# 基于 SM9 的匿名广播加密方案

崔 岩[1], 黄欣沂[1], 赖建昌[1], 何德彪[2], 程朝辉[3]

[1]福建师范大学 计算机与网络空间安全学院 福州 中国 350007
[2]武汉大学 国家网络空间安全学院 武汉 中国 430072
[3]深圳奥联信息安全科技有限公司 深圳 中国 518000

**摘要** 广播加密允许数据拥有者通过不安全的公开信道将数据安全地发送给一组指定的用户, 只有组内用户（授权用户）利用自身私钥才能正确解密密文, 恢复出明文数据, 不在组内的用户（非授权用户）即使合谋也无法获取数据内容。标识加密是一种非对称加密体制, 可利用能够唯一标识用户身份的任意字符串作为用户的公钥, 消除了传统公钥体制中用于绑定用户公钥的证书。匿名标识广播加密不仅能充分继承标识加密的优点实现多用户数据的安全共享, 而且能有效保护接收者的身份信息。本文以国产商用标识密码算法 SM9 为基础, 采用多项式技术构造了首个基于 SM9 的匿名广播加密方案。方案具有与 SM9 加密算法相同的私钥生成算法, 用户私钥由一个群元素组成。方案的密文由($n$+3)个元素组成, 与接收者数量($n$)线性相关, 解密仅包含一次双线性对计算。基于 $q$ 类型的 GDDHE 困难假设, 在随机谕言器模型中证明方案在静态选择明文攻击下具有不可区分的安全性且满足接收者匿名性。比较分析表明本文方案的计算开销和通信代价与现有高效匿名标识广播加密方案是可比的。最后, 对方案进行编程实验, 在相同安全级别下, 本文方案对比其他方案具有较优的密文长度, 实验结果表明本文方案是可行的。

**关键词** 广播加密; SM9; 匿名性; 选择明文安全
**中图法分类号** TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.11.02

# Anonymous Broadcast Encryption Based on SM9

CUI yan[1], HUANG Xinyi[1], LAI Jianchang[1], HE Debiao[2], CHENG Zhaohui[3]

[1] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China
[2] School of Cyber Science and Engineering, Wuhan University, Wuhan 430072 China
[3]Olym Information Security Technology Ltd., Shenzhen 518000 China

**Abstract** Broadcast encryption allows a data owner to share a data with a group of designated users simultaneously by generating a single ciphertext via an insecure public channel. Every one listening to the public channel can download the ciphertext. But only the chosen users are able to decrypt the ciphertext successfully and then recover the plaintext. While users who are not in the group, namely the unauthorized users, learn nothing about the broadcast message even they collude. Identity-based encryption is a special asymmetric encryption system, in which the public key of a user can be any string that can uniquely identify his/her identity. It efficiently eliminates the certificate appeared in the traditional public key cryptosystem which is used to guarantee the validity of user's public key. Anonymous identity-based broadcast encryption inherits the merit of identity-based encryption and broadcast encryption. It not only can securely share data with multiple users, but also can protect the privacy of receivers. In this paper, we proposed the first anonymous identity-based broadcast encryption scheme based on the Chinese standard SM9 by using the technology of polynomials. The user private key generation is the same as the SM9 identity encryption algorithm, which consists of one group element. The size of the ciphertext is linear in the number of receivers for one encryption. More precisely, it contains $n$+3 elements. The decryption includes one pairing operation only. Based on $q$ type GDDHE assumptions, we prove that the proposed scheme is secure against selective identity and chosen-plaintext attacks and satisfies anonymity of receivers in the random oracle model. The theoretical analysis shows that the proposed scheme is comparable to the existing efficient anonymous identity-based broadcast encryption schemes in terms of the computational cost and communication overhead. Finally, we demonstrate our proposed scheme by programming. The demonstration shows that in the same security level, our proposed scheme has shorter ciphertext length and is feasible.

**通讯作者：** 黄欣沂, 博士, 教授, Email: xyhuang@fjnu.edu.cn。

本课题得到国家自然科学基金 (No. 61902191, No. 62032005, No. 61972294, No. 61972094)、江苏省自然科学基金(No. BK20190696)、福建省科技厅科学基金(No. 2020J02016)、山东省重点研发计划(No. 2020CXGC010115)、深圳市科技研发资金(No. JSGG20201102170000002)、广东省重点领域研发计划(No. 2020B1111410001)资助。
收稿日期: 2022-03-24; 修改日期: 2022-05-13; 定稿日期: 2023-09-02

**Key words** broadcast encryption; SM9; anonymity; CPA

# 1 引言

广播加密(broadcast encryption, BE)[1]是一种多用户安全数据共享技术, 允许数据拥有者（加密者）通过不安全信道发送同一个数据给多个用户。数据发送方首先选定一组接收者, 将明文数据加密后广播到某一公开信道, 任何收听此信道的用户均可获取密文数据。然而, 只有在接收者集合 $S$ 内的用户才能通过自己的解密密钥正确解密获得明文, 不在 $S$ 内的任何用户则无法正确解密, 即使 $S$ 外的所有用户进行合谋。与多次重复使用点对点加密方式相比, 广播加密能有效提高加密效率和通信效率。广播加密目前在付费电视订阅服务、无线传感网、云存储的访问控制等应用中广泛使用, 实现多用户安全数据访问。

文献[2]中采用门限秘密共享的方法, 首次给出了基于公钥的 BE 方案。然而基于传统公钥的密码体制在实际应用中需要引入证书, 以保证每个用户的信息和公钥一一对应, 进而确保用户公钥具有真实性和有效性。但证书的引入不得不考虑证书传输的通信代价以及证书验证的计算代价。为消除证书, Shamir 提出标识（身份）密码体制(identity-based cryptosystem, IBC) [3]。可将邮件地址、电话号码或社保号码等能唯一标识用户的字符串作为用户公钥。Delerablée[4]于 2007 年提出第一个具有定长密文和密钥的标识广播加密(identity-based broadcast encryption, IBBE)方案, 且利用随机谕言模型证明方案在选择明文攻击下(chosen plaintext attack, CPA)具有不可区分性。随后, 标识广播加密得到了积极的研究[5-9]。

匿名性是密码学研究的一个重要性质, 比如在区块链应用中需要有效保护用户的隐私。上述广播加密方案在解密时都需要以所有接收者的标识信息为输入, 因此不能有效保护接收者的隐私。在一些特殊应用中, 比如广播订阅, 一些敏感广播的订阅者并不希望其他订阅者知道他所订阅的频道。因此, 匿名性也是广播加密的一个重要安全需求。如何在广播加密过程中实现接收者匿名性在文献[10]中首次得到研究。为保护接收者的标识信息, Barth 提出私有广播加密发概念, 并给出了一个满足选择密文攻击安全(chosen ciphertext attack, CCA)的私有广播加密方案通用构造。具有匿名性质的广播加密在文献[11-13]得到进一步研究。

SM9 标识密码是我国自主研发的基于椭圆曲线的密码算法, SM9 全系列算法现已成为国家标准, 且被纳入 ISO/IEC 国际标准。自 SM9 标识密码提出后, 得到了国内学者积极的研究, 取得了一系列的研究成果[14-20]。最近, 赖建昌等[9]基于 SM9 密钥封装算法提出了首个基于 SM9 的广播加密方案, 方案在随机谕言模型下可证明是 CPA 安全的。但密文解密需要输入所有接收者的标识信息, 无法实现匿名性。目前在密码学主流期刊和会议上未发现基于 SM9 的匿名广播加密的研究成果发表。

本文的主要贡献包括 3 个方面:

1) 本文借鉴文献[13]的设计思路, 以 SM9 标识加密算法架构为基础, 利用多项式技术, 构造了首个基于 SM9 的匿名广播加密方案, 实现多用户数据匿名安全共享。保护数据安全的同时能有效保护接收者的身份信息。

2) 用户私钥长度由定长的一个群元素构成, 系统公钥长度为 $O(m)$, 密文长度为 $O(n)$, 其中 $m$ 表示系统可容纳的最大接收者（授权用户）个数; $n$ 表示一次广播加密中实际的接收者个数。与使用 SM9 加密算法生成 $n$ 个会话密钥, 再利用会话密钥加密消息生成 $n$ 段密文实现的匿名广播加密方式相比, 本文方案的密文长度有明显优势, 且任何用户在解密过程中仅包含一个双线性对计算, 具有较高的解密效率。通过比较分析, 结果表明方案的计算开销和通信代价与现有高效匿名标识广播加密方案也是可比的。

3) 在随机谕言模型下, 证明方案在静态选择明文攻击下满足不可区分性和匿名性, 方案的安全性依赖于 $q-$ GDDHE 假设的困难性。

# 2 相关工作

本节将围绕安全性、效率、IBBE 拓展研究以及 SM9 算法, 描述公钥广播加密和 SM9 算法研究进展。

**安全性:** 选择密文攻击安全是公钥加密方案的理想安全概念, 在广播加密中可抵抗一些有能力篡改广播密文的主动攻击者。而选择明文攻击安全的安全性则较弱一些。广播加密作为多用户数据共享方案, 还需考虑的重要安全问题是抗合谋攻击, 以确保非授权用户不能通过盗版“解密盒”解密广播密文, 其中该“解密盒”可能通过授权用户利用自己的私钥通过合谋生成。

Boneh 等在文献[21]中利用双线性对技术提出首个完全抗合谋(fully collusion resistant)攻击的广播加密方案。Gentry 和 Waters[22]提出具有抵抗自适应性选择明文攻击安全的标识广播加密方案。Kim 等[6]利用对偶加密(dual system encryption)技术提出一个

自适应(adaptive)选择密文安全的 IBBE 方案。刘潇等[7]通过引入虚拟标识, 提出一个具有静态(selective)选择密文安全的 IBBE 方案, 要求敌手在发起攻击之前确定要攻击的身份。

