中国科学: 信息科学 2022 年 第 52 卷 第 12 期: 2321–2335
SCIENTIA SINICA Informationis
论文

# 基于国产密码 SM2 的实用公钥广播加密方案

陈泌文[1,2,4], 向涛[1*], 何德彪[2], 黄欣沂[3]

1. 重庆大学计算机学院, 重庆 400044
2. 武汉大学国家网络安全学院, 武汉 430072
3. 福建师范大学计算机与网络空间安全学院, 福州 350117
4. 桂林电子科技大学广西可信软件重点实验室, 广西 541004
* 通信作者. E-mail: txiang@cqu.edu.cn

收稿日期: 2021–12–20; 修回日期: 2022–02–02; 接受日期: 2022–02–10; 网络出版日期: 2022–12–06

国家自然科学基金 (批准号: U20A20176, 62102050, 62032005, U21A20466)、教育部科技司区块链核心技术战略项目 (批准号: 2020KJ010301)、中国博士后科学基金 (批准号: BX2021399)、湖北省重点研发计划 (批准号: 2020AEA013)、中央高校基本科研业务费专项资金 (批准号: 2042021kf1030)、湖北省自然科学基金重点项目 (批准号: 2020CFA052)、武汉市科技计划项目 (批准号: 2020010601012187) 和广西可信软件重点实验室研究课题 (批准号: kx202043) 资助

**摘要** 近年来网络攻击与数据泄露事件层出不穷, 网络安全受到国家及相关部门的高度关注. 国产密码算法作为保障我国网络与信息安全的关键技术, 推动其应用与实施既符合构建我国网络强国的战略需求, 又能保障实际应用的健康发展. SM2 公钥加密算法是我国自主设计的国产商用密码之一, 可有效保障数据在通信过程中的安全性. 然而, 经典 SM2 公钥加密算法适合 “一对一” 通信场景, 在 “一对多” 通信场景中需承担较大的计算与通信开销. 为提升 SM2 公钥加密算法在 “一对多” 通信场景中计算与通信效率, 扩展我国商用密码的应用范围, 本文将我国商用密码 SM2 公钥加密算法和广播加密概念相结合, 利用 Diffie-Hellman 密钥交换和多项式秘密分享的思想, 设计了基于 SM2 的公钥广播加密方案. 所构造方案最大程度地保留原有 SM2 公钥加密算法结构, 通过简单地扩展即可实现在多用户场景下消息安全广播的自主可控. 与现有广播加密方案相比, 所构造方案的系统参数大小与接收者数量无线性关系, 以及系统无需指定数据发送者广播消息. 所构造方案的安全性分析表明, 本文方案与 SM2 公钥加密算法具有相同安全强度. 理论分析与实验仿真表明, 所构造方案具有较好的性能, 显著增强了我国商用密码的实用性.

**关键词** 公钥加密, SM2 公钥密码算法, 广播加密, Diffie-Hellman 密钥协商

## 1 引言

密码技术为大数据、物联网、5G 等新技术、新业态的发展提供了重要的安全技术保障, 加密算法作为其重要分支在保障数据安全和用户隐私方面发挥了重要作用. 随着时代的信息化变革, 社会生产

**引用格式:** 陈泌文, 向涛, 何德彪, 等. 基于国产密码 SM2 的实用公钥广播加密方案. 中国科学: 信息科学, 2022, 52: 2321–2335, doi: 10.1360/SSI-2021-0424
Chen B W, Xiang T, He D B, et al. An efficient public-key broadcast encryption scheme based on SM2 (in Chinese). Sci Sin Inform, 2022, 52: 2321–2335, doi: 10.1360/SSI-2021-0424

 

生活都离不开密码的保护, 如在线支付、医疗健康数据管理等. 加密算法通过生成仅有授权用户才能正确解密的密文来确保数据应用过程中的机密性, 进而在新技术、新业态中实现数据安全存储和传输. 特别是在抗击新冠疫情的斗争中, 通过利用加密算法, 国家疾控数据、个人身份信息等得到了有效的保障.

面对全球日益严峻的网络安全形势, 发展我国自主可控的国产加密算法已经成为维护社会正常运转的重中之重. 当前网络安全威胁日趋呈现复杂、多元等特征, 严重威胁了国家安全和人民合法权益, 网络空间安全已经上升到新的高度. 国家相继颁布与实施《密码法》和《数据安全法》等政策法规, 有关部门站在国家战略层面, 积极推动国产密码算法应用与实施. 通过国产化网络产品及服务中的加密方法, 有效摆脱对国外技术的过度依赖, 加速自主可控的网络安全环境建设.

我国在加密算法方面已取得显著成果, 在新时代背景下仍面临严峻挑战. 2010 年, 国产商用密码算法 SM2 经国家密码管理局发布, 不仅成为我国密码标准, 还已经成为了 ISO/IEC 国际标准 [1]. SM2 已在全国范围内进行了推广和普及, 包括安全传输、身份认证等众多领域, 为系统安全提供了安全技术保障. 然而, 经典 SM2 公钥加密算法在每次执行过程中实现的是面向单用户公钥的加密, 严重限制了其在新型信息技术场景中应用. 以物联网场景为例, 如需向多个远程设备下达相同命令, 基于 SM2 的方法只能通过重复执行 SM2 加密算法为不同设备产生对应的不同密文, 增加了整个系统的计算与通信开销, 极大地降低了系统数据安全共享效率.

广播加密 (broadcast encryption, BE) [2] 是一种以广播的方式实现 “一对多” 场景的安全数据共享机制. 广播加密概念于 1993 年被提出并得到广泛应用, 如智能电网、卫星广播等. 受新冠疫情影响, 视频会议、在线学习等已逐渐成为当前主流的沟通与学习方式, 这为广播加密方案应用提供了更广阔的应用场景. 广播加密的基本通信框架主要包含两类角色: 数据发送者 (data sender) 和接收者 (data user). 数据发送者利用广播加密算法生成可供多个不同接收者解密的广播密文, 每个接收者均可通过解密该密文获得共享明文数据. 数据发送者无需单独为某个接收者产生密文, 进而降低了系统的通信与计算开销.

广播加密自提出以来, 一直受到广泛关注 [3~6], 但现有方案在我国实际应用中仍面临诸多关键挑战. 大部分现有广播加密方案在我国应用时, 主要面临以下 3 类挑战: (1) 实用的广播加密方案自主可控程度不高, 我国自主可控的商用广播加密算法还鲜有研究. 最近, Lai 等 [6] 基于商用密码 (SM9 身份标识算法) 提出了一种身份标识的广播加密方案, 进一步丰富了我国商用密码的理论体系. 然而, 该方案对 SM9 进行了较大改造 (仅保留了密钥生成算法结构), 导致其无法直接部署于现有支持 SM9 的基础设施中. 同时, 他们的方案属于基于标识的密码体制, 依赖密钥中心为新增用户产生密钥, 密钥托管问题将限制其应用场景. (2) 现有多数广播加密方案需要预先初始化系统最大接收者数量, 而事先确定系统规模的方法将严重限制方案的可扩展性和实用性. 如在方案 [4,7] 中密钥中心需根据接收者数量确定系统公开参数, 导致在系统初期存在大量数据冗余, 以及当系统人数超过预期时不得不重启整个系统. (3) 部分广播加密方案需要提前指定数据发送者进行数据广播, 这将限制方案应用的灵活性. 实际应用中, 除电视、卫星广播这种单中心共享场景外, 还包括多中心相互共享场景, 如视频会议. 在这种场景下, 每个系统的参与者均可能有安全广播的需求, 因而提前指定数据发送者的方案应用场景有限.

为有效应对上述挑战, 受方案 [6] 的思想启发, 我们探索能否基于国产密码 SM2 设计我国自主可控的公钥广播加密方案, 该类型方案主要优势包括: (1) SM2 公钥加密算法已成为国家标准并具有相对成熟的应用基础, 构建基于 SM2 的广播加密方案可降低企业设备升级开销, 可在现有基础上进行推广应用. (2) SM2 公钥加密算法无需密钥中心, 不存在密钥托管问题, 能与基于 SM9 的标识广播加密

方案 [6] 在应用场景上形成互补. 因此, 本文结合广播加密需求与 SM2 公钥加密算法特点, 提出了适应“一对多” 场景的基于 SM2 的公钥广播加密方案. 方案可在不修改现有 SM2 公钥加密算法基础设施的条件下, 通过适当增加步骤实现 “一对多” 安全传输的目标. 本文的主要贡献如下:

(1) 针对我国实际应用对广播加密方案自主可控的战略需求, 提出了基于国产密码 SM2 的公钥广播加密方案. 方案在避免密钥分发与管理问题的同时, 最大程度地保留了 SM2 公钥加密算法原有结构, 使得所构造方案满足安全可控的要求的同时, 减少对现有设备的升级成本.

