（5）胜利条件：

签名验证通过：$\text{Verify}(\text{gpk}, M^*, \sigma^*) = 1$；

追踪结果不在腐化集中：$\text{Open}(\text{sk}_{\text{gm}}, \text{gpk}, \sigma^*) \notin C$；

若满足以上两点，则代表获胜。

安全性要求：$\left|\Pr[\text{Exp}_A^{\text{trace}}(1^\lambda) = 1]\right| \le \text{negl}(\lambda)$。

1.3.4 不可诬陷性

定义：敌手无法伪造未被腐化成员的合法签名，即使掌握其他成员的私钥。

对于所有概率多项式时间（PPT）敌手 A，需满足：

$$\Pr\left[\text{Verify}(\text{gpk}, M^*, \sigma^*) = 1 \wedge \text{Open}(\text{sk}_{\text{gm}}, \text{gpk}, \sigma^*) = i \wedge i \notin C \wedge (M^*, i) \notin Q_{\text{sign}}\right] \le \text{negl}(\lambda) \quad (3)$$

式中：Q_{sign} 为签名预言机查询记录。

1.3.5 前向安全撤销

定义：成员在时间 t 被撤销后，撤销前签名仍可被正确追踪（Open 返回真实签名者），撤销后签名验证失败（Verify 输出 0）。

若成员 i 在时间 t 被撤销，则对 $t' < t$ 时期的签名仍然可以被追踪：

$$\forall \sigma \leftarrow \text{Sign}(\text{gpk}, \text{usk}_i^{(t')}, M), \text{Open}(\text{sk}_{\text{gm}}, \text{gpk}, \sigma) = i \quad (4)$$

但对应的签名验证失败：$\text{Verify}(\text{gpk}, M, \sigma, \text{RL}_t) = 0$，若 $\tau_i \in \text{RL}_t$。

2 群签名的应用领域

2.1 电子投票

电子投票系统需满足匿名性、不可伪造性和可验证性。传统方案依赖可信第三方，而群签名技术可实现去中心化信任。Malina 等 [1] 提出基于群签名的端到端安全投票方案：选民以群成员身份签名，计票端仅验证签名合法性，无法关联选民身份，群管理员可在争议阶段追溯签名者，确保投票匿名且可审计。Alshammari 等 [2] 引入群签名纠缠机制，通过多群联合签名与交叉验证，提高抗合谋能力，设计批量验证算法降低计算开销。乔汇东等 [3] 构建了完整的投票 - 计票 - 验证流程，利用群签名隐藏选民身份，结合公开计票通道保证投票结果可被公开验证，实现了无记名投票与透明计票的统一。

2.2 区块链

区块链技术凭借去中心化、不可篡改和透明可追溯的特性，成为数字经济的重要基础设施，但也存在隐私泄漏风险。群签名技术为区块链隐私保护提供了理想方案。Devidas 等 [4] 提出完全去中心化的群签名，契合区块链分布式信任模型。Devidas 等 [5] 引入动态成员管理，满足区块链网络变化需求。Boongasame 等 [6] 将群签名应用于买家联盟链，实现交易隐匿与公平结算。Wang 等 [7] 结合群签名与智能合约，构建可审计的图像交易平台。为提升监管性能，Tang 等 [8] 提出多群管理员架构，分散追踪权限。张蒙等 [9] 结合动态群签名与联邦学习，为区块链模型训练提供隐私保障。

2.3 物联网

物联网设备数量递增，但其资源受限特性使得传统公钥基础设施难以直接应用。群签名技术允许设备以群身份认证，显著降低密钥管理复杂度。石妍妍 [10] 提出基于短群签名的轻量级认证协议，隐藏设备真实身份，将追踪权限交给网络管理员。陈纪成等 [11] 将群签名嵌入安全指令通道，控制平台验证群签名合法性即可确认指令来源，有效防止针对关键终端的定向攻击。徐川等 [12] 利用格基密码构造抗量子群签密方案，显著降低通信与计算开销，适用于功耗和时延敏感的物联网场景。

2.4 车载网

在车联网领域，群签名技术通过轻量级签名与可控追溯，平衡通信安全与身份隐私。车辆使用群证书对广播消息进行轻量级签名，接收方可在毫秒级内验证消息来源的可信性，保障实时通信效率。交通管理中心作为群管理员，在检测到伪造消息时，可通过追溯机制定位肇事车辆并追究责任。甘锦 [13] 将群签名与区块链结合，智能合约仅记录签名哈希，防止恶意关联真实身份。郭健等 [14] 针对路侧单元设计可溯源的批量验证协议，单次验证多车签名，并将追踪权限交给交通管理中心。Jiang 等 [15] 设计的方案在签名中嵌入时效令牌，实现车辆快速匿名接入与撤销。Mamun 等 [16] 针对安全应用层需求，细化群签名访问策略，增强应用层安全。Zhang 等 [17] 将群签名与群会话密钥结合，在车辆完成匿名认证后，可通过群签名协商生成临时通信密钥，同步实现消息认证与机密性保护。