上述广播加密方案均未考虑保护用户隐私问题, 解密过程需要输入所有接收者的身份信息, 然而在某些特殊应用中, 接收者并不希望暴露自己的身份信息。Barth、Boneh 和 Waters 在文献[10]中首次考虑保护广播加密中接收者隐私, 给出了一个具有 CCA 安全的私有广播加密方案的通用构造, 能够保证在不泄露接收者身份信息的情况下正确解密。Fazio 和 Perera[11]提出的基于子集覆盖(subset-cover)技术的 IBBE 方案中, 用户的标识以接收者集合 $S$ 外的用户视角来看是匿名的, 但对于 $S$ 内的用户不满足匿名性。因此, 该方案仅满足外部匿名性。Libert 等[12]指出文献[11]中的匿名性较弱, 无法满足完全匿名性, 于是给出了匿名标识广播加密(anonymous identity-based broadcast encryption, AIBBE)的形式化定义, 并提出两个具有 CCA 安全的匿名标识广播加密的一般构造。He 等[13]采用多项式技术提出了一种具有自适应 CCA 安全的匿名标识广播加密方案。

**效率:** Boneh 等在文献[21]提出了两种高效的公钥广播加密方案, 第一种构造中密文的大小是恒定的。然而, 系统公共参数的长度和解密代价分别随着广播系统中的最大接收机数量和当前目标接收机的数量呈线性增长。在第二种构造中, 系统公共参数和密文的大小以及解密成本都与最大接收器数量呈次线性关系, 是目前最有效的方案之一。Delerablée[4]于 2007 年提出第一个具有定长私钥、定长密文的 IBBE 方案, 消除了传统公钥体制中的证书。刘潇等对文献[4]中的方案进行优化, 在不增加密文长度的情况下使其满足 CCA 安全。Boneh 和 Hamburg[5]使用分层标识加密技术构造了首个具有短密文的分层标识广播加密方案, 密文由三个元素组成。Libert 提出的 AIBBE 方案是将多次对称加密形成多个密文来实现匿名广播加密, 通信代价和解密计算开销较大。目前匿名广播加密方案还不能达到常数级的密文长度。

**IBBE 拓展研究:** 文献[8]把内积加密技术融合到广播加密系统中, 提出一个解密结果不是明文的内积型 IBBE 方案, 其解密结果为一个与用户私钥和明文数据关联的内积值, 可用于数理统计等应用场景。Zhao 等[23]提出具有定长私钥、定长密文的可问责 IBBE 方案。Lai 等[24]提出一种可撤销的 AIBBE 方案, 可实现无需进行解密并撤销接收者集合中部分用户的解密权限。

**SM9 算法研究现状:** 随着 2016 年国家密码管理局发布了 SM9 密码算法, SM9 密码得到了积极的研究。Cheng[14]基于随机谕言模型, 给出了 SM9 密钥协商协议、密钥封装机制和公钥加密算法的安全性分析。文献[25]针对 SM9 配对运算中的 Miller loop 计算过程提出优化方案, 提出提高 BN 曲线上函数计算效率的方法, 提升了 SM9 双线性对运算的效率。Zhang 等在文献[26]中分析了针对 SM9 算法的 3 种侧信道攻击方法并给出了具体防御方案。文献[27]中融合签名和加密技术, 提出了基于 SM9 的高效标识签密方案, 在适应性选择消息和标识攻击模型下证明了方案满足抗伪造性, 且能够抵抗选择密文攻击。Lai 等[9]提出基于 SM9 的高效广播加密方案, 密文长度只有三个元素, 与接收者数量无关。目前有关基于 SM9 的匿名广播加密研究尚未发现。

## 3 预备知识

本节简要回顾双线性群、基于标识的匿名广播加密以及安全模型和困难问题假设等基础知识, 首先给出可忽略函数的定义。

令$|\mathbb{N}|$为自然数集合, 对于任意 $d \in N$, 若存在 $\lambda_d \in \mathbb{N}$, 使得对于任意$\lambda > \lambda_d$, $\varepsilon(\lambda) \leqslant \lambda^{-d}$始终成立。那么函数$\varepsilon: N \to [0,1]$称为可忽略函数。

### 3.1 双线性群

设$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$是阶为 $p$ 的循环群, $p$ 为素数, $P,Q$ 分别为群$\mathbb{G}_1,\mathbb{G}_2$的生成元, 双线性映射 $e:\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 满足: 1) 对任意的 $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ 和 $a,b \in \mathbb{Z}_p^*$, 有 $e(aP,bQ) = e(P,Q)^{ab}$; 2) 存在 $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$, 满足 $e(P,Q) \neq 1$; 3) 对于任意 $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$, 存在能够在多项式时间内计算出 $e(P,Q)$的算法。双线性群 $\mathcal{BP}$ 由 $(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e(\cdot,\cdot))$构成。SM9 标识密码算法利用非对称双线性群构造, 即: $\mathbb{G}_1 \neq \mathbb{G}_2$。

### 3.2 匿名标识广播加密

AIBBE 方案由以下四个可在多项式时间内计算出的算法组成(Setup, KeyGen, Encrypt, Decrypt):

1) $\boldsymbol{Setup}(1^\lambda, m) \to (mpk, msk)$: 输入安全参数λ和系统可容纳的最大接收者个数 $m$, 密钥生成中心(key generator center, KGC)运行 $\boldsymbol{Setup}$ 算法, 输出系统主私钥 $msk$、系统主公钥 $mpk$。KGC 秘密保存系统主私钥, 公开系统主公钥。

2) $\boldsymbol{KeyGen}(mpk, msk, ID) \to sk_{ID}$: 输入系统主公钥 $mpk$, 主私钥 $msk$, 用户标识 $ID$, KGC 运行 $\boldsymbol{KeyGen}$ 算法生成用户私钥 $sk_{ID}$。

3) $\boldsymbol{Encrypt}(mpk, S, M) \to CT$: 输入系统主公钥 $mpk$、接收者标识集合 $S = (ID_1, ID_2, \cdots, ID_n)$和待加密

消息 $M$, 其中 $n\leqslant m$, 加密者运行加密算法 $\boldsymbol{Encrypt}$, 输出密文 $CT$ 并通过公开信道广播。

4) $\boldsymbol{Decrypt}(mpk,CT,ID,sk_{ID}) \rightarrow (M/\perp)$: 输入系统主公钥 $mpk$、密文 $CT$、接收者标识 $ID$ 以及对应的私钥 $sk_{ID}$, 解密者运行解密算法 $\boldsymbol{Decrypt}$, 输出正确的明文数据 $M$ 或者是⊥代表解密失败。

基于标识的广播加密的正确性要求对任意的消息 $M$, $(mpk,msk) \leftarrow Setup(1^{\lambda},m)$, $sk_{ID} \leftarrow \boldsymbol{KeyGen}(mpk,msk,ID)$, $CT \leftarrow \boldsymbol{Encrypt}(mpk,S,M)$。若 $ID \in S$, 那么

$$Pr[\boldsymbol{Decrypt}(mpk,CT,ID,sk_{ID}) = M] = 1.$$

注: 若解密算法的输入需要接收者的标识集合, 则相应的方案不具备匿名性。

### 3.3 安全模型

匿名标识广播加密既要保证数据的机密性, 又要保证接收者标识的隐私性。针对上述特性, 本文首先给出静态选择明文攻击下的不可区分性(indistinguishability against selective identity and chosen plaintext attacks, IND-sID-CPA), 旨在保证数据的机密性。接着, 给出静态选择明文攻击下的匿名性(anonymity against selective identity and chosen plaintext attacks, ANO-sID-CPA), 旨在保证接收者身份的匿名性。两个安全模型都是通过敌手和挑战者之间进行交互游戏定义, 设敌手和挑战者都以系统可容纳的最大接收者个数 $m$ 为输入。

**IND-sID-CPA** 安全模型定义如下:

1) 攻击初始阶段: 敌手 $\mathcal{A}$ 输出 $S^* = \{ID_1^*,ID_2^*,\cdots,ID_n^*\}$作为挑战标识集合, 其中 $n\leqslant m$。

2) 系统建立阶段: 已知安全参数λ和系统可容纳的最大接收者个数 $m$, 挑战者运行 $\boldsymbol{Setup}(1^{\lambda},m)$算法, 输出主公钥 $mpk$、主私钥 $msk$, 将 $mpk$ 发送给 $\mathcal{A}$。

3) 询问阶段 1: 敌手允许在该阶段自适应询问任意标识 $ID \notin S^*$的私钥。挑战者以标识 $ID$ 为输入, 运行 $\boldsymbol{KeyGen}$ 算法生成用户私钥 $sk_{ID}$, 将 $sk_{ID}$发送给 $\mathcal{A}$。

4) 挑战阶段: 当 $\mathcal{A}$ 决定询问阶段 1 结束, 敌手输出长度相等的两个明文数据$M_0,M_1$, 挑战者随机选取比特 $c \in \{0,1\}$, 运行 $\boldsymbol{Encrypt}(mpk,S^*,M_c)$算法, 输出密文 $CT$, 将 $CT$ 发送给敌手。

5) 询问阶段 2: $\mathcal{A}$ 允许在该阶段继续进行私钥生成询问, 挑战者回复询问的方式与询问阶段 1 相同。

6) 猜测阶段: 最后, $\mathcal{A}$ 输出一比特对 $c$ 的猜测值$c' \in \{0,1\}$, 若 $c = c'$, 则定义为敌手获胜。

将$q_D$记为敌手 $\mathcal{A}$ 在游戏交互期间可以发起询问阶段 1 的询问次数, 将$q_D$,$m$ 视为攻击参数, 定义敌手 $\mathcal{A}$ 的优势为

$$\begin{aligned}&\mathrm{Adv}_{AIBBE}^{\text{IND-sID-CPA}}(q_D,m,\mathcal{A})\\&=\left|\Pr[c=c']-\frac{1}{2}\right|\\&=\left|\Pr[c'=1\mid c=1]-\Pr[c'=1\mid c=0]\right|.\end{aligned}$$