(2) 对基于 SM2 的公钥广播加密方案的定义和安全模型进行了刻画, 并基于安全模型证明了所构造方案的安全性. 方案的安全性依赖椭圆曲线上的困难问题和 SM2 公钥加密算法的安全性, 其安全强度与 SM2 相同.

(3) 通过与其他功能类似的广播方案进行比较分析以及编程实现所构造方案, 对所构造方案的计算与通信开销进行理论与实验评估. 相比现有方案, 所构造方案以少量计算性能为代价来显著提升方案的通信性能, 有效地平衡了计算与通信开销.

## 2 相关工作

广播加密概念自提出以来, 因其有广泛的应用场景和实际意义一直受到广泛关注, 并形成了丰富的理论与应用成果. 基于本文研究侧重点和发展趋势, 本小节分别从安全性、功能性和实用性 3 个方面对广播加密研究现状进行分析.

**安全性.** 早期的广播加密方案 [2] 只能在确定数量的合谋者情况下才是安全的, 导致在实际中存在应用限制和安全隐患. 为此, 设计面向不同安全模型的安全广播加密方案成为研究热点. 不同于多数实现选择明文安全的广播加密方案 [8,9], Li 等 [10] 提出了抵抗私钥持续泄漏的方案, 并证明了方案的安全性. Goyal 等 [11] 介绍了一种支持索引隐藏和消息隐藏的增强广播加密方案, 并基于位置证据加密方案给出了实例化构造, 增强广播加密的安全性. Chen 等 [12] 基于证书的密码系统的启发, 设计了可实现自适应选择密文安全的广播加密方案. 除此之外, 研究者们也构造了具有其他安全属性的广播加密方案以提升方案在实际应用过程中安全性. 考虑到量子计算机的挑战, Agrawal 等 [13] 和 Brakerski 等 [14] 提出了抗量子计算机攻击的安全广播加密方案. 为满足应用对隐私保护的安全需求, Lai 等 [15] 提出了一种隐私保护的广播加密方案, 该方案在实现与多人共享数据的同时, 维护数据接收者身份的隐私.

**功能性.** 广播加密除满足与多人共享数据的基本需求外, 可能还需要根据实际应用提供其他特定功能, 如内积 [16]、可撤销 [17,18]、访问控制 [19,20] 等. 为应对数据接收者集合发生变化的情况, 带撤销功能的广播加密受到广泛关注 [21~23]. 带撤销功能的广播加密方案可以在部署成功后, 通过撤销机制来实现对授权用户集合的管理, 进而有效应对如离职、职务变更等实际情况. 支持访问控制的广播加密方案可实现对数据的灵活访问控制授权, 通过访问控制策略和订阅集合共同组成授权集合. Lai 等 [24] 考虑到云计算场景中授权集合变化的情况, 通过融合基于身份的密码系统提出了可扩展的广播加密方案, 进一步提升了云计算场景中数据访问控制的灵活性. 支持个性化消息的广播加密方案不仅支持向多个数据接收者发送同一个消息, 同时还支持为特定用户发送个性化消息. Chen 等 [25] 结合基于证书的密码系统和匿名性提出了一种支持个性化消息的广播加密方案. 他们的方案不仅保护了数据接收者的隐私, 在性能方面也具有较好的优势. 除上述之外, Wang 等 [26] 提出功能广播加密方案的概念, 这种方案可同时实现对加密数据和数据接收者的控制, 进一步增强了云计算环境中数据共享的灵活性. Jiang 等 [27] 将关键词搜索功能融合到广播加密方案中, 提出了实现关键词搜索的广播加密方案, 扩展

**表 1　主要符号**

**Table 1**　Main symbols

| Symbol | Description |
|---|---|
| $\lambda$ | System security parameter |
| ecc | Elliptic curve parameters such as $F_p, E(F_p), G, n$ |
| $n$ | Prime order of $G$ |
| $m$ | Number of data users |
| $M$ | A message string of length ml-bits |
| $S_R$ | A set of all authenticated data users |
| $(w_0, w_1, \ldots, w_m)$ | Polynomial coefficients and as part of the ciphertext |

了方案的功能性. Deng 等 [28] 提供了一种方案转化机制, 可将加密方案转化为广播加密方案, 转换后方案因无需提前确定接收者而具有更好的扩展性.

**实用性.** 提升广播加密方案的实用性也是广播加密研究的热点方向之一. 早期方案由于密文大小与授权用户数量呈线性关系, 导致系统的通信效率极低, 因而设计固定密文大小的广播加密方案成为主要挑战. Zhao 等 [29] 提出可实现固定密文和密钥大小的广播加密方案, 定义了支持公开溯源的弱黑盒广播加密. Zhu 等 [30] 从授权集合与非授权集合大小关系角度, 提出了一种双模式的广播加密方案. 他们的方案通过找到授权与非授权集合的最小值来确定加密的模式. 除了考虑密文大小, 降低公开参数的规模也是提升广播加密实用性的方法. Li 等 [31] 提出了基于证书的匿名广播加密方案, 该方案避免密钥托管问题的同时, 降低了系统参数的大小. Wee [3] 依赖双向 K-Lin 假设, 提出了公开参数大小仅为 $O(N^{1/3})$ ($N$ 为系统用户数) 的广播加密方案, 极大地降低了公开参数的存储空间. 除考虑提升存储通信效率外, Kim 等 [4] 提出支持外包部分解密的广播加密方案以提升数据接收者的解密效率, 并通过仿真实验证明他们的方案可有效提升边缘节点到终端设备之间的性能. Canard 等 [32] 设计多信道广播加密方案, 该方案可利用最短的全局密文来为不同群组授权接收者分发密钥, 增强信息共享效率. 最近, Chhatrapati 等 [33] 基于 MCL java library 实现了当前主流的基于双线性对的广播加密方案, 对他们的性能进行了对比评估, 为广播加密方案的设计与应用提供了重要参考.

本文从实用性角度出发, 构造了基于 SM2 公钥加密的公钥广播加密方案. 与现有方案相比主要区别在于: (1) 本文方案是基于现有 SM2 公钥加密算法而设计, 可通过简单地扩展现有 SM2 公钥加密方案来实现广播加密, 因而能直接部署到现有 SM2 公钥加密基础设施中, 实现多用户的数据传输与共享. (2) 本文方案无需在系统初始化阶段确定接收者集合大小, 消息广播者可根据具体情况确定授权接收者规模. (3) 本文方案无需指定广播者, 系统中任意用户均可根据需要进行消息广播.

## 3　预备知识

### 3.1　符号定义

ecc $= (F_p, E(F_p), G, n)$ 为椭圆曲线相关参数, 其中 $E(F_p)$ 为由椭圆曲线点集, $G = (x_1, y_1)$ 为 $E(F_p)$ 上的基点, $(x_1, y_1)$ 分别表示 $G$ 的横、纵坐标, $n$ 为 $G$ 的阶. 定义 $[d]G$ 表示 $d$ 个点 $G$ 相加, 即 $G+G+\cdots+G$. 定义 $||$ 为连接符, 如 $s_1||s_2$ 表示 $s_1$ 与 $s_2$ 的串联. 定义 $\oplus$ 表示逐比特异或操作. 本文其他符号的定义如表 1.

### 3.2 困难问题假设

为便于后期方案的安全性证明, 本小节对 CDH (computational Diffie-Hellman problem) 困难问题进行了简单的扩展, 定义了一个扩展的 CDH 困难问题, 记为 $m$-CDH.

**定义1** ($m$-CDH 困难问题) 对于基于安全参数确定的群 $\mathbb{G}$ (阶为 $p$), 已知的元素 $G, [x]G$, $[y_1]G$, $[y_2]G, \ldots, [y_m]G \in \mathbb{G}$, $(x, \{y_j|j=1,\ldots,m\}) \in \mathbb{Z}_p$ 是均匀分布且未知的随机数, 则在多项式时间内计算任意 $[xy_i]G$ 是困难的.

对于任意 $i=1,\ldots,m$, $(G, [x]G, [y_i]G)$ 可构成标准的 CDH 困难问题, 因而计算 $[xy_i]G$ 是困难的. 又因为 $([y_1]G, [y_2]G, \ldots, [y_m]G$ 是彼此相互独立, 进而使得已知任意 $[y_j]G, j \neq i$, 对加速计算 $[xy_i]G$ 无影响. 因此, $m$-CDH 问题也是困难的.