3 研究背景

群签名的概念最早由 Chaum 和 VanHeyst 在 1991 年的文献 [18] 提出，明确了匿名性与可追溯性两大核心特性，为后续研究提供了方向指引。1994 年，Chen 等 [19] 提出一种改进的群签名方案，在计算复杂度与签名长度上有所优化；次年进一步针对信息论模型下的匿名性假设，开展效率优化研究，为特定场景下的高效方案设计提供了理论参考。1996 年，Kim 等 [20] 提出可转换的群签名方案，支持在特定条件下将匿名签名转换为可识别签名，增强了方案的灵活性与实用性。

1998 年，Lee 等 [21] 基于离散对数问题构建群签名方案，利用其计算复杂性提升了安全性。2003 年，Bellare 等 [22] 对群签名进行了形式化定义，并构建了标准化的安全模型，推动了该技术的规范化发展。

在群签名技术的发展过程中，基于身份的群签名方案因其签名和验证过程中的高效性与实用性，逐渐成为研究焦点。1995 年，Park 等 [23] 提出基于身份的群签名方案，显著提高了签名验证效率。1999 年，Tseng 等 [24] 进一步改进算法，提升了方案安全性与运行效率。2003 年，Chen 等 [25] 利用双线性配对技术构建新型基于身份的群签名方案，验证了该技术在群签名场景的应用潜力。2008 年，杨学俊等 [26] 提出一种基于身份的可删除群签名方案，拓展了实际应用场景。

针对大规模群组的高效管理需求，研究者聚焦成员撤销与性能优化。1997 年，Camenisch 等 [27] 设计了适用大规模群组的群签名方案，通过算法与数据结构优化显著提升系统效率。2000 年，Ateniese 等 [28] 构建了可证明安全的抗合谋群签名方案，结合严格的安全证明与结构设计，增强了抗攻击能力。2001 年，Bresson 等 [29] 针对成员动态管理问题，提出高效的撤销机制。

近年来，随着量子计算的发展，基于传统数论难题的群签名方案面临安全挑战，而基于格的群签名因具备抗量子特性成为研究热点。2010 年，Gordon 等 [30] 首次提出基于格的群签名方案，创新性融合原像采样函数与零知识证明技术。2019 年，李雪莲等 [31] 提出适用大群组的格基动态群签名方案，通过引入撤销图灵机，构建管理员与成员协同撤销机制，支持撤销列表的动态更新。

此外，不同特殊形式的数字签名技术与群签名技术相结合，衍生出各种新型签名技术，如群盲签名、分级多群签名、门限群签名等。这些新型签名技术能够满足不同场景的多样化需求，进一步拓展了应用范围。

4 发展趋向

群签名技术正快速发展，重点关注效率提升、后量子安全、动态性增强、安全模型完善及应用拓展。当前研究致力于突破大规模应用的效率瓶颈，以增强实用性和可扩展性。随着量子计算的兴起，后量子安全成为关键研究方向，旨在应对量子威胁。

在动态性方面，成员撤销机制不断优化，验证者本地撤销和完全动态方案逐渐取代传统高开销的撤销列表，适用于企业 VPN 等高流动性场景。然而，跨链兼容性和前向安全性仍需进一步加强。安全模型也在持续改进，Bellare 提出的完全匿名性 / 可追踪性框架成为当前基准，但在标准模型下的可证安全仍面临挑战。

在应用层面，群签名技术不断深化。例如，在区块链智能合约中，自动撤销机制成为研究热点；在电子投票领域的批量验证技术持续优化；在医疗数据共享等隐私场景中，群签名与群盲签名等技术的整合推动了其实用化。未来，需构建监管友好型协议，在保护隐私的同时满足审计需求，实现技术应用与监管要求的平衡。

5 总结

本文系统梳理了群签名的分类、定义、安全模型及其在多个领域的应用。通过对群签名技术的深入探讨，分析了其实际应用价值与面临的挑战。未来，如何设计更高效、安全的群签名方案，并进一步拓展其应用场景，将成为群签名技术研究的重要方向。

参考文献：

[1]MALINA L, SMRZ J, HAJNY J, et al. Secure electronic voting based on group signatures[C]//2015 38th International Conference on Telecommunications and Signal Processing (TSP). Piscataway: IEEE, 2015: 6-10.

[2]ALSHAMMARI H, ELLEITHY K, ALMGREN K, et al. Group signature entanglement in e-voting system[C]//IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014. Piscataway: IEEE,2014: 1-4.

[3] 乔汇东 , 胡瑛 . 基于群签名的电子投票方案 [J]. 湖南工程学院学报 : 自然科学版 , 2012, 22(4): 23-27.

[4]DEVIDAS S, SUBBA RAO Y V, RUKMA REKHA N. A decentralized group signature scheme for privacy protection in a blockchain[J].International journal of applied mathematics and computer science, 2021, 31(2):353-364.

[5]DEVIDAS S, RUKMA REKHA N, SUBBA RAO Y V. Dynamic decentralized group signature scheme for privacy protection in blockchain[C]//International Conference on Innovative Computing and Communications.Berlin:Springer,2022: 745-760.