**定义 1.** 若对任意多项式时间的 IND-sID-CPA 敌手 $\mathcal{A}$ 来说, 在与挑战者的交互过程中, $Adv_{AIBBE}^{IND-sID-CPA}(\lambda)$ 都是可忽略的, 则定义方案为 IND-sID-CPA 安全的。

**ANO-sID-CPA** 安全模型定义如下:

1) 攻击初始阶段: 敌手 $\mathcal{A}$ 输入 $S_0 = (ID_{0,1},ID_{0,2},\cdots,ID_{0,n})$, $S_1 = (ID_{1,1},ID_{1,2},\cdots,ID_{1,n})$作为挑战标识集合, 其中 $n\leqslant m$。

2) 系统建立阶段: 已知安全参数λ和系统可容纳的最大接收者个数 $m$, 挑战者运行 $\boldsymbol{Setup}(1^{\lambda}, m)$算法, 输出主私钥 $msk$、主公钥 $mpk$, 将 $mpk$ 发送给敌手。

3) 询问阶段 1: $\mathcal{A}$ 允许在该阶段自适应询问任意标识 $ID$ 的私钥, 其中 $ID \notin (S_0 \cup S_1)\backslash(S_0 \cap S_1)$。挑战者以标识 $ID$ 为输入, 运行 $\boldsymbol{KeyGen}$ 算法生成用户私钥 $sk_{ID}$, 将 $sk_{ID}$发送给 $\mathcal{A}$。

4) 挑战阶段: 首先敌手输出明文消息 $M$, 接着挑战者随机选取 1 比特 $b \in \{0,1\}$, 挑战者运行 $\boldsymbol{Encrypt}(mpk,S_b,M)$算法, 输出密文 $CT$ 并发送给 $\mathcal{A}$。

5) 询问阶段 2: $\mathcal{A}$ 允许在该阶段继续进行私钥生成询问, 挑战者回复询问的方式与询问阶段 1 相同。

6) 猜测阶段: 最后, 敌手输出 1 比特对 $b$ 的猜测值$b' \in \{0,1\}$, 若 $b = b'$, 则定义敌手获胜。

将$q_D$记为敌手 $\mathcal{A}$ 在游戏交互期间可以发起询问阶段 1 的询问次数, 将$q_D$,$m$ 视为攻击参数, 定义敌手 $\mathcal{A}$ 的优势为

$$\begin{aligned}&\mathrm{Adv}_{AIBBE}^{\text{ANO-sID-CPA}}(q_D,m,\mathcal{A})\\&=\left|\Pr[b=b']-\frac{1}{2}\right|\\&=\left|\Pr[b'=1\mid b=1]-\Pr[b'=1\mid b=0]\right|.\end{aligned}$$

**定义 2.** 若对任意多项式时间的 ANO-sID-CPA 敌手 $\mathcal{A}$ 来说, 在与挑战者的交互过程中, $Adv_{AIBBE}^{IND-sID-CPA}(\lambda)$ 都是可忽略的, 则称方案是 ANO-sID-CPA 安全的。

### 3.4 困难问题假设

本文方案的安全性基于广义判定性 $Diffie-Hellman$ 假设(general decision diffie-hellman exponent assumption, GDDHE), 记为 $(f,g)$-GDDHE

假设。消息的不可区分性和接收者匿名性分别依赖$(q,2m,f,g)$-GDDHE 困难假设和$(q,3m,f,g)$-GDDHE 困难假设。

$(q,2m,f,g)$ -GDDHE 问题定义如下:

**定义 3**. 令 $\mathcal{BP}=(\boldsymbol{p},\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,\boldsymbol{e}(\cdot,\cdot))$为双线性群, $\boldsymbol{f}$ 和 $\boldsymbol{g}$ 为两个互质多项式, 阶分别为 $\boldsymbol{q}$ 和 $\boldsymbol{m}$, 且不存在重根。$\boldsymbol{P}$, $\boldsymbol{Q}$ 分别为群$\mathbb{G}_1$, $\mathbb{G}_2$的生成元, 给定

$$\mathcal{R}=\begin{pmatrix}P,aP,a^2P,\cdots,a^{2m}P,rg(a)P,T,\\ Q,aQ,a^2Q,\cdots,a^qQ,ra^2f(a)Q\end{pmatrix},$$

判断 $T=e(P,Q)^{raf(a)}$或 $T\leftarrow_R\mathbb{G}_T$。

以 $\mathcal{R}$ 为输入, 定义多项式时间算法 $\mathcal{D}$ 解决 $(q,2m,f,g)$ -GDDHE 问题的优势为

$$\mathrm{Adv}(\lambda)=\left|\Pr\left[\mathcal{D}\left(\mathcal{R},T=e(P,Q)^{raf(a)}\right)=1\right]-\Pr\left[\mathcal{D}\left(\mathcal{R},T\neq e(P,Q)^{raf(a)}\right)=1\right]\right|.$$

**定理 1.** $(q,2m,f,g)$-GDDHE 问题假设: 对任意的 PPT 算法$\mathcal{D}$, 成功解决$(q,2m,f,g)$ -GDDHE 问题的优势是可以忽略的。

$(q,3m,f,g)$-GDDHE 问题定义如下:

**定义 4.** 令 $\mathcal{BP}=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e(\cdot,\cdot))$为双线性群, $f$ 和 $g$ 为两个互质多项式, 阶分别为 $q$ 和 $m$, 且不存在重根。$P$, $Q$ 分别为群$\mathbb{G}_1$, $\mathbb{G}_2$的生成元, 给定

$$\mathcal{R}=\begin{pmatrix}P,aP,a^2P,\cdots,a^{3m}P,rg(a)P,T,\\ Q,aQ,a^2Q,\cdots,a^qQ,ra^2f(a)Q\end{pmatrix},$$

判断 $T=e(P,Q)^{raf(a)}$或 $T\leftarrow_R\mathbb{G}_T$。

以 $\mathcal{R}$ 为输入, 定义多项式时间算法 $\mathcal{D}$ 解决 $(q,3m,f,g)$-GDDHE 问题的优势为

$$\mathrm{Adv}(\lambda)=\left|\Pr\left[\mathcal{D}\left(\mathcal{R},T=e(P,Q)^{raf(a)}\right)=1\right]-\Pr\left[\mathcal{D}\left(\mathcal{R},T\neq e(P,Q)^{raf(a)}\right)=1\right]\right|.$$

**定理 2.** $(q,3m,f,g)$ -GDDHE 问题假设: 对任意的 PPT 算法$\mathcal{D}$, 成功解决$(q,3m,f,g)$ -GDDHE 问题的优势是可以忽略的。

## 4 方案构造

本文方案使用与 SM9 相同的参数符号, 本文方案基于双线性群构造, 选取与 SM9 加密算法相同的私钥生成算法。首先给出方案的具体构造, 接着给出方案的正确性证明。

### 4.1 方案描述

1) **Setup**. 已知安全参数$\lambda$和系统可容纳的最大接收者个数$m$, KGC 首先选择一个满足安全参数的双线性群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p)$, 其中 $p$ 为大素数且 $p>2^{\lambda}$, 随后随机选择群$\mathbb{G}_1$的生成元$P_1$, 群$\mathbb{G}_2$的生成元$P_2$, 选择随机数$\alpha\in\mathbb{Z}_p^*$, 两个安全的密码杂凑函数 $H_1:\{0,1\}^*\to\mathbb{Z}_p^*$, $H_2:\mathbb{G}_T\to\mathbb{Z}_p^*$, 密钥派生函数 $KDF:\mathbb{G}_1\times(\mathbb{Z}_p^*)^2\to\{0,1\}^{\ell}$, 其中 $\ell$ 为消息长度。对任意 $i=1,2,\cdots,m$, 计算群$\mathbb{G}_1$中的元素$\alpha^iP_1$。输出系统主公钥 $msk$ 和主私钥 $msk$ 为

$$mpk=\left(\mathcal{BP},P_1,P_2,\{\alpha^iP_1\}_{i=1}^m,H_1,H_2,\ell,KDF\right),$$
$$msk=\alpha.$$

2) **KeyGen**. 已知用户标识 $ID\in\{0,1\}^*$, 计算 $t_1=H_1(ID)+\alpha$, 若$t_1=0$, 则重新生成并更新主公钥、主私钥; 否则计算$t_2=\alpha\cdot t_1^{-1}$, 计算用户私钥 $sk_{ID}=t_2\cdot P_2$.

3) **Encrypt**. 已知待加密的消息为比特串 $M\in\{0,1\}^{\ell}$, 接收者标识集合 $S=(ID_1,ID_2,\cdots,ID_n)$, 其中 $n\leqslant m$, 加密者按照以下步骤计算密文:

①定义多项式

$$p(x)=\prod_{i=1}^{n}(x+H_1(ID_i))=\sum_{i=0}^{n}a_i\,x^i\ \ mod\quad p,$$

$$p_i(x)=\frac{p(x)}{x+H_1(ID_i)}\ \ mod\quad p=\sum_{i=0}^{n-1}c_i\,x^i,$$

其中, $a_i,c_i$是可计算的多项式系数;

② 选取随机数 $r,k\in\mathbb{Z}_p^*$;

③ 计算群 $\mathbb{G}_1$ 中的元素 $C_0=rp(\alpha)P_1=r\cdot\sum_{i=0}^{n}a_i(\alpha^iP_1)$, 对于任意 $i\in[1,m]$, $\alpha^iP_1$为主公钥, 因此$C_0$是可计算的;

④ 对任意 $i=1,2,\cdots,n$, 计算

$$w_i=e(\alpha p_i(\alpha)P_1,P_2)^r=e\left(\sum_{i=0}^{n-1}c_i\,(\alpha^{i+1}P_1),P_2\right)^r.$$

由于$\alpha p_i(\alpha)P_1$是可计算的, 因此, $w_i$是可计算的;

⑤ 定义多项式

$$q(x)=\prod_{i=1}^{n}(x-H_2(w_i))+k\ mod\quad p=\sum_{i=0}^{n}b_i\,x^i\ mod\quad p$$

其中, $b_n=1$;

⑥ 计算 $K=KDF(C_0,k,l)$;

⑦ 计算$C_1=K\oplus M$;

⑧ 输出密文 $CT=(C_0,C_1,b_0,b_1,\cdots,b_n)$.