### 3.3 密码模块

#### 3.3.1 Diffie-Hellman 密钥协商

Diffie-Hellman (DH) 密钥协商是一种可在非安全信道中安全的协商出共享密码的算法. 自被提出以来, 该算法已被广泛应用于安全领域, 如 Https 协议的 transport layer security (TLS). DH 密钥协商过程如下:

(1) A, B 双方协商确定公开参数, 如选取群 $\mathbb{G}$ 和生成元 $G$, 令 $n$ 表示群的阶.

(2) A, B 双方分别选择随机数 $(a, b) \in [1, n-1]$ 和计算对应的 $X=[a]G$ 和 $Y=[b]G$.

(3) A, B 双方分别向对方发送 $X$ 和 $Y$, 并根据收到的信息计算密钥 $k=[a]Y=[b]X=[ab]G$.

#### 3.3.2 SM2 公钥加密算法

SM2 公钥加密算法 [1] 主要用于实际系统中消息的加解密, 具有密钥短和加密速度快等特征. SM2 公钥加密算法详细步骤如下.

• **Setup**$(\lambda) \to$ pp. 根据选定的 $\lambda$, 选定椭圆曲线系统参数 $\mathrm{ecc}=(F_p, E(F_p), G, n)$. 再分别选择密钥派生函数 $\mathrm{KDF}: \{0,1\}^* \times \mathrm{ml} \to \{0,1\}^{\mathrm{ml}}$ 和哈希函数 $h: \{0,1\}^* \to \{0,1\}^{\mathrm{hl}}$, ml, hl 分别表示待加密消息和哈希输出的长度. 最后, 公布上述系统参数 $\mathrm{pp}=(\mathrm{ecc}, h, \mathrm{KDF})$. 系统用户本地存储上述系统参数.

• **KeyGen**$(\mathrm{pp}) \to (\mathrm{PK}, \mathrm{sk})$. 根据确定的 pp, 接收者选择随机私钥 $\mathrm{sk}=d \in [1, n-1]$ 并计算对应公钥 $\mathrm{PK}=[d]G \in E(F_p)$. 最后, 接收者秘密地保存私钥 sk 和并向认证中心注册 (certificate authority, CA) 公钥 PK. 系统中每个用户的公钥由证书认证中心进行验证, 将公钥与其真实身份进行映射, 保障消息发送者均可以正确获得其他用户的公钥.

• **Enc**$(\mathrm{pp}, \mathrm{PK}, M) \to C$. 为保障传输消息 $M$ 的机密性, 发送者根据确定的 pp, PK 和消息 $M$, 通过执行以下操作产生接收者可解密的密文.

(1) 发送者以随机的方式选择 $k \in [1, n-1]$, 并根据 $k$ 计算获得 $C_1=[k]G=(x_1, y_1) \in E(F_p)$, 其中 $x_1$ 和 $y_1$ 分别表示点 $C_1$ 的横、纵坐标.

(2) 发送者利用公钥 PK 计算椭圆曲线点 $[k]\mathrm{PK}=(x_2, y_2)$, 并基于椭圆曲线点的横、纵坐标 $(x_2, y_2)$ 生成长度为 ml 的字符串: $t=\mathrm{KDF}(x_2||y_2, \mathrm{ml})$. 如果生成的字符串 $t$ 为全 0, 则重新执行.

(3) 发送者利用字符串 $t$ 计算 $C_2=M \oplus t$, 并利用点 $[k]\mathrm{PK}$ 的横、纵坐标计算 $C_3=h(x_2||M||y_2)$. 最后, 发送者输出在公钥 PK 下的密文 $C=(C_1, C_2, C_3)$.

• **Dec**$(\mathrm{pp}, \mathrm{sk}, C) \to M'$. 为获得在公钥 PK 下密文 $C=(C_1, C_2, C_3)$ 对应的明文消息, 接收者根据确定的 pp、私钥 sk, 通过执行以下步骤获得密文所对应的明文.

(1) 接收者利用私钥和密文 $C_1$ 计算 $[\mathrm{sk}]C_1 = [k]\mathrm{PK} = (x_2, y_2)$, 进而基于对横、纵坐标恢复字符串 $t = \mathrm{KDF}(x_2||y_2, \mathrm{ml})$. 如果字符串 $t$ 为全 0, 则解密失败并直接退出; 否则, 执行步骤 (2).

(2) 接收者利用字符串 $t$ 恢复 $M' = C_2 \oplus t$, 并计算对应的 $C_3' = h(x_2||M'||y_2)$.

(3) 接收者判断 $C_3'$ 与 $C_3$ 是否相等; 如果相等, 解密成功; 否则, 则直接退出.

为易于理解和简化表达, 在随后描述中用 SM2.**X** 表示 SM2 公钥加密算法的 **X** 操作, 如 SM2.**Enc** 表示执行 SM2 算法中的 **Enc** 加密操作.

### 3.4 公钥广播加密方案

#### 3.4.1 方案系统模型

公钥广播加密方案包括 3 类实体: 可信中心、数据发送者和数据接收者. 可信中心负责生成系统公开可信参数和维护用户的公钥证书列表, 数据发送者负责产生支持多人解密的广播密文, 而数据接收者则利用私钥享受数据共享服务.

#### 3.4.2 方案形式化定义

为实现 "一对多" 通信, 专家学者提出了公钥广播加密的概念. 它主要是指在公钥基础设施上, 产生支持多接收者解密的广播密文以提升数据共享效率. 公钥广播加密包括初始化 (**Setup**)、密钥生成 (**KeyGen**)、广播加密 (**Encryption**) 和解密 (**Decryption**) 4 个算法.

• **Setup**$(\lambda) \to \mathrm{pp}$. 该算法由可信方运行来确定公开参数. 算法以输入 $\lambda$ 作为开始, 确定公开参数 pp 后结束, 包括椭圆曲线参数和哈希函数等.

• **KeyGen**$(\mathrm{pp}) \to (\mathrm{PK}, \mathrm{sk})$. 该算法由系统中用户运行以确定加/解密文所需的公私钥. 算法以输入 pp 作为开始, 确定密钥 $(\mathrm{PK}, \mathrm{sk})$ 后结束. 类似于 SM2, 用户需要对公钥进行认证, 保障系统中其他用户可以正确获得指定接收者的公钥.

• **Encryption**$(\mathrm{pp}, S_R, M) \to C$. 该算法由发送者运行, 生成支持多接收者可解密的密文. 算法以 pp, 接收者公钥集合 $S_R = (\mathrm{PK}_1, \ldots, \mathrm{PK}_m)$ 以及待加密的明文 $M$ 为输入, 并输出在 $S_R$ 下的密文 $C$. 不同于经典 SM2 公钥加密算法, 本文所构造方案加密算法需要输入多个接收者的公钥集合 $S_R$.

• **Decryption**$(\mathrm{pp}, C, \mathrm{PK}, \mathrm{sk}) \to M/\perp$. 该算法由接收者运行, 用于从密文中恢复明文. 算法以 pp, $C$, PK 以及对应的 sk 为输入, 并输出消息 $M$ 或者 $\perp$. 如果输入为无效密文或 $\mathrm{PK} \notin S_R$, 解密算法输出 $\perp$.

基于广播加密方案的功能要求, 其正确性可定义为: 如果对于任意 $\mathrm{pp} \leftarrow$ **Setup**$(\lambda)$, $(\mathrm{PK}_i, \mathrm{sk}_i) \leftarrow$ **KeyGen**$(\mathrm{pp})$, $C \leftarrow$ **Encryption**$(\mathrm{pp}, S_R, M)$, 等式成立

$$\textbf{Decryption}(\mathrm{pp}, C, \mathrm{PK}_i, \mathrm{sk}) = \begin{cases} = M, & \mathrm{PK}_i \in S_R, \\ = \perp, & \mathrm{PK}_i \notin S_R, \end{cases} \tag{1}$$

则说明公钥广播加密方案满足正确性要求. 基于 SM2 的广播加密方案延续上述方案的形式化定义, 因而如何在保持 SM2 算法原有结构的情况下实现安全广播加密是本文构造方案的主要挑战.

#### 3.4.3 方案威胁模型

方案主要面临来自外部敌手的攻击, 其主要目标是获得广播密文所对应的明文信息. 敌手的攻击能力主要包括: (1) 可以窃听、拦截公开信道上的信息, 如公开参数等; (2) 可以获得算法的具体信息, 如加/解密算法流程; (3) 可以根据公开参数仿真算法, 如利用公开参数生成合法的公私钥.

#### 3.4.4 方案安全模型

公钥广播加密的安全模型 [2] 通过密文不可区分来定义, 并利用攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间通信情况进行刻画, 具体包括如下几个阶段:

• **初始化阶段.** $\mathcal{A}$ 选择挑战公钥集合 $S_R^* = (\mathrm{PK}_1^*, \ldots, \mathrm{PK}_m^*)$ 作为确定攻击目标, 其中 $m$ 表示接收者数量. $\mathcal{C}$ 基于给定的 $\lambda$, 通过运行 **Setup**($\lambda$) 算法生成 pp.