[6]BOONGASAME L, CHAISING S, TEMDEE P .Blockchain-based trusty buyer coalition scheme using A group signature[J].Journal of mobile multimedia, 2022,18(2):203 - 230.

[7]WANG L, LIU X F, LIN X D. A fair and privacy-preserving image trading system based on blockchain and group signature[J]. Security and communication networks, 2021(1): 5701258.

[8]TANG F, FENG Z, GONG Q H ,et al.Privacy-Preserving scheme in the blockchain based on group signa-

ture with multiple[J/OL].Security and communication networks,2021[2025-12-30].https://onlinelibrary.wiley.com/doi/10.1155/2021/7094910.

[9] 张蒙 , 古春生 , 张言 , 等 . 基于动态群签名的区块链联邦学习隐私保护方案 [J]. 计算机应用研究 ,2025,42(11):3468-3475.

[10] 石妍妍 . 基于群签名的物联网终端隐私保护技术研究 [D]. 北京 : 北方工业大学 ,2023.

[11] 陈纪成 , 包子健 , 罗敏 , 等 . 一种面向工业物联网的远程安全指令控制方案 [J]. 计算机工程 ,2024,50(3):28-35.

[12] 徐川 , 艾星好 , 王杉杉 , 等 . 一种基于格的轻量级物联网群签密认证方案 [J]. 电信科学 , 2024, 40(4):88-106.

[13] 甘锦 . 车联网中结合区块链和群签名的车辆隐私保护方案研究 [D]. 昆明 : 昆明理工大学 , 2021.

[14] 郭健 , 龚银燕 . 一个可溯源的车联网群签名批量验证协议 [J]. 长沙大学学报 , 2023,37(5):7-12.

[15]JIANG Y J, GE S C, SHEN X L. AAAS: an anonymous authentication scheme based on group signature in VANETs[J]. IEEE access, 2020, 8: 98986-98998.

[16]MAMUN M S I, MIYAJI A. Secure VANET applications with a refined group signature[C]//2014 Twelfth Annual International Conference on Privacy, Security and Trust. Piscataway: IEEE,2014: 199-206.

[17]ZHANG C H, XUE X P, FENG L J, et al. Group-signature and group session key combined safety message authentication protocol for VANETs[J]. IEEE access, 2019,7: 178310-178320.

[18]CHAUM D, VAN HEYST E. Group signatures[C]// Advances in Cryptology—EUROCRYPT'91. Berlin:Springer,1991: 257-265.

[19]CHEN L D, PEDERSEN T P. New group signature schemes[C]//Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology.Berlin: Springer, 1994: 171-181.

[20]KIM S J, PARK S J, WON D H. Convertible group signatures[C]// Advances in Cryptology—ASIACRYPT 1996, Lecture Notes in Computer Science.Berlin:Springer,1996: 311-321.

[21]LEE W B, CHANG C C. Efficient group signature scheme based on the discrete logarithm[J]. IEEE proceedings-computers and digital techniques, 1998, 145(1): 15-20.

[22]BELLARE M, SHI H X, ZHANG C. Foundations of group signatures: the case of dynamic groups[C]//Topics in Cryptology–CT-RSA 2005. Berlin:Springer, 2005:136-153.

[23]PARK S, KIM S, WON D. ID-based group signature[J]. Electronics letters, 1997, 33(19): 1616-1617.

[24]TSENG Y M, JAN J K. A novel ID-based group signature[J]. Information sciences, 1999, 120(1-4): 131-141.

[25]CHEN X F, ZHANG F G, KIM K. A new ID-based group signature scheme from bilinear pairings[EB/OL]. 2003[2025-12-30].https://www.researchgate.net/publication/220335324_A_New_ID-based_Group_Signature_Scheme_from_Bilinear_Pairings.

[26] 杨学俊 , 王灯国 , 黄徐徐 . 一个基于 ID 的可删除群签名方案 [J]. 计算机应用 ,2008(4):918-920.

[27]CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[C]//Advances in Cryptology — CRYPTO'97. Berlin: Springer, 1997: 410-424.

[28]ATENIESE G, CAMENISCH J, JOYE M, et al. A practical and provably secure coalition-resistant group signature scheme[C]//Advances in Cryptology—CRYPTO 2000.Berlin: Springer, 2000: 255-270.

[29]BRESSON E, STERN J. Efficient revocation in group signatures[C]//Public Key Cryptography.Berlin:Springer,2001: 190-206.

[30]DOV GORDON S, KATZ J, VAIKUNTANATHAN V. A group signature scheme from lattice assumptions[C]//Advances in Cryptology-ASIACRYPT 2010.Berlin:Springer, 2010: 395-412.

[31] 李雪莲 , 吕晓琳 , 郭利娟 , 等 . 适合大群组的格基动态群签名方案 [J]. 电子科技大学学报 ,2019,48(1):80-87.

【作者简介】

刘丹（1991—），女，安徽芜湖人，硕士，工程师，研究方向：网络信息安全。

胡桃英（1987—），女，安徽芜湖人，硕士，讲师，研究方向：软件技术开发、目标检测算法研究。

（收稿日期：2025-07-12 修回日期：2026-01-27）