4) **Decrypt.** 为解密接收到的密文 $CT=(C_0,C_1,b_0,b_1,\cdots,b_n)$, 解密者 $ID_i$按照以下步骤计算明文:

①首先利用私钥 $sk_{ID_i}$计算$w_i'=e(C_0,sk_{ID_i})$, $k'=q(H_2(w_i'))=\sum_{i=0}^{n}b_i\,(H_2(w_i'))^i\ \ mod\quad p$;

②接着计算$K'=KDF(C_0,k',\ell)$, $M'=C_1\oplus K'$并输出解密消息 $M'$。若 $ID_i\in S$, 则$w_i'=w_i$, $k'=k$, $K'=K$, $M'=C_1\oplus K'=K\oplus M\oplus K'=M$, 能够正

确解密。

### 4.2 方案正确性分析

若接收者收到的密文 $CT=(C_0,C_1,b_0,b_1,\cdots,b_n)$为正确的密文, 且 $ID_i\in S$, 解密者可以利用私钥 $sk_{ID_i}$ 和密文 $CT$ 中的$C_0$获取正确的 $w'$, 即: $w_i'=w_i$, 其具体计算过程如下:

$$\begin{aligned}w_i' &= e\left(C_0, sk_{ID_i}\right)\\ &= e\left(rp(a)P_1, \frac{\alpha}{H_1(ID_i)+\alpha}P_2\right)\\ &= e(rp_i(a)P_1, \alpha P_2)\\ &= w_i.\end{aligned}$$

若$w_i'$能够正确计算出, 那么$k'=k$, $K'=K$, 方案满足正确性要求。

## 5 方案安全性分析

本节分析消息的不可区分安全性和接收者匿名性, 得到定理 3 和定理 4。

**定理 3**（消息的不可区分性）.设$H_1,H_2$为随机谕言器, 若$(q,2m,f,g)-$GDDHE 假设在双线性群中成立, 则本文方案满足 IND-sID-CPA 安全。

证明. 假设存在一个多项式时间敌手 $\mathcal{A}$, 能够以一个不可忽略的优势$\varepsilon_1$攻破本文所构造方案的 IND-sID-CPA 安全性。那么可构造一个模拟算法 $\mathcal{B}$, 利用 $\mathcal{A}$ 能以不可忽略的优势解决$(q,2m,f,g)-$GDDHE 问题。设系统中最大的接收者数量为 $m$, 随机谕言器$H_1$的询问次数为 $q$。$\mathcal{A},\mathcal{B}$ 以 $m$ 和 $q$ 为输入, 模拟算法 $\mathcal{B}$ 额外输入一个$(q,2m,f,g)$ -GDDHE 问题实例。其中问题实例中的 $f(z)$和 $g(z)$是定义在$\mathbb{Z}_p^*$上的次数为 $q$ 阶和 $m$ 阶的互质多项式。

在证明中规定如下表示:

- $f(z)=\prod_{i=1}^{q}(z+x_i)$, $g(z)=\prod_{i=q+1}^{q+m}(z+x_i)$;
- 对任意 $i\in[1,q]$, $f_i(z)=\frac{f(z)}{z+x_i}=\sum_{i=0}^{q-1}d_iz^i$, $f_i(z)$为 $q-1$ 阶多项式, $d_i$为多项式$f_i(z)$的系数;
- 对任意 $i\in[q+1,q+m]$, $g_i(z)=\frac{g(z)}{z+x_i}$, $g_i(z)$为 $m-1$ 阶多项式。

1) 攻击初始阶段

敌手 $\mathcal{A}$ 输出$S^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$作为挑战标识集合, 其中 $n\leqslant m$。

2) 系统建立阶段

模拟算法 $\mathcal{B}$ 按照如下方式设置系统参数。首先隐含的设$\alpha=a$, 接着, $\mathcal{B}$ 设置

$$P_1=\prod_{i=q+n+1}^{q+m}(a+x_i)P,$$

$$a^jP_1=a^j\cdot\prod_{i=q+n+1}^{q+m}(a+x_i)P, j=1,2,\cdots,m,$$

$$P_2=f(a)Q,$$

从上述设置可以看出, $P_1,a^jP_1,P_2$都可以通过问题实例计算得到。选取密钥派生函数 $KDF:\mathbb{G}_1\times(\mathbb{Z}_p^*)^2\to\{0,1\}^{\ell}$。$\mathcal{B}$ 将系统公共参数设置为

$$mpk=\left(P_1,\{a^jP_1\}_{j=1}^{m},P_2,KDF,l\right),$$

并将 $mpk$ 发送给敌手, 其中$H_1$, $H_2$是由 $\mathcal{B}$ 控制的随机谕言器。

3) 哈希询问

$\mathcal{A}$ 可以适应性发出如下的哈希询问:

① $H_1$询问: $\mathcal{A}$ 可以发出对标识 $ID$ 的哈希询问, $\mathcal{B}$ 建立列表$\mathcal{L}_1$用于回复 $\mathcal{A}$ 发出的询问, $\mathcal{L}_1$中包括$(ID_i,x_i)$, 初始状态如下:

$$\{*,x_i\}_{i\in[1,q]},\quad \{ID_i,x_i\}_{i\in[q+1,q+n]},$$

(*表示$\mathcal{L}_1$中的空条目), 其中

$$(ID_{q+1},ID_{q+2},\cdots,ID_{q+n})=(ID_1^*,ID_2^*,\cdots,ID_n^*).$$

当 $\mathcal{A}$ 发出 $ID_i$的询问, 若$(ID_i,x_i)$在列表$\mathcal{L}_1$中, $\mathcal{B}$ 返回$x_i$。否则, 记 $ID_i$为第 $i$ 个新标识, 设$H_1(ID)=x_i$, 将$(ID_i,x_i)$添加到列表$\mathcal{L}_1$中, 并返回$x_i$。

② $H_2$询问: $\mathcal{A}$ 发出对$w_i$的哈希询问, $\mathcal{B}$ 建立列表$\mathcal{L}_2$用于回复 $\mathcal{A}$ 发出的询问, $\mathcal{L}_2$中包括$(w_i,V_i)$, 初始状态为空。当 $\mathcal{A}$ 发出$w_i$的询问, 若$(w_i,V_i)$在列表$\mathcal{L}_2$中, $\mathcal{B}$ 返回$V_i$。否则, 随机选取$V_i\in\mathbb{Z}_p^*$, 设$H_2(w_i)=V_i$, 将$(w_i,V_i)$添加到列表$\mathcal{L}_2$中, 并返回$V_i$。

4) 询问阶段 1

敌手 $\mathcal{A}$ 在该阶段可以发出任意 $ID_i\notin S^*$的私钥询问, $\mathcal{B}$ 建立列表$\mathcal{L}_K$用于回复 $\mathcal{A}$ 发出的询问, $\mathcal{L}_K$中包括$(ID_i,sk_{ID_i})$, 初始状态为空。对于 $\mathcal{A}$ 发出的询问, 若$(ID_i,sk_{ID_i})$在列表$\mathcal{L}_K$中, $\mathcal{B}$ 返回 $sk_{ID_i}$。否则, $\mathcal{B}$ 查找列表$\mathcal{L}_1$获得$x_i$(若不存在, 以 $ID_i$作为输入询问$H_1$, 获得$x_i$), 计算

$$\begin{aligned}sk_{ID_i}&=\sum_{i=0}^{q-1}d_i(a^{i+1}Q)=af_i(a)Q=\frac{af(a)}{a+x_i}Q\\ &=\frac{a}{a+H_1(ID_i)}P_2,\end{aligned}$$

其中, $d_i$为$f_i(z)$的多项式系数。因此 $sk_{ID_i}$可以通过问题实例计算得到。最后, 将$(ID_i,sk_{ID_i})$添加到列表$\mathcal{L}_K$中, 并返回 $sk_{ID_i}$。

5) 挑战阶段

当敌手 $\mathcal{A}$ 决定询问阶段 1 结束时, 输出两个不

同且长度相等的明文数据$(M_0,M_1)$。$\mathcal{B}$ 首先在列表$\mathcal{L}_1$查询标识 $ID_i^* \in S^*$对应的哈希值$x_i$, 定义

$$p(a)=\prod_{i=q+1}^{q+n}(a+x_i)=\prod_{i=1}^{n}(a+H_1(ID_i^*)),$$

$$p_i(a)=\prod_{j=1,j\neq i}^{n}(a+H_1(ID_j^*))=\frac{p(a)}{a+H_1(ID_i^*)},$$

令$C_0^*=rg(a)P$, 设用于生成挑战密文的随机数$r^*=r$, 则有

$$\begin{aligned}C_0^* &= rg(a)P\\ &= r\cdot\prod_{i=q+1}^{q+n}(a+x_i)\cdot\prod_{i=q+n+1}^{q+m}(a+x_i)P\\ &= r^*p(a)P_1,\end{aligned}$$

对于任意 $ID_i \in S^*$, 计算

$w_i^*=T^{\prod_{j=q+1,j\neq i}^{q+m}x_j}\cdot e\left(\frac{1}{a}\left(g_i(a)-\prod_{j=q+1,j\neq i}^{q+m}x_j\right)P,ra^2f(a)Q\right)$, 以$w_i^*$为输出, 运行$H_2$询问得到$V_i^*$, 其中$V_i^*=H_2(w_i^*)$。接着, $\mathcal{B}$ 随机选取$k^*\in\mathbb{Z}_p^*$, $c\in\{0,1\}$, 计算 $q(x)=\prod_{i=1}^{n}(x-V_i^*)+k^*=\sum_{i=0}^{n}b_i^*x^i \mod p$, 输出$(b_0^*,b_1^*,\cdots,b_n^*)$。接着, 计算$K^*=KDF(C_0^*,k^*,\ell)$, 计算$C_1^*=K^*\oplus M_c$, $\mathcal{B}$ 输出挑战密文 $CT^*=(C_0^*,C_1^*,b_0^*,\cdots,b_n^*)$。