• **询问阶段 1.** 该过程主要用于刻画攻击者 $\mathcal{A}$ 在方案执行过程可获得的信息. 主要询问包括.

(1) 公钥查询. $\mathcal{A}$ 能询问接收者的公钥. 如果挑战者存储公钥列表已有对应的公钥 PK, 则直接返回; 否则, $\mathcal{C}$ 通过 **KeyGen**(pp) 产生密钥对 (PK, sk). $\mathcal{C}$ 将公钥 PK 发送给 $\mathcal{A}$, 并将 PK 存储于已知公钥集合中. 同时, 为了应对攻击者的其他挑战, $\mathcal{C}$ 秘密地保存私钥 sk.

(2) 解密查询. $\mathcal{A}$ 能询问已知公钥对应密文 $C$ 的解密. $\mathcal{C}$ 根据已知公钥集合中已查询公钥 $\mathrm{PK} \notin S_R^*$ 确定对应的私钥, 并通过运行解密算法 **Decryption** 获得解密明文, 并将其返回给 $\mathcal{A}$.

值得注意的是, 由于公钥广播加密方案属于非对称加密体制, $\mathcal{A}$ 可自行生成任意已知公钥下对应的密文, 无需进行加密查询.

• **挑战阶段.** 当 $\mathcal{A}$ 决定结束询问阶段 1 之后, 根据获得的信息选择两个长度相同的挑战消息 $(M_0, M_1)$ 并发送给 $\mathcal{C}$. 一旦收到挑战消息, $\mathcal{C}$ 首先选择一个随机比特 $b \in \{0,1\}$, 再执行加密算法 **Encryption**$(\mathrm{pp}, S_R^*, M_b)$ 生成 $M_b$ 的密文 $C_b$, 并将其发给攻击者 $\mathcal{A}$ 作为响应.

• **询问阶段 2.** 在获得挑战密文后, $\mathcal{A}$ 仍可按照询问阶段 1 继续进行公钥查询. 该阶段有效刻画了攻击者能否根据挑战密文获得额外辅助信息. 攻击者 $\mathcal{A}$ 在该阶段唯一的限制是不能对挑战密文 $C_b$ 进行解密查询, 否则可直接判断挑战密文来自那个挑战消息.

• **猜测阶段.** 当攻击者 $\mathcal{A}$ 决定终止询问后, 它根据获得的信息输出对 $b$ 的猜测 $b^* \in \{0,1\}$. 如果 $b = b^*$, 判定 $\mathcal{A}$ 在本游戏中获胜.

根据上述游戏描述, $\mathcal{A}$ 在上述 IND-sPK-CCA 游戏中获胜的优势 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\lambda)$ 可定义为

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\lambda) = \left| Pr[b = b^*] - \frac{1}{2} \right|, \tag{2}$$

其中 $\frac{1}{2}$ 为随机概率. 如果 $\mathcal{A}$ 可以攻击所构造方案, 则意味着能以不可忽略的优势赢得上述游戏.

**定义2** 对于任意的公钥广播加密方案, 如果攻击者 $\mathcal{A}$ 在上述游戏中获胜的优势 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\lambda)$ 不是难以被忽略的, 则称方案在上述的安全模型下是安全的.

## 4 方案构造

### 4.1 方案描述

(1) **Setup.** 基于安全参数 $\lambda$, 首先是确定椭圆曲线系统参数 $\mathrm{ecc} = (F_p, E(F_p), G, n)$. 接着选择安全哈希函数 $h: \{0,1\}^* \to \{0,1\}^{\mathrm{hl}}$, $h_1: G \to [1, n-1]$ 以及密钥派生函数 $\mathrm{KDF}: \{0,1\}^* \to \{0,1\}^{\mathrm{ml}}$. 最后是公开系统公共参数 $\mathrm{pp} = \{\mathrm{ecc}, h, h_1, \mathrm{KDF}\}$. 值得注意的是, 由于上述参数 $(\mathrm{ecc}, h, \mathrm{KDF})$ 与 SM2 算法相同, 因而支持 SM2 公钥加密算法的设施无需重复, 仅需要添加 $h_1$ 模块.

(2) **KeyGen.** 该算法由用户本地运行. 根据确定的 pp, 用户 $i$ 选择 $\mathrm{sk}_i = d_i \in [1, n-1]$ 作为私钥和计算对应的公钥 $\mathrm{PK}_i = [d_i]G$. 对于现有支持 SM2 公钥加密算法的设施, 用户通常已具有安全的公私钥对, 因而也无需重复执行此算法.

(3) **Encryption.** 该算法由数据发送者执行, 生成支持多接收者解密的密文. 为加密明文 $M$ 给接收者集合 $S_R=(\mathrm{PK}_1,\mathrm{PK}_2,\ldots,\mathrm{PK}_m)$, 发送者执行以下操作:

• 发送者以随机的方式选择 $r\in[1,n-1]$ 并计算获得部分密文 $C_0=[r]G$.

• 发送者利用接收者公钥集合和选定的随机数构造多项式

$$\phi(X)=(X-h_1([r]\mathrm{PK}_1))(X-h_1([r]\mathrm{PK}_2))\cdots(X-h_1([r]\mathrm{PK}_m))+r=\sum_{j=0}^{m}w_jX^j, \tag{3}$$

其中 $(w_0,w_1,\ldots,w_m)\in[1,n-1]$ 表示多项式 $\phi(X)$ 的系数.

• 发送者以 $C_0$ 作为 SM2 方案的 "公钥", 通过调用 SM2 的加密操作产生部分密文 $(C_1,C_2,C_3)\leftarrow \mathrm{SM2}.\mathbf{Enc}\ (\mathrm{pp},C_0,M)$ (详细过程参见 3.3.2 小节). 在本文方案中 SM2 算法被作为安全组件直接调用.

• 发送者获得在 $S_R$ 下的密文 $C=(C_0,C_1,C_2,C_3,\{w_j|j=0,\ldots,m\})$.

(4) **Decryption.** 该算法由数据接收者 $i$ 执行以恢复密文所对应的明文. 为对密文 $C=(C_0,C_1,C_2,C_3,\{w_j|j=0,\ldots,m\})$ 进行解密, 接收者执行以下操作:

• 接收者 $i$ 利用私钥 $\mathrm{sk}_i$ 计算 $x=h_1([\mathrm{sk}_i]C_0)=h_1([d_i][r]G)=h_1([r]\mathrm{PK}_i)$.

• 接收者利用多项式系数 $\{w_j|j=0,\ldots,m\}$ 计算当 $X=x$ 时, 多项式 $\phi(X)$ 的值 $\phi(x)=\sum_{j=0}^{m}w_jX^j$. 根据 $\phi(X)$ 的构造过程可知, $x$ 是 $\phi(X)-r=0$ 的根, 从而 $\phi(x)=r$.

• 接收者设置 $r$ 为 SM2 方案的 "私钥" 和 $C^*=(C_1,C_2,C_3)$ 为对应的 SM2 密文, 并将它们分别作为 SM2 解密操作的输入. 最后通过调用 SM2 的解密操作恢复明文 $M/\perp\leftarrow \mathrm{SM2}.\mathbf{Dec}(\mathrm{pp},r,C^*)$.

根据上述过程可知, 本文所构造的基于 SM2 的公钥广播加密方案保留了完整的 SM2 算法, 因而可通过简单地升级现有支持 SM2 的设备达到消息安全广播的目的.

### 4.2 方案正确性

方案的正确性基于 SM2 公钥加密算法的正确性. 基于 SM2 的加密操作描述, 如果将 $C_0=[r]G$ 作为 "公钥", SM2 可生成在 "公钥" $C_0$ 下的密文 $(C_1,C_2,C_3)$. 为此, 接收者仅需正确计算 "公钥" $C_0$ 对应的 "私钥" $r$, 并通过调用 SM2 解密操作就可正确解密. 根据多项式系数 $\{w_j|j=0,\ldots,m\}$, 接收者可完整恢复多项式 $\phi(X)$. 又根据多项式 $\phi(X)$ 的构造方法可知, $(h_1([r]\mathrm{PK}_1),\ldots,h_1([r]\mathrm{PK}_m))$ 是方程 $\phi(X)-r=0$ 的根. 因此, 对于合法的接收者 $\mathrm{PK}_i\in S$, 其可利用私钥 $\mathrm{sk}_i$ 计算

$$x=h_1([\mathrm{sk}_i]C_0)=h_1([\mathrm{sk}_i][r]G)=h_1([r][\mathrm{sk}_i]G)=h_1([r]\mathrm{PK}_i), \tag{4}$$

进而通过系数 $\{w_j|j=0,\ldots,m\}$ 可计算 $\sum_{j=0}^{m}w_jx^j=\phi(x)=r$. 至此, 接收者 $i$ 正确恢复 "公钥" $C_0$ 对应的私钥 $r$, 并可通过调用 SM2 的解密操作正确解密密文 $(C_1,C_2,C_3)$, 其中恢复明文的正确性基于 SM2 公钥加密算法的正确性. 然而, 由于非授权接收者无法计算 $\phi(X)-r=0$ 的根以及难以正确得到 "公钥" $C_0$ 对应 $r$, 因而无法正确解密.

综上, 授权多个接收者 $S_R=(\mathrm{PK}_1,\mathrm{PK}_2,\ldots,\mathrm{PK}_m)$ 基于正确的信息 (系统参数、密文等) 可利用其私钥 $\mathrm{sk}_i$ 正确解密密文获得对应明文消息, 而非授权接收者 $\mathrm{PK}\notin S_R$ 无法正确解密.

## 5 安全性分析

所构造方案依赖的安全哈希函数、密钥派生函数等通过 SM3 算法实现, 因而在安全性证明中不考虑这些工具的安全性. 为安全性证明需要, 在安全模型框架下哈希函数被定义为随机谕言机. 本文方案

的安全性证明与 SM2 公钥加密算法的安全性证明不同 (其基于一般群模型), 主要通过证明密文中非标准 SM2 密文部分不会向非授权接收者泄露有用信息以此辅助破解正确的 SM2 密文 (即 $C_1, C_2, C_3$). 由于所构造方案生成消息的密文可分为两部分: (1) 由 SM2 生成的标准密文 $(C_1, C_2, C_3)$; (2) 辅助授权接收者恢复应用到 SM2 解密操作中 "私钥" 的密文 $(C_0, w_0, \ldots, w_m)$. 由于该密文为标准的 SM2 密文, 基于 SM2 的安全性可确保敌手在无额外信息辅助的情况下是难以获得明文信息. 因此, 本文方案的安全性等同于 SM2 公钥加密算法的安全性, 其中规约过程依赖于 $m$-CDH 假设.

**定理1** 如果 $m$-CDH 困难问题成立, 则基于 SM2 的公钥广播加密方案的安全性与国产密码 SM2 相同.

**证明** 首先假设 IND-sPK-CCA 游戏中存在攻击者 $\mathcal{A}$ 以无法忽略的优势 $\epsilon$ 打破本文所构造方案. $\mathcal{C}$ 通过与 $\mathcal{A}$ 交互, 试图借助攻击者的能力以难以被忽略的概率攻破 $m$-CDH 问题. 为此, 挑战者 $\mathcal{C}$ 将 $m$-CDH 问题实例 $(G, [x]G, [y_1]G, \ldots, [y_m]G)$ 嵌入到与攻击者 $\mathcal{A}$ 交互过程中. 通过借助攻击者打破所构造方案的能力解决困难问题. 具体交互过程如下.

• **初始化阶段.** $\mathcal{A}$ 与 $\mathcal{C}$ 选择集合 $S_R^* = (\mathrm{PK}_1^* = [y_1]G, \ldots, \mathrm{PK}_m^* = [y_m]G)$ 作为公钥集合. $\mathcal{C}$ 选择并发送 ecc 等公开参数, 其中将哈希函数 $h_1$ 功能通过哈希询问实现.

• **哈希询问.** 在任何阶段 $\mathcal{A}$ 均可发起哈希询问以获得相应的哈希值, 并假设 $\mathcal{A}$ 最多发起 $q_{h_1}$ 次哈希询问. 为响应攻击者询问, $\mathcal{C}$ 需构建并维护形如 $(R \in \mathbb{G}, r \in [1, n])$ 的元组列表 $L$. 列表 $L$ 开始被设置为空, 用于记录 $\mathcal{A}$ 所有查询以及对应的响应值. 对于第 $i$ 次询问 $R_i \in \mathbb{G}$, 如果列表 $L$ 中存在对应的响应值 $r_i$, 则直接返回 $r_i$ 作为响应; 否则, $\mathcal{C}$ 选择随机数 $r_i \in [1, n]$ 和设置 $h_1(R_i) = r_i$ 作为响应值. 最后, $\mathcal{C}$ 将二元组 $(R_i, r_i)$ 插入到列表 $L$ 中.

• **询问阶段 1.** $\mathcal{A}$ 向 $\mathcal{C}$ 发起以下询问, 具体过程如下:

(1) 公钥询问. 挑战者 $\mathcal{C}$ 构建并维护由公、私钥对 $(\mathrm{PK}, \mathrm{sk}_i)$ 组成的列表 PL. 如果攻击者询问的第 $i$ 个公钥已经存在列表 PL, 则挑战者 $\mathcal{C}$ 直接通过查表返回公钥 PK; 否则, 挑战者 $\mathcal{C}$ 选择随机数 $\mathrm{sk}_i \in [1, n]$ 作为私钥, 计算 $\mathrm{PK}_i = [\mathrm{sk}_i]G$ 作为公钥返回给攻击者 $\mathcal{A}$. 同时, 挑战者 $\mathcal{C}$ 更新列表 PL.

(2) 解密询问. $\mathcal{A}$ 询问选择公钥集合 $S_R$ 对应的密文 $C$, 其中 $S_R \cap S_R^* = \emptyset$. $\mathcal{C}$ 根据列表 PL 选择公钥 $\mathrm{PK} \in S$ 对应的私钥 sk 作为 SM2 解密操作 **Decryption** 的输入, 并将解密结果返回给 $\mathcal{A}$.

• **挑战阶段.** 当上述阶段结束后, $\mathcal{A}$ 选择长度相同的挑战消息 $(M_0, M_1) \in \{0,1\}^*$ 发送给 $\mathcal{C}$. $\mathcal{C}$ 选择 $b \in \{0,1\}$ 和利用挑战公钥集合 $S_R^*$ 按照如下方式产生 $M_b$ 的挑战密文:

$$C^* = (C_0^* = [x]G, C_1^*, C_2^*, C_3^*, \{w_j^* | j = 0, \ldots, m\}), \tag{5}$$

其中 $(C_1^*, C_2^*, C_3^*)$ 是通过调用 SM2 的加密操作 (SM2.**Enc**) 生成的在 "公钥" $C_0^*$ 的标准 SM2 密文. 同时, $\{w_j^* | j \in [0, m-1]\}$ 是选择的随机数和 $w_m^*$ 的值设置为 1. 根据所构造方案描述, $\{w_j^* | j = 0, \ldots, m\}$ 暗含应当满足 $(h_1([xy_1]G), \ldots, h_1([xy_m]G))$ 满足

$$\begin{cases} \prod\limits_{j=1}^{m} h_1([xy_j]G) + x = w_0^*, \\ \sum\limits_{j=1}^{m} \dfrac{w_0^*}{h_1([xy_j]G)} = w_1^*, \\ \cdots \\ 1 = w_m^*. \end{cases} \tag{6}$$

在攻击者视图中, $\{w_j^*|j=0,\ldots,m\}$ 是通过计算 $\phi(x)=(X-h_1([xy_1]G))(X-h_1([xy_2]G))\cdots(X-h_1([xy_m]G))+x$ 获得的多项式系数.

• **询问阶段 2.** $\mathcal{A}$ 可继续发起类似询问阶段 1 的公钥与解密询问, 但要求是 $\mathcal{A}$ 不能对 $C^*$ 进行解密询问.

• **猜测阶段.** 当询问终止后, 攻击者 $\mathcal{A}$ 通过获得的信息, 给出对 $b$ 的猜测 $b'\in\{0,1\}$. 当且仅当 $b=b'$ 时, $\mathcal{A}$ 本游戏中获胜.