若 $T=e(P,Q)^{raf(a)}$, 有如下等式成立

$$\begin{aligned}w_i^* &= e\left(\frac{1}{a}\left(g_i(a)-\prod_{j=q+1,j\neq i}^{q+m}x_j\right)P,ra^2f(a)Q\right)\cdot T^{\prod_{j=q+1,j\neq i}^{q+m}x_j}\\ &= e\left(\left(g_i(a)-\prod_{j=q+1,j\neq i}^{q+m}x_j\right)P,raf(a)Q\right)\\ &\quad\cdot\left(e(P,Q)^{raf(a)}\right)^{\prod_{j=q+1,j\neq i}^{q+m}x_j}\\ &= e(P,Q)^{raf(a)\prod_{j=q+1,j\neq i}^{q+m}x_j}\cdot e\left(P,Q\right)^{raf(a)g_i(a)-raf(a)\prod_{j=q+1,j\neq i}^{q+m}x_j}\\ &= e\left(P,Q\right)^{raf(a)g_i(a)}\\ &= e\left(P,Q\right)^{raf(a)\prod_{j=q+1,j\neq i}^{q+n}(a+x_i)\cdot\prod_{j=q+n+1}^{q+m}(a+x_i)}\\ &= e\left(a\cdot\prod_{j=q+1,j\neq i}^{q+n}(a+x_i)\cdot\prod_{j=q+n+1}^{q+m}(a+x_i)P,f(a)Q\right)^{r}\\ &= e\left(ap_i(a)P_1,P_2\right)^{r^*}.\end{aligned}$$

因此, 当 $T=e(P,Q)^{raf(a)}$时, $CT^*$为正确封装密文。

6) 询问阶段 2

$\mathcal{A}$ 允许在该阶段继续进行私钥生成询问, 挑战者回复询问的方式与询问阶段 1 相同。

7) 猜测阶段

$\mathcal{A}$ 输出对 $c$ 的猜测值 $c'$, 若$c'=c$, 则 $\mathcal{B}$ 输出 1, 表示 $\mathcal{B}$ 猜测 $T=e(P,Q)^{raf(a)}$, 否则输出 0, 表示 $\mathcal{B}$ 猜测 $T\neq e(P,Q)^{raf(a)}$。

下面分析 $\mathcal{B}$ 成功解决$(q,2m,f,g)$ -GDDHE 问题的优势, 根据假设可知, 当 $T=e(P,Q)^{raf(a)}$时, 挑战密文是正确的封装密文, 模拟和真实情况是不可区分的, 则 $\mathcal{A}$ 成功猜测 $c$ 的概率为

$$Pr\left[c=c'|T=e(P,Q)^{raf(a)}\right]=1/2+\varepsilon_1.$$

当 $T\neq e(P,Q)^{raf(a)}$时, $w_i^*$为随机值, 与$C_0^*,C_1^*$无关, 消息$M_c$相当于由一次一密的密钥加密。敌手 $\mathcal{A}$ 正确猜测 $c$ 的概率为 $1/2$, 即

$$Pr\left[c=c'|T\neq e(P,Q)^{raf(a)}\right]=1/2.$$

因此, $\mathcal{A}$ 成功攻破方案的优势为

$$\begin{aligned}\mathrm{Adv}(\lambda) &= \left|Pr\left[\mathcal{A}\left(\mathcal{R},T=e(P,Q)^{raf(a)}\right)=1\right]-\right.\\ &\quad\left.Pr\left[\mathcal{A}\left(\mathcal{R},T\neq e(P,Q)^{raf(a)}\right)=1\right]\right|\\ &= \left|Pr\left[c=c'\,|\,T=e(P,Q)^{raf(a)}\right]-\right.\\ &\quad\left.Pr\left[c=c'\,|\,T\neq e(P,Q)^{raf(a)}\right]\right|\\ &= \left|1/2+\varepsilon_1-1/2\right|\\ &= \varepsilon_1.\end{aligned}$$

综上, 若 $\mathcal{A}$ 能够有不可忽略的优势$\varepsilon_1$攻破本文所构造方案的 IND-sID-CPA 安全性。那么模拟算法可以通过 $\mathcal{A}$ 以$\varepsilon_1$的优势解决$(q,2m,f,g)-$ GDDHE 问题。

注意到, 本文方案在随机谕言模型中满足 CPA 的安全性。我们可以通过 FO 转化技术[28]进一步实现 CCA 安全。

**定理 4**（接收者匿名性）. 假设密码函数$H_1,H_2$是随机谕言器, 如果$(q,3m,f,g)-$ GDDHE 假设成立, 则本文方案是 ANO-sID-CPA 安全的。

证明. 假设存在一个多项式时间敌手 $\mathcal{A}$, 能够有不可忽略的优势$\varepsilon_2$攻破本文所构造方案的 ANO-sID-CPA 安全性。那么可构造一个模拟算法 $\mathcal{B}$, 以不可忽略的优势解决$(q,3m,f,g)-$ GDDHE 问题。设系统中可容纳的最大接收者个数为 $m$, 随机谕言器$H_1$的询问次数为 $q$。$\mathcal{A}$, $\mathcal{B}$ 以 $m$ 和 $q$ 为输入, $\mathcal{B}$ 选取随机数 $s\in[1,m],u\in[1,s]$, 并随机选取向量$\vec{x}=(x_1,x_2,\cdots,x_q,\cdots,x_{q+m})$, 定义

$$f(z)=\prod_{i=1}^{q-(s-u)}(z+x_i),\quad g(z)=\prod_{i=q-(s-u)+1}^{q+m}(z+x_i),$$

模拟算法 $\mathcal{B}$ 额外输入一个$(q,3m,f,g)$ -GDDHE 问题实例。问题实例中的 $f(z)$和 $g(z)$是定义在$\mathbb{Z}_p$上的次数为 $q-(s-u)$阶和 $m+(s-u)$阶的互质多项式。

1) 攻击初始阶段

敌手 $\mathcal{A}$ 输出两个挑战标识集合

$$S_0 = (ID_{0,1}, ID_{0,2}, \cdots, ID_{0,n}),$$
$$S_1 = (ID_{1,1}, ID_{1,2}, \cdots, ID_{1,n}),$$

其中 $n \leqslant m$。

2) 系统建立阶段

$\mathcal{B}$ 首先判断 $s = n$ 是否成立, 若不成立, 则终止模拟。若成立, 则继续执行以下步骤: 若 $s = n$, 则敌手输出的两个集合中至少有一个标识是不同的。不妨设两个挑战标识集合中不同标识的个数 $t$, 接着判断 $u = t$ 是否成立, 若不成立, 则终止模拟。若成立, 则

$$f(z) = \prod_{i=1}^{q-(s-u)} (z + x_i) = \prod_{i=1}^{q-(n-t)} (z + x_i),$$
$$g(z) = \prod_{i=q-(s-u)+1}^{q+m} (z + x_i) = \prod_{i=q-(n-t)+1}^{q+m} (z + x_i),$$

$f(z)$和 $g(z)$的生成方式由图 1 所示。为便于证明, 不妨设挑战标识集合中前 $t$ 个元素不同, 即:

$$S_0 = (ID^*_{0,1}, ID^*_{0,2}, \cdots, ID^*_{0,t}, ID_{0,t+1}, \cdots, ID_{0,n}),$$
$$S_1 = (ID^*_{1,1}, ID^*_{1,2}, \cdots, ID^*_{1,t}, ID_{1,t+1}, \cdots, ID_{1,n}),$$

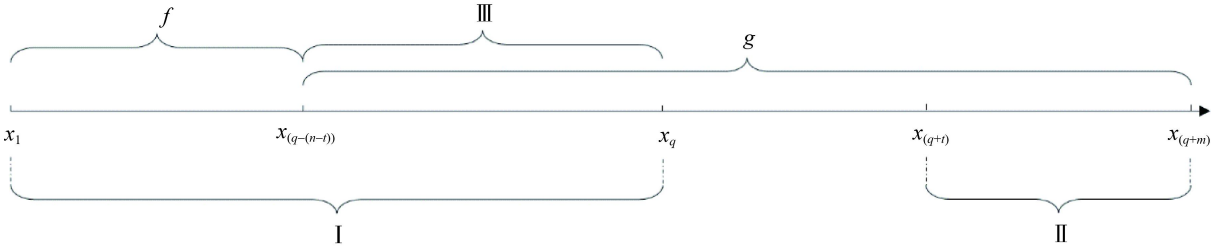


**图 1 参数设置示意图**

**Figure 1 Setting of parameters**

其中, $(ID_{0,t+1}, \cdots, ID_{0,n}) = (ID_{1,t+1}, \cdots, ID_{1,n})$, $\mathcal{B}$ 随机选取比特 $b \in \{0,1\}$, 则$S^*_b = (ID^*_{b,1}, ID^*_{b,2}, \cdots, ID^*_{b,t}, ID_{b,t+1}, \cdots, ID_{b,n})$。模拟算法 $\mathcal{B}$ 按照如下方式设置系统参数。首先隐含的设$\alpha = a$, 定义$g_i(z) = \frac{g(z)}{z + x_i}$, $g_i(z)$为 $m + (n - t) - 1$ 阶多项式。接着, 设

$$P_1 = \prod_{i=q+t+1}^{q+m} (a + x_i)\, P,$$
$$a^j P_1 = a^j \cdot \prod_{i=q+t+1}^{q+m} (a + x_i)\, P, j = 1,2,\cdots,m.$$