根据上述描述, 如果攻击者 $\mathcal{A}$ 未对 $\{[xy_j]G\in\mathbb{G}|j\in[1,m]\}$ 进行过哈希询问, 则 $(h_1([xy_1]G),\ldots,h_1([xy_m]G))$ 在攻击者 $\mathcal{A}$ 视图下是随机分布的. 对于攻击者 $\mathcal{A}$ 来说, $C^*$ 是基于 SM2 的公钥广播加密方案生成的合法密文. 同时, 由于 $(C_0^*,\{w_j^*|j=0,\ldots,m\})$ 对于攻击者 $\mathcal{A}$ 是随机的, 而 $(C_1^*,C_2^*,C_3^*)$ 又是通过调用 SM2 的加密操作生成的标准 SM2 密文. 攻击者 $\mathcal{A}$ 在获得 $(C_0^*,\{w_j^*|j=0,\ldots,m\})$ 后对破解密文 $(C_1^*,C_2^*,C_3^*)$ 没有任何优势, 因而仅以 $\frac{1}{2}$ 的概率获胜. 然而, 如果 $\mathcal{A}$ 对任意 $\{[xy_j]G\in\mathbb{G}|j\in[1,m]\}$ 进行过哈希询问, 则可以根据列表 $L$ 构造正确的 $\{w_j^*|j=0,\ldots,m\}$ 使得等式 (6) 成立. 对于攻击者 $\mathcal{A}$, 挑战密文 $C^*$ 是由本文所构造方案生成的标准密文, 以及 $\mathcal{A}$ 攻破方案的概率为 $\epsilon$, 因而其可以以 $\epsilon$ 的概率产生正确的猜测. 这意味着 $\mathcal{A}$ 能以无法被忽略的优势 $(\epsilon-\frac{1}{2})$ 获胜. 由于 $\mathcal{A}$ 最多可进行 $q_{h_1}$ 次, 挑战者 $\mathcal{C}$ 在列表 $L$ 中选择一个 $R\in\mathbb{G}$ 等于 $[xy_j]G$ 的概率是 $\frac{1}{q_{h_1}}$, 而 $[xy_j]G$ 是 $m$-CDH 困难问题的一个解. 也就是说, 如果攻击者 $\mathcal{A}$ 能以 $\epsilon$ 的概率获胜, 则挑战者 $\mathcal{C}$ 可以 $\epsilon\frac{1}{q_{h_1}}$ 破解 $m$-CDH 问题.

## 6 方案性能分析

本节从理论分析和实验评测两方面对本文所设计方案进行分析, 并通过与同类型方案 [5,7,34] 比较来呈现本文方案的特征. 同类型方案作为对比方案, 方案 [5,7,34] 被选择的原因主要包括: (1) 功能类似, Tan 等 [34] 和 Li 等 [7] 设计的方案均避免了密钥托管问题, 使得所设计方案不同于现有大多数基于身份的广播加密方案; (2) Lai 等 [5] 和本文所设计方案均是基于 SM2 公钥加密算法设计.

### 6.1 理论分析

首先, 从公开参数大小 (public parameters)、发送者密钥大小 (keys) 和密文大小 (ciphertexts) 3 方面评估方案的存储与通信开销 (对比结果如表 2 所示). 让 |ml|, $|\mathbb{G}_1|^*$, $|\mathbb{G}_T|^*$, $|\mathbb{G}_1|$ 分别表示消息, 群 $\mathbb{G}_1$, $\mathbb{G}_T$ 元素, 无双线性对运算的群 $\mathbb{G}_1$ 元素的长度. 让 $m$, $|q|$, $|N|$ 分别表示接收者个数、群 $\mathbb{G}_1$ 阶、$\prod_{i=1}^m p_i$ 的值. 让 $p_i=2q_i+1\geqslant 2q+1$ 且 $q_i$ 为素数. 从表 2 可以看出, 本文方案具有如下特征: (1) 方案的公开参数是定长的, 其大小与接收者数量 $m$ 无关; (2) 方案中接收者存在的密钥仅为一个大整数, 大小为 $|q|$ (方案 [34] 中为 $2|q|$, 方案 [7] 中为 $6|q|$); (3) 方案的密文大小与接收者数量 $m$ 相关, 但与消息的长度 |ml| 无线性关系, 大小为 $2|\mathbb{G}_1|+|\text{hl}|+|\text{ml}|+m|q|$ (方案 [5] 中密文大小与接收者数量 $m$ 和消息长度 |ml| 呈线性相关).

在存储开销方面, 本文方案与方案 [5] 相同且小于方案 [7,34]. 在通信方面, 本文方案和方案 [7,34] 的开销为 $(O(m|q|))$, 而方案 [5] 开销为 $O(m|\text{ml}|)$. 也就是说, 如果 $|\text{ml}|<|q|$, 则方案 [5] 优于其他方案; 而 |ml| 远大于 $|q|$, 则本文方案略优于其他方案.

方案各算法的计算开销可通过其主要操作耗时进行理论评估. 表 3 呈现了各算法的主要操作, 未统计计算开销较低的运算, 如哈希运算. 令 $e$, $Et$ 表示双线性对和群 $\mathbb{G}_T$ 上指数运算的时间开销, $\text{SM}^*$, SM 分别表示在有无双线性对的群 $\mathbb{G}_1$ 的标量乘运算的时间开销, $\text{ME}_p$, MI, $\text{ME}_N$ 则分别表示不同模数下的模乘运算、模指数运算和模逆运算的时间开销.

**表 2 存储与通信开销比较**

**Table 2** Comparisons with BE schemes in storage and communication costs

| Schemes | Public parameters | Keys | Ciphertexts |
|---|---|---|---|
| Tan et al. [34] | $2\|N\|+3m\|q\|$ | $2\|q\|$ | $2\|p\|\|q\|+2m\|q\|+\|\mathrm{ml}\|$ |
| Li et al. [7] | $2\|\mathbb{G}_1\|^*+\|\mathbb{G}_T\|^*+m\|q\|$ | $6\|q\|$ | $\|N\|+m\|\mathbb{G}_1\|^*+\|\mathrm{ml}\|$ |
| Lai et al. [5] | $\|\mathbb{G}_1\|$ | $\|q\|$ | $\|\mathbb{G}_1\|+m(\|\mathrm{ml}\|+\|\mathrm{hl}\|)$ |
| Our | $\|\mathbb{G}_1\|$ | $\|q\|$ | $2\|\mathbb{G}_1\|+\|\mathrm{hl}\|+\|\mathrm{ml}\|+m\|q\|$ |

**表 3 方案计算开销比较**

**Table 3** Comparisons with BE schemes in computation costs

| Schemes | Setup | KeyGen | Encryption | Decryption |
|---|---|---|---|---|
| Tan et al. [34] | – | $6\mathrm{ME}_p$ | $(3m+2)\mathrm{ME}_N$ | $4\mathrm{ME}_p+\mathrm{MI}$ |
| Li et al. [7] | $e+\mathrm{SM}^*$ | $\mathrm{ME}_p+\mathrm{SM}^*$ | $2m\mathrm{SM}^*+m\mathrm{ME}_N$ | $e+\mathrm{ME}_p+Et+\mathrm{MM}_p$ |
| Lai et al. [5] | – | SM | $m\mathrm{SM}$ | SM |
| Ours | – | SM | $(m+2)\mathrm{SM}+\frac{m(m+1)}{2}\mathrm{MM}_p$ | $\mathrm{SM}+m\mathrm{MM}_p$ |

在初始化算法中, 方案 [7] 除确定基础参数之外, 还需要进行一次双线性对运算和标量乘运算, 导致其计算开销要高于其他方案. 在密钥生成算法中, 本文方案与方案 [5] 均只需要在无双线性对群 $\mathbb{G}_1$ 中执行一次标量乘运算 SM, 因而要优于方案 [7,34]. 在加密算法中, 所有方案的加密算法计算开销均与接收者数量 $m$ 有关. 方案 [5] 通过重复执行 SM2 公钥加密算法产生密文, 仅需要执行 $m$ 次标量乘运算 SM, 其计算开销最低. 本文方案需要 $(m+3)\mathrm{SM}+\frac{m(m+1)}{2}\mathrm{MM}_p$, 因而在群组大小适中的情况 (如 $m\leqslant 128$) 能够表现更优的性能. 在解密算法中, 本文方案除直接调用 SM2 解密算法算法外, 还需要进行阶为 $m$ 的多项式求值运算, 因而计算开销与 $m$ 相关 ($\mathrm{SM}+m\mathrm{MM}_p$), 并且略高于方案 [5]. 总体而言, 本文方案在计算性能方面略低于方案 [5], 但优于方案 [7,34]. 本文通过牺牲一定的计算开销, 避免了方案 [5] 中需要为每个用户生成对应消息密文的方法, 从而使得密文的长度与消息的长度无线性关系.

### 6.2 实验评测

为准确评估方案的性能, 本文对方案进行了编程实现, 测试了常用操作的耗时以及本方案中各个算法的运行时间. 实验中测试设备的核心配置为: 16.0 GB 内存, i5-8250U CPU @ 1.60 GHz 1.80 GHz. 本文实现结果均是多次测量的平均值. 方案实现是基于流行的密码库 Miracl (version 7.0.0.[1)]), 采用的是 2 阶 Tate 双线性对超奇异曲线和 SM2 标准曲线. 为达到 AES-128 比特[2)]安全强度, 各元素比特长度分别为 $|p|=|q|=256$ bits, $|\mathbb{G}_1|^*=|\mathbb{G}_T|^*=3072$ bits, $|\mathbb{G}_1|=512$ bits, $|N|=m|q|$ bits ($N$ 的长度在对比方案 [7,34] 中与接收者数量有关).

基于确定的参数, 可对各个方案的密文大小进行定量分析. 图 1 展现了当传输消息的长度固定时, 各方案密文大小随接收者数量变化情况. 图 2 展现了当接收者数量固定时, 各方案密文大小随消息长度变化情况. 显然, 本文方案具有最好的通信开销 (密文大小最低). 此外, 本文方案随消息长度和接收者数量增加, 密文大小增长速度均低于其他方案, 进而使得方案具有更好的扩展性.

本文测试了不同操作的耗时 (表 4). 基于本文所确定的参数, 双线性对计算耗时 (193.361 ms) 最

1) https//github.com/miracl/MIRACL.

2) 安全性等同于密钥长度为 128 比特的 AES 算法.

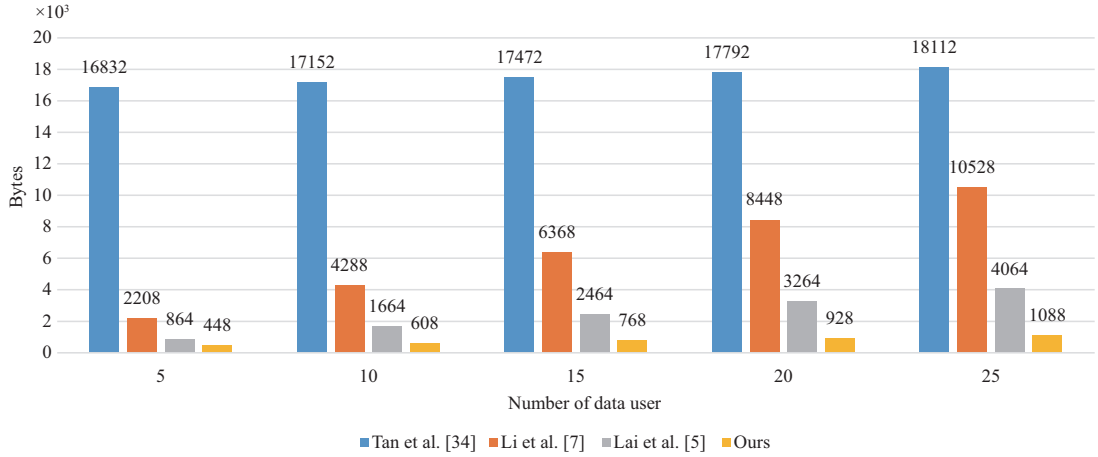


**图 1** (网络版彩图) 密文大小比较 (消息长度固定)

**Figure 1** (Color online) Ciphertext size comparison (|ml|=1024)

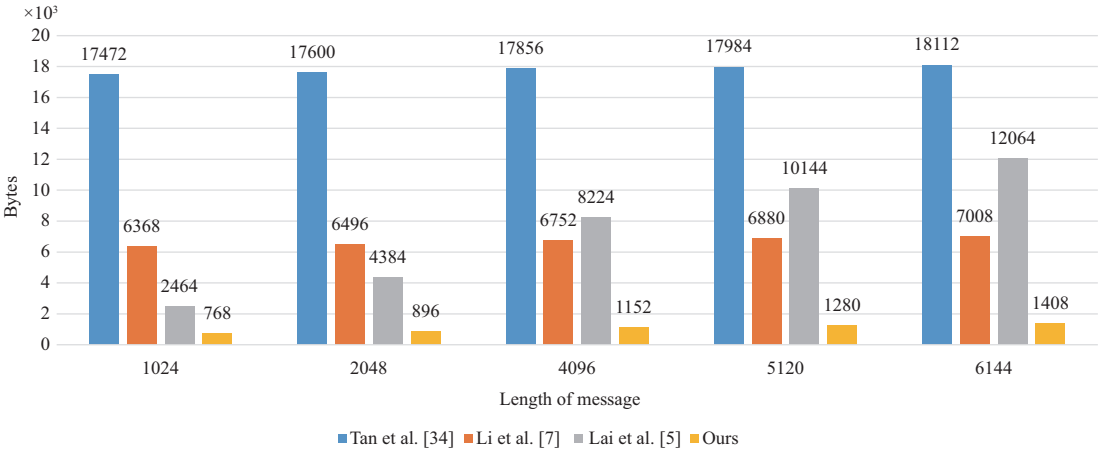


**图 2** (网络版彩图) 密文大小比较 (接收者数量固定)

**Figure 2** (Color online) Ciphertext size comparison ($m = 15$)

大, 其次则是标量乘运算 (支持双线性对, 约为 47.864 ms), 相反的是在 $p$ 下的模乘运算耗时最小 (仅为 0.003 ms). 相比于在无双线性对运算中群 $\mathbb{G}_1$ 的标量乘运算 SM 仅需要 2.861 ms. 值得注意的是, 在 $N$ 下的模指数运算耗时与接收者数量有关, 本文提供的测试数据 7.353 ms 是 $|N| = 1536$ 比特的测试数据 (相当于 $m = 6$). 基于表 3 和 4, 可以对各个方案中不同算法的计算开销进行定量评估. 在接收者数量为 6 的情况下, 方案 [5,7,34] 和本文方案的加密算法分别需要 147.06, 618.486, 17.166, 17.229 ms, 解密算法需要 1.228, 206.495, 2.861, 2.879 ms. 显然, 方案 [5] 和本文方案的加密与解密算法具有较好的计算效率. 主要原因是两个方案仅需在无双线性对群下进行标量乘运算. 值得注意的是, 上述计算的时间只是在理想情况的算法计算开销的估计值, 未考虑其他操作对算法的影响, 算法实际开销会高于上述计算的时间, 但上述数据可在一定程度上反映各个方案计算开销的趋势情况.

同时, 本文完整地测试了密钥产生算法 (KeyGen)、加密算法 (Encryption) 和解密算法 (Decryption) 的计算耗时. 图 3 呈现了本文方案在不同接收者数量下各个算法的计算耗时情况. 对于密钥产

表 4 主要操作耗时 (ms)

**Table 4** Time costs of main operations (ms)

| | $e$ | SM* | SM | Et | $\mathrm{MM}_p$ | $\mathrm{ME}_p$ | $\mathrm{ME}_N$ | MI |
|---|---|---|---|---|---|---|---|---|
| Time costs | 193.361 | 47.864 | 2.861 | 12.864 | 0.003 | 0.267 | 7.353 | 0.016 |

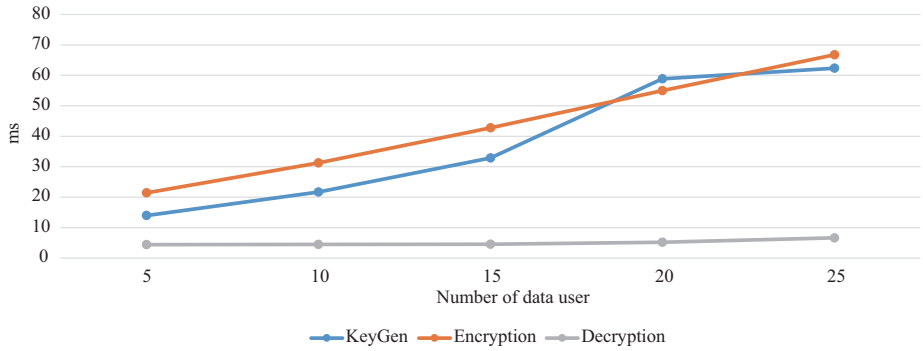


图 3 (网络版彩图) 各算法计算开销

**Figure 3** (Color online) Time costs of each algorithm in our scheme

生算法, 整个系统中密钥产生的计算开销逐渐增加, 然而单个用户的计算开销并不会受影响以及系统加入新用户并不影响其他用户的密钥. 对于加密算法, 完成一次加密所需的时间与接收者数量近似呈线性相关. 主要原因是系统计算的多项式项数与接收者数量相关. 对于解密算法, 其计算耗时受接收者数量影响较小, 其增长趋势相对缓慢. 比如, 算法在接收者数量为 5 时需要 4.402 ms, 而在接收者数量为 25 时仅需要 6.644 ms. 值得注意的是, 实际算法的测试值要略大于上述的评估值, 其主要原因是统计了中间操作的计算开销.