定义多项式

$$\sum_{i=0}^{q} b_i (a^i Q) = \prod_{i=q-(n-t)+1}^{q} (a + x_i)\, f(a) Q,$$

其中, $b_i$为可计算的多项式系数。令$P_2 = \prod_{i=q-(n-t)+1}^{q} (a + x_i) f(a) Q$, 从上述设置可以看出, $a^i Q$ 可以从问题实例中获得, 因此$P_1, a^j P_1, P_2$都可以通过问题实例计算得到。$P_1$、$P_2$的生成方式如图 1 所示, $P_1$由区间 $II$ 生成, $P_2$由区间 $I$ 生成, 选取密钥派生函数 $KDF$: $\mathbb{G}_1 \times (\mathbb{Z}_p^*)^2 \to \{0,1\}^\ell$。$\mathcal{B}$ 将系统公共参数设置为

$$mpk = \left(P_1, \{a^j P_1\}_{j=1}^m, P_2, KDF, l\right),$$

并将 $mpk$ 发送给敌手, $H_1$, $H_2$是由$\mathcal{B}$ 控制的随机谕言器。

3) 哈希询问

① $H_1$询问: $\mathcal{A}$ 可以发出对标识 $ID$ 的哈希询问, $\mathcal{B}$ 建立列表$\mathcal{L}_1$用于回复 $\mathcal{A}$ 发出的询问, $\mathcal{L}_1$中包括 $(ID_i, x_i)$, 初始状态如下:

$$\{*, x_i\}_{i \in [1, q-(n-t)]}, \quad \{ID_{b,i}, x_i\}_{i \in [q-(n-t)+1, q]},$$
$$\{ID^*_{b,i}, x_i\}_{[i=q+1, q+t]},$$

(*表示$\mathcal{L}_1$中的空条目), 其中

$$(ID_{q-(n-t)+1}, \cdots, ID_q) = (ID_{b,t+1}, \cdots, ID_{b,n}),$$
$$(ID_{q+1}, \cdots, ID_{q+t}) = (ID^*_{b,1}, \cdots, ID^*_{b,t}),$$

当 $\mathcal{A}$ 发出 $ID_i$的询问, 若$(ID_i, x_i)$在列表$\mathcal{L}_1$中, $\mathcal{B}$ 返回 $x_i$。否则, 记 $ID_i$为第 $i$ 个新标识, 设$H_1(ID) = x_i$, 将 $(ID_i, x_i)$添加到列表$\mathcal{L}_1$中, 并返回$x_i$。

② $H_2$询问: 与定理 3 的设置相同。

4) 询问阶段 1

除了集合$(S_0 \cup S_1) \backslash (S_0 \cap S_1)$内的标识, 敌手可以发出任意标识 $ID_i$的私钥询问, $\mathcal{B}$ 建立列表$\mathcal{L}_K$用于回复 $\mathcal{A}$ 发出的询问, $\mathcal{L}_K$中包括$(ID_i, sk_{ID_i})$, 初始状态为空。对于 $\mathcal{A}$ 发出的询问, 若$(ID_i, sk_{ID_i})$在列表$\mathcal{L}_K$中, $\mathcal{B}$ 返回 $sk_{ID_i}$。否则, $\mathcal{B}$ 查找列表$\mathcal{L}_1$获得$x_i$(若不存在, 以 $ID_i$作为输入询问$H_1$, 获得$x_i$)。计算

$$sk_{ID_i} = \frac{af(a)}{a + x_i} \cdot \prod_{j=q-(n-t)+1}^{q} (a + x_j)\, Q = \frac{a}{a + H_1(ID_i)} P_2. \quad (1)$$

下面分两种情况讨论等式(1)是可计算的:

① 若 $ID_i \in S_0 \cap S_1$, $H_1(ID_i)$的选取通过图 1 中区间 III 得到, 则$x_i$为多项式$\prod_{j=q-(n-t)+1}^{q} (a + x_j)$的负根, 多项式$\prod_{j=q-(n-t)+1}^{q} (a + x_j)$可被$(a + x_i)$整除;

② 若 $ID_i \notin S_0 \cap S_1$, 则$(a + x_i)$可以整除 $f(a)$。

故 $sk_{ID_i}$是可计算的。最后, 将$(ID_i, sk_{ID_i})$添加到列表$\mathcal{L}_K$中, 并返回 $sk_{ID_i}$。

5) 挑战阶段

$\mathcal{A}$ 输出挑战明文数据$M^* \in \{0,1\}^{\ell}$, $\mathcal{B}$ 按照如下步骤计算:

① 首先定义

$$p(a)=\prod_{i=q-(n-t)+1}^{q+t}(a+x_i)=\prod_{i=1}^{t}(a+H_1(ID_{b,i}^*))\cdot\prod_{i=t+1}^{n}(a+H_1(ID_{b,i})),$$

$$p_i(a)=\prod_{j=1,j\neq i}^{n}(a+H_1(ID_j))=\frac{p(a)}{a+H_1(ID_i)}.$$

$$w_i^*=e\left(\frac{1}{a}\left(\prod_{j=q-(n-t)+1}^{q}(a+x_j)\cdot g_i(a)-\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j\right)P,ra^2f(a)Q\right)\cdot T^{\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j},$$

以$w_i^*$作为输入, 运行$H_2$询问, 得到$V_i^*=H_2(w_i^*)$;

③ 对于任意标识 $ID_i \in S_0 \cap S_1$, 即: 标识集合$(ID_{b,t+1},\cdots,ID_{b,n})$, 计算标识 $ID_i$的私钥 $sk_{ID_i}$, 并计算 $w_i^*=(rg(a)P,sk_{ID_i})=(C_0^*,sk_{ID_i})$, 以$w_i^*$作为输入, 运行$H_2$询问, 得到$V_i^*=H_2(w_i^*)$;

计算

$$\begin{aligned}C_0^*&=rg(a)P\\&=r\cdot\prod_{i=q-(n-t)+1}^{q+m}(a+x_i)P\\&=r\cdot\prod_{i=q-(n-t)+1}^{q+t}(a+x_i)\cdot\prod_{i=q+t+1}^{q+m}(a+x_i)P\\&=r^*p(a)P_1;\end{aligned}$$

② 对于任意标识 $ID_i \in S_b^* \backslash (S_0 \cap S_1)$, 即: 标识集合$(ID_{b,1}^*,ID_{b,2}^*,\cdots,ID_{b,t}^*)$, 对应哈希值为$(x_{q+1},\cdots,x_{q+t})$, 计算

$$w_i^*=e\left(\frac{1}{a}\left(\prod_{j=q-(n-t)+1}^{q}(a+x_j)\cdot g_i(a)-\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j\right)P,ra^2f(a)Q\right)\cdot T^{\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j}$$

$$=e\left(\left(\prod_{j=q-(n-t)+1}^{q}(a+x_j)\cdot g_i(a)-\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j\right)P,raf(a)Q\right)\cdot e(P,Q)^{raf(a)\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j}$$

$$=e(P,Q)^{raf(a)\prod_{j=q-(n-t)+1}^{q}(a+x_j)\prod_{j=q-(n-t)+1,j\neq i}^{q+t}(a+x_j)\prod_{j=q+t+1}^{q+m}(a+x_j)}$$

$$=e\left(ap_i(a)P_1,P_2\right)^{r^*}.$$

④ 随机选取 $k^* \in \mathbb{Z}_p^*$, 计算 $q(x)=\prod_{i=1}^{n}(x-V_i^*)+k^*=\sum_{i=0}^{n}b_ix^i \bmod p$, 输出$(b_0^*,b_1^*,\cdots,b_n^*)$;

⑤ 计算 $K^*=KDF(C_0^*,k^*,\ell)$, $C_1^*=K^* \oplus M^*$, 输出挑战密文 $CT^*=(C_0^*,C_1^*,b_0^*,\cdots,b_n^*)$。

若 $T=e(P,Q)^{raf(a)}$, 如下等式成立:

$$w_i^*=e\left(\frac{1}{a}\left(\prod_{j=q-(n-t)+1}^{q}(a+x_j)\cdot g_i(a)-\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j\right)P,ra^2f(a)Q\right)\cdot T^{\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j}$$

$$=e\left(\left(\prod_{j=q-(n-t)+1}^{q}(a+x_j)\cdot g_i(a)-\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j\right)P,raf(a)Q\right)\cdot e(P,Q)^{raf(a)\prod_{j=q-(n-t)+1}^{q}x_j\cdot\prod_{j=q-(n-t)+1,j\neq i}^{q+m}x_j}$$

$$=e(P,Q)^{raf(a)\prod_{j=q-(n-t)+1}^{q}(a+x_j)\prod_{j=q-(n-t)+1,j\neq i}^{q+t}(a+x_j)\prod_{j=q+t+1}^{q+m}(a+x_j)}$$

$$=e\left(ap_i(a)P_1,P_2\right)^{r^*}.$$

6) 询问阶段 2

在该阶段, $\mathcal{A}$ 允许继续进行私钥生成询问, 挑战者回复询问的方式与询问阶段 1 相同。

7) 猜测阶段

$\mathcal{A}$ 输出对 $b$ 的猜测值, 若$b'=b$, 则 $\mathcal{B}$ 输出 1 表示 $\mathcal{B}$ 猜测 $T=e(P,Q)^{raf(a)}$, 否则输出 0 表示 $\mathcal{B}$ 猜测 $T \neq e(P,Q)^{raf(a)}$。

下面分析 $\mathcal{B}$ 成功解决$(q,3m,f,g)$ -GDDHE 问题的优势。根据假设可知, 当 $T=e(P,Q)^{raf(a)}$时, 挑战密文是正确的封装密文, 模拟和真实情况是不可区分的。若 $\mathcal{B}$ 成功猜测 $n$ 和 $t$, 那么模拟成功的概率为 $\frac{1}{mn}$, $\mathcal{A}$ 成功猜测 $c$ 的概率为 $Pr[b=b'|T=e(P,Q)^{raf(a)}]=1/2+\varepsilon_2$。当 $T \neq e(P,Q)^{raf(a)}$时, $w_i^*$为随机值, 与$C_0^*$, $C_1^*$无关, 消息$M^*$相当于由一次一密的密钥加密, 敌手 $\mathcal{A}$ 有 $1/2$ 的概率成功猜猜 $b$, 即 $Pr[b=b'|T \neq e(P,Q)^{raf(a)}]=1/2$。因此, $\mathcal{A}$ 成功攻破方案的优势为

$$\begin{aligned}\mathrm{Adv}(\lambda)&=\left|\Pr\left[\mathcal{A}\left(\mathcal{R},T=e(P,Q)^{raf(a)}\right)=1\right]-\Pr\left[\mathcal{A}\left(\mathcal{R},T\neq e(P,Q)^{raf(a)}\right)=1\right]\right|\cdot\frac{1}{mn}\\&=\left|\Pr\left[b=b'|T=e(P,Q)^{raf(a)}\right]-\Pr\left[b=b'|T\neq e(P,Q)^{raf(a)}\right]\right|\cdot\frac{1}{mn}\\&=\left|1/2+\varepsilon_2-1/2\right|\cdot\frac{1}{mn}=\frac{\varepsilon_2}{mn}\leqslant\frac{\varepsilon_2}{m^2}.\end{aligned}$$