## 7 总结

本文通过结合我国商用密码 SM2 和广播加密的思想, 设计了基于国产密码 SM2 的广播加密, 实现了在多接收者场景中自主可控的安全消息传输. 方案最大化地避免对现有支持 SM2 算法模块的修改, 利用多项式秘密共享方式实现广播加密. 方案无需指定发送者进行数据广播, 以及系统公开参数规模与接收者数量无关. 同时, 方案有效平衡了通信与计算开销, 以牺牲少量的计算代价提升通信效率近 50%, 在实用性方面具有明显提升. 然而, 为最大化保留 SM2 公钥加密算法框架, 本文所提出的方案中密文大小与接收者数量相关, 使得方案在大规模用户场景中应用仍在一定限制. 因此, 未来的研究重点是如何构造密文定长的自主可控广播加密方案.

## 参考文献

1 State Cryptography Administration. GM/T003-2012 Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves. Beijing: Standards Press of China, 2010 [国家密码管理局. GM/T003-2012 SM2 椭圆曲线公钥密码算法. 北京: 中国标准出版社, 2010]

2 Fiat A, Naor M. Broadcast encryption. In: Proceeding of the Annual International Cryptology Conference, 1993. 480–491

3 Wee H. Broadcast encryption with size $N^{1/3}$ and more from k-Lin. In: Proceeding of the Annual International Cryptology Conference, 2021. 155–178

4 Kim J, Camtepe S, Susilo W, et al. Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing. In: Proceeding of the Annual ACM Asia Conference on Computer and Communications Security, Auckland, 2019. 55–66

5 Lai J Z, Huang Z A, Weng J, et al. SM2-based multi-recipient public-key encryption. J Cryptolog Res, 2021, 8: 699–709 [赖俊祚, 黄正安, 翁健, 等. 基于 SM2 的多接收方公钥加密方案. 密码学报, 2021, 8: 699–709]

6 Lai J C, Huang X Y, He D B. An efficient identity-based broadcast encryption scheme based on SM9. Chin J Comput, 2021, 44: 897–907 [赖建昌, 黄欣沂, 何德彪. 一种基于商密 SM9 的高效标识广播加密方案. 计算机学报, 2021, 44: 897–907]

7 Li J G, Zhang Y C, Wei X X. A provably secure certificate-based broadcast encryption scheme. ACTA Electron Sin, 2016, 44: 1101–1110 [李继国, 张亦辰, 卫晓霞. 可证安全的基于证书广播加密方案. 电子学报, 2016, 44: 1101–1110]

8 Li X J, Yuan Y W, Jin C H. An attribute-based broadcast encryption scheme suitable for the broadcasting network. J Comput Res Dev, 2018, 55: 1409–1420 [李学俊, 袁亚文, 金春花. 一种适用于广电网的属性基广播加密方案. 计算机研究与发展, 2018, 55: 1409–1420]

9 Ramanna S C, Sarkar P. Efficient adaptively secure IBBE from the SXDH assumption. IEEE Trans Inform Theor, 2016, 62: 5709–5726

10 Li J G, Yu Q H, Zhang Y C. Identity-based broadcast encryption with continuous leakage resilience. Inf Sci, 2018, 429: 177–193

11 Goyal R, Vusirikala S, Waters B. Collusion resistant broadcast and trace from positional witness encryption. In: Proceeding of the Annual International Workshop on Public Key Cryptography, Beijing, 2019. 3–33

12 Chen L, Li J, Lu Y, et al. Adaptively secure certificate-based broadcast encryption and its application to cloud storage service. Inf Sci, 2020, 538: 273–289

13 Agrawal S, Wichs D, Yamada S. Optimal broadcast encryption from LWE and pairings in the standard model. In: Proceeding of the Annual International Theory of Cryptography Conference, Durham, 2020. 149–178

14 Brakerski Z, Vaikuntanathan V. Lattice-inspired broadcast encryption and succinct ciphertext-policy ABE. In: Proceedings of the 13th Innovations in Theoretical Computer Science Conference, 2020

15 Lai J C, Mu Y, Guo F C, et al. Fully privacy-preserving ID-based broadcast encryption with authorization. Comput J, 2017, 60: 1809–1821

16 Lai J C, Mu Y, Guo F C, et al. Identity-based broadcast encryption for inner products. Comput J, 2018, 61: 1240–1251

17 Ge A J, Wei P W. Identity-based broadcast encryption with efficient revocation. In: Proceeding of the Annual International Workshop on Public Key Cryptography, Beijing, 2019. 405–435

18 Sun Y, Mu Y, Susilo W, et al. Revocable identity-based encryption with server-aided ciphertext evolution. Theor Comput Sci, 2020, 815: 11–24

19 Guo D, Wen Q, Jin Z, et al. Authenticated public key broadcast encryption with short ciphertexts. Multimed Tools Appl, 2019, 78: 23399–23414

20 Xiong H, Zhao Y, Peng L, et al. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing. Future Gener Comput Syst, 2019, 97: 453–461

21 Yi X, Paulet R, Bertino E, et al. Practical anonymous subscription with revocation based on broadcast encryption. In: Proceeding of the IEEE International Conference on Data Engineering, Dallas, 2020. 241–252

22 Jia H, Chen Y, Yang K, et al. Revocable broadcast encryption with constant ciphertext and private key size. Chin J Electron, 2019, 28: 690–697

23 Ge C P, Liu Z, Xia J, et al. Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. IEEE Trans Depend Secure Comput, 2021, 18: 1214–1226

24 Lai J, Guo F, Susilo W, et al. Data access control in cloud computing: flexible and receiver extendable. IEEE Trans Serv Comput, 2021. doi: 10.1109/TSC.2021.3057197

25 Chen L, Li J, Zhang Y. Anonymous certificate-based broadcast encryption with personalized messages. IEEE Trans Broadcast, 2020, 66: 867–881

26 Wang H G, Zhang Y, Chen K F, et al. Functional broadcast encryption with applications to data sharing for cloud storage. Inf Sci, 2019, 502: 109–124

27 Jiang P, Guo F, Mu Y. Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems. Theor Comput Sci, 2019, 767: 51–72

28 Deng H, Qin Z, Wu Q H, et al. Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Trans Inform Forensic Secur, 2020, 15: 3168–3180
29 Zhao Z, Guo F, Lai J, et al. Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. Theor Comput Sci, 2020, 809: 73–87
30 Zhu Y, Yu R Y, Chen E, et al. Dual-mode broadcast encryption. Sci China Inf Sci, 2018, 61: 118101
31 Li J, Chen L, Lu Y, et al. Anonymous certificate-based broadcast encryption with constant decryption cost. Inf Sci, 2018, 454: 110–127
32 Canard S, Phan D H, Pointcheval D, et al. A new technique for compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption. Theor Comput Sci, 2018, 723: 51–72
33 Chhatrapati A, Hohenberger S, Trombo J, et al. A performance evaluation of pairing-Based broadcast encryption systems. In: Proceedings of the 20th International Conference on Applied Cryp- tography and Network Security, 2021
34 Tan Z W, Liu Z J, Xiao H G. A fully public key tracing and revocation scheme provably secure against adaptive adversary. J Softw, 2005, 16: 1333–1343 [谭作文, 刘卓军, 肖红光. 一个安全公钥广播加密方案. 软件学报, 2005, 16: 1333–1343]

# An efficient public-key broadcast encryption scheme based on SM2

Biwen CHEN[1,2,4], Tao XIANG[1*], Debiao HE[2] & Xinyi HUANG[3]

1. *College of Computer Science, Chongqing University, Chongqing* 400044*, China*;
2. *School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072*, China*;
3. *Computer and Cyber Security, Fujian Normal University, Fuzhou* 350117*, China*;
4. *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin* 541004*, China*
* Corresponding author. E-mail: txiang@cqu.edu.cn

**Abstract** Because of the increasing frequency of cyber-attacks and data breaches, network security has received a large emphasis from the related departments. Therefore, the development of national cryptographic algorithms not only conforms to the needs of building an internet superpower but also guarantees healthy and secure application development. The SM2 is a domestically designed commercial cryptographic algorithm that guarantees the confidentiality of data during data transmission. The SM2 encryption algorithm is suitable for one-to-one communication scenarios but incurs large repetitive computation and communication costs when applied to one-to-many communication scenarios. To enhance the performance and expand the application areas of the SM2, this paper combines the ideas of the SM2 encryption algorithm and broadcast encryption and defines the first public key broadcast encryption based on SM2 by leveraging the Diffie-Hellman key exchange and polynomial-based secret share scheme. Specifically, the proposed scheme keeps the original SM2 framework as much as possible and achieves an independent and controllable information transformation by simply upgrading the communication facilities with SM2. Compared with existing broadcast encryption schemes, the designed scheme has constant-size public system parameters and does not need to specify a broadcaster to send messages. Additionally, the designed scheme has the same security as the SM2, and evaluation and performance tests demonstrate its practicality.

**Keywords** publi-key encryption, SM2 public key cryptography, broadcast encryption, Diffie-Hellman key exchange