综上, 若 $\mathcal{A}$ 能够以不可忽略的优势$\varepsilon_2$攻破方案。那么模拟算法 $\mathcal{B}$ 可以通过以$\frac{\varepsilon_2}{m^2}$的优势解决$(q,3m,f,g)$ -GDDHE 问题。

## 6 性能分析

本节分别从理论和实验仿真两部分分析基于 SM9 的匿名广播加密方案。

表 1 通信代价和安全性比较

Table 1 Comparison of communication cost and security

| 方案 | 公钥长度 | 私钥长度 | 密文长度 | 困难假设 | 匿名性 |
|---|---|---|---|---|---|
| 方案[4] | $\|\mathbb{G}_1\|+(m+1)\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$ | $\|\mathbb{G}_1\|$ | $\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$ | $q$-GDDHE | ✘ |
| 方案[13] | 5\|G\| | $\|\mathbb{G}\|$ | 2\|G\|+$(n+1)\|\mathbb{Z}_p^*\|+\ell$ | DBDH | √ |
| 方案[29] | $\|\mathbb{G}\|+\|\mathbb{G}_T\|$ | $\|\mathbb{G}\|$ | 2\|G\|+$2n\|\mathbb{G}_T\|$ | DBDH | √ |
| 方案[9] | $(m+1)\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\|\mathbb{G}_T\|$ | $\|\mathbb{G}_2\|$ | $\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+\ell$ | $q$-GDDHE | ✘ |
| $n$-SM9 | $2\|\mathbb{G}_1\|+\|\mathbb{G}_2\|$ | $\|\mathbb{G}_2\|$ | $n(\|\mathbb{G}_1\|+\|\mathbb{Z}_p^*\|)+\ell$ | Gap-$q$-BCAA1 | √ |
| 本文方案 | $(m+1)\|\mathbb{G}_1\|+\|\mathbb{G}_2\|$ | $\|\mathbb{G}_2\|$ | $\|\mathbb{G}_1\|+n\|\mathbb{Z}_p^*\|+\ell$ | $q$-GDDHE | √ |

## 6.1 理论分析

本节从通信代价和计算效率两方面分析本文方案, 并与现有的标识广播加密方案比较, 结果如表 1 和表 2 所示。$n$-SM9 表示重复利用 SM9 加密算法为 $n$ 个接收者生成 $n$ 份 SM9 密文, 并与组标识技术结合实现匿名通信。要求从组标识计算出组内某个标识在计算上是不可行的。表 2 只统计开销较大的运算, 对于轻量级运算比如模运算, 则未统计。符号说明如下: $|\mathbb{G}_x|$表示群$\mathbb{G}_x$中元素的长度, 其中 $x\in\{1,2,T\}$, $|\mathbb{G}|$表示对称群 $\mathbb{G}$ 中元素的长度, $\ell$ 表示消息的长度, $m$ 表示系统可容纳的最大接收者个数, $n$ 表示一次广播加密中实际的接收者个数, $\mathcal{P}$ 表示双线性对运算, $\mathcal{M}$ 表示对称群 $\mathbb{G}$ 中的标量乘法运算, $\mathcal{M}_i$表示非对称群$\mathbb{G}_i(i=1,2)$中的标量乘法运算, $\mathcal{E}$ 表示群$\mathbb{G}_T$中的指数运算。

表 2 计算开销比较

Table 2 Comparison of computational overhead

| 方案 | 公钥生成 | 私钥生成 | 密文生成 | 解密 |
|---|---|---|---|---|
| 方案[4] | $\mathcal{M}_1+m\mathcal{M}_2+\mathcal{P}$ | $\mathcal{M}_1$ | $\mathcal{M}_1+(n+1)\mathcal{M}_2+E$ | $(n-1)\mathcal{M}_2+2P+E$ |
| 方案[13] | $\mathcal{M}$ | $\mathcal{M}$ | $4M+n(P+E)$ | $3P+2M$ |
| 方案[29] | $\mathcal{M}$ | $\mathcal{M}$ | $2M+2n(P+E)$ | $2P$ |
| 方案[9] | $m\mathcal{M}_1+\mathcal{M}_2+\mathcal{P}$ | $\mathcal{M}_2$ | $(n+1)\mathcal{M}_1+\mathcal{M}_2+E$ | $(n-1)\mathcal{M}_1+2P+E$ |
| $n$-SM9 | $\mathcal{M}_1$ | $\mathcal{M}_2$ | $2n\mathcal{M}_1+(\mathcal{P}+\mathcal{E})$ | $\mathcal{P}$ |
| 本文方案 | $m\mathcal{M}_1$ | $\mathcal{M}_2$ | $(n^2+n+1)\mathcal{M}_1+n(P+E)$ | $\mathcal{P}$ |

从表 1 可知, 本文方案与文献[4]和文献[9]具有较长的公钥, 长度随着系统可容纳的最大接收者个数线性增长。虽然文献[4]和文献[9]具有定长的密文, 但其不满足隐私性, 无法保护接收者隐私。其他比较方案密文长度都随接收者个数$n$ 线性增长,其中本方案和文献[13]的密文相当, 优于文献[29]。表 2 比较了计算开销, 本文方案的解密开销只包含一个双线性对运算, 在所有比较方案中是最优的。虽然密文生成的时间复杂度较高, 但当 $n$ 较小时, 和其他方案是可比的。

## 6.2 实验仿真

本小节对第 4 节所设计的 SM9 匿名广播加密方案进行实验性能评估。测试环境为一台 64 位 manjaro linux 操作系统, Intel i5-5257U CPU, 8GB RAM 的联想笔记本电脑。仿真方案采用 Pairing-Based Cryptography (PBC) Library, 并采用 PBC 中的 Type F 曲线。在比较中, 考虑 128 比特的安全性, 设置非对称群中 $|\mathbb{G}_1|=256$ bits, $|\mathbb{G}_2|=512$ bits, $|\mathbb{G}_T|=3072$ bits, 在对称群中设$|\mathbb{G}|=1536$ bits。设消息长度$|\ell|$ =256 bits。测试中设置的最大接收者数量为 100, 四个算法运行结果如图 2～5 所示。

由上述结果可知, 在最大接收者数量不变的情况下, Setup, KeyGen, Decrypt 算法时间复杂基本为 $O(1)$, 但加密时间随着接收者数量的增加而增加, 实验结果与理论分析一致。图 6 给出了具有匿名性方案的密文长度对比。由图 6 可知, 本文方案能有效减少通过多次运行 SM9 算法实现广播的密文长度。在密文长度都为线性的情况下, 本文方案的密文长度最短。代价是增加了系统公钥长度, 更适用于传输带宽有限的应用。

# 7 总结

本文在 SM9 加密算法的基础上, 构造了首个基于 SM9 的匿名广播加密方案。可在实现多人高效数据共享

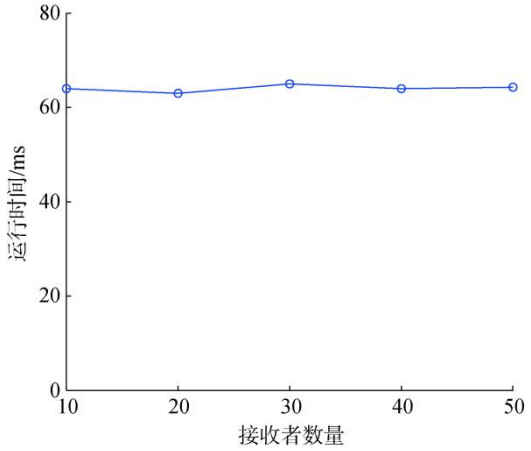


**图 2　Setup 算法运行时间**

**Figure 2　The running time of Setup**

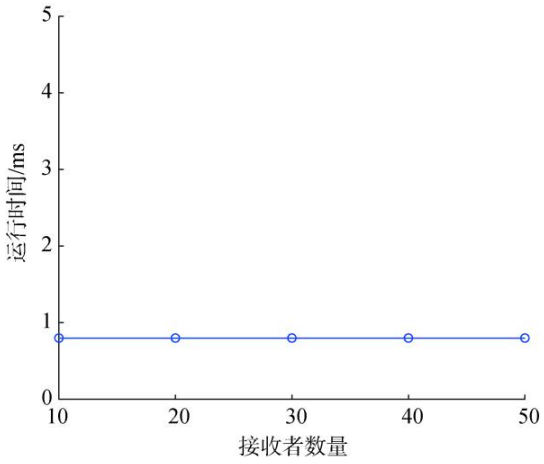


**图 3　KeyGen 算法运行时间**

**Figure 3　The running time of KeyGen**

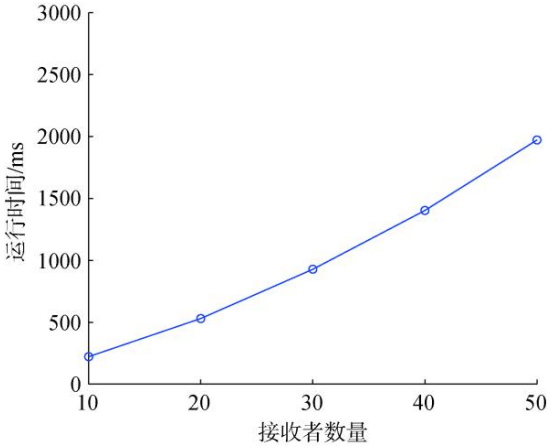


**图 4　Encrypt 算法运行时间**

**Figure 4　The running time of Encrypt**

的同时有效保护接收者的隐私, 有助于完善 SM9 密码体制。方案的计算效率和通信代价与现有匿名标识广播加密方案相当, 安全性基于 $q-$ GDDHE 困难假设。在随机谕言模型中证明了方案在静态选择明文攻击下具有不可区分的安全性和接收者匿名性。最后对方案进行实验仿真测试算法的效率。

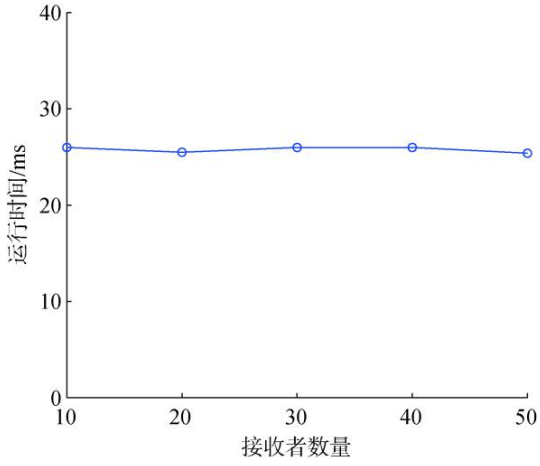


**图 5　Decrypt 算法运行时间**

**Figure 5　The running time of Decrypt**

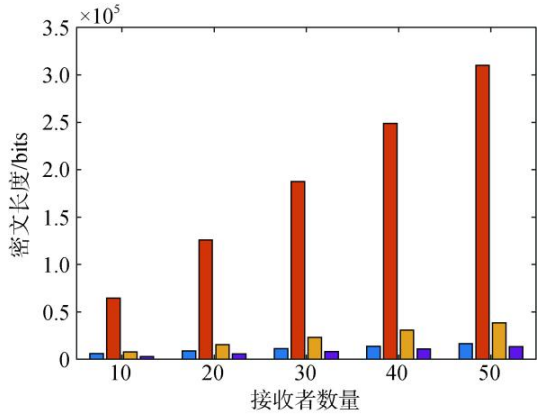


**图 6　密文长度对比**

**Figure 6　Comparison of Ciphertext Length**

## 参考文献

[1] Fiat A, Naor M. Broadcast Encryption[M]. *Advances in Cryptology — CRYPTO' 93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 480-491.

[2] Naor M, Pinkas B. Efficient Trace and Revoke Schemes[J]. *International Journal of Information Security*, 2010, 9(6): 411-424.

[3] Shamir A. Identity-based cryptosystems and signature schemes [C]. *Workshop on the theory and application of cryptographic techniques*, 1984: 47-53.

[4] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys [C]. *International Conference on the Theory and Application of Cryptology and Information Security*, 2007: 200-215.

[5] Boneh D, Hamburg M. Generalized identity based and broadcast encryption schemes [C]. *International Conference on the Theory*

*and Application of Cryptology and Information Security*, 2008:455-470.

[6] Kim J, Susilo W, Au M H, et al. Adaptively Secure Identity-Based Broadcast Encryption with a Constant-Sized Ciphertext[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(3): 679-693.

[7] Liu X, Liu W R, Wu Q H, et al. Chosen Ciphertext Secure Identity-Based Broadcast Encryption[J]. *Journal of Cryptologic Research*, 2015, 2(1): 66-76.
(刘潇, 刘巍然, 伍前红, 等. 选择密文安全的基于身份的广播加密方案[J]. *密码学报*, 2015, 2(1): 66-76.)

[8] Lai J C, Mu Y, Guo F C, et al. Identity-Based Broadcast Encryption for Inner Products[J]. *The Computer Journal*, 2018, 61(8): 1240-1251.

[9] Lai J C, Huang X Y, He D B. An Efficient Identity-Based Broadcast Encryption Scheme Based on SM9[J]. *Chinese Journal of Computers*, 2021, 44(5): 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[J]. *计算机学报*, 2021, 44(5): 897-907.)

[10] Barth A, Boneh D, Waters B. Privacy in Encrypted Content Distribution Using Private Broadcast Encryption[C]. *The 10th international conference on Financial Cryptography and Data Security*, 2006: 52-64.

[11] Fazio N, Perera I M. Outsider-Anonymous Broadcast Encryption with Sublinear Ciphertexts[C]. *The 15th international conference on Practice and Theory in Public Key Cryptography*, 2012: 225-242.

[12] Libert B, Paterson KG, Quaglia EA. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model [C]. *International Workshop on Public Key Cryptography*, 2012: 206-224.

[13] He Kai, Weng Jian, Liu JN, et al. Anonymous identity-based broadcast encryption with chosen-ciphertext security[C]. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016: 247-255.

[14] Cheng Zhaohui. Security analysis of SM9 key agreement and encryption[C]. *International Conference on Information Security and Cryptology*, 2018: 3-25.

[15] Yang Y T, Cai J L, Zhang X W, et al. Privacy Preserving Scheme in Block Chain with Provably Secure Based on SM9 Algorithm[J]. *Journal of Software*, 2019, 30(6): 1692-1704.
(杨亚涛, 蔡居良, 张筱薇, 等. 基于 SM9 算法可证明安全的区块链隐私保护方案[J]. *软件学报*, 2019, 30(6): 1692-1704.)

[16] Wang S, Fang L G, Han L B, et al. Fast Implementation of SM9 Digital Signature and Verification Algorithms[J]. *Communications Technology*, 2019, 52(10): 2524-2527.
(王松, 房利国, 韩炼冰, 等. 一种 SM9 数字签名及验证算法的快速实现方法[J]. *通信技术*, 2019, 52(10): 2524-2527.)

[17] Gan Z W, Liao F Y. Rapid Calculation of R-Ate Bilinear Pairing in China State Cryptography Standard SM9[J]. *Computer Engineering*, 2019, 45(6): 171-174.
(甘植旺, 廖方圆. 国密 SM9 中 R-ate 双线性对快速计算[J]. *计算机工程*, 2019, 45(6): 171-174.)

[18] Zhang X F, Peng H. Blind Signature Scheme Based on SM9 Algorithm[J]. *Netinfo Security*, 2019(8): 61-67.
(张雪锋, 彭华. 一种基于 SM9 算法的盲签名方案研究[J]. *信息网络安全*, 2019(8): 61-67.)

[19] Wang M D, He W G, Li J, et al. Optimal Design of R-Ate Pair in SM9 Algorithm[J]. *Communications Technology*, 2020, 53(9): 2241-2244.
(王明东, 何卫国, 李军, 等. 国密 SM9 算法 R-ate 对计算的优化设计[J]. *通信技术*, 2020, 53(9): 2241-2244.)

[20] Xu S W, Ren X P, Yuan F, et al. A Secure Key Issuing Scheme of SM9[J]. *Computer Applications and Software*, 2020, 37(1): 314-319.
(许盛伟, 任雄鹏, 袁峰, 等. 一种关于 SM9 的安全密钥分发方案[J]. *计算机应用与软件*, 2020, 37(1): 314-319.)

[21] Boneh D, Gentry C, Waters B. Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys[M]. Advances in Cryptology – CRYPTO 2005. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 258-275.

[22] Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts) [C]. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2009:171-188.

[23] Zhao Z, Guo F C, Lai J C, et al. Accountable Authority Identity-Based Broadcast Encryption with Constant-Size Private Keys and Ciphertexts[J]. *Theoretical Computer Science*, 2020, 809: 73-87.

[24] Lai Jianchang, Mu Yi, Guo Fuchun, et al. Anonymous identity-based broadcast encryption with revocation for file sharing [C]. *Australasian Conference on Information Security and Privacy*, 2016:223-239.

[25] Zhen P, Hu X B, Yu Y Y, et al. Research on the Optimization Computation of SM9 Bilinear Pairings[C]. *The 2017 2nd International Conference on Communication and Information Systems*, 2017: 256-261.

[26] Zhang Q, Wang A, Niu Y C, et al. Side-Channel Attacks and Countermeasures for Identity-Based Cryptographic Algorithm SM9[J]. *Security and Communication Networks*, 2018, 2018: 1-14.

[27] Lai J C, Huang X Y, He D B, et al. An Efficient Identity-Based Signcryption Scheme Based on SM9[J]. *Journal of Cryptologic Research*, 2021, 8(2): 314-329.
(赖建昌, 黄欣沂, 何德彪, 等. 基于商密 SM9 的高效标识签密[J]. *密码学报*, 2021, 8(2): 314-329.)

[28] Fujisaki E, Okamoto T. Secure Integration of Asymmetric and Symmetric Encryption Schemes[J]. *Journal of Cryptology*, 2013, 26(1): 80-101.

[29] Xu P, Li J N, Wang W, et al. Anonymous Identity-Based Broadcast Encryption with Constant Decryption Complexity and Strong Security[C]. *The 11th ACM on Asia Conference on Computer and Communications Security*, 2016: 223-233.

**崔岩** 于2019年在东北石油大学物联网工程专业获得学士学位。现在福建师范大学网络空间安全专业攻读硕士学位。研究领域为公钥广播加密、公钥签名。研究兴趣包括: 区块链、零知识证明。Email: _crocky829@gmail.com

**黄欣沂** 于 2009 年在伍伦贡大学信息安全专业获得博士学位。现任职于福建师范大学, 教授, 博士生导师。研究领域为密码学、信息安全。Email: xyhuang@fjnu.edu.cn

**赖建昌** 于 2017 年在伍伦贡大学信息安全专业获得博士学位。现任职于福建师范大学副教授, 硕士生导师。研究领域为公钥密码学、信息安全。Email: jclai@fjnu.edu.cn

**何德彪** 于 2009 年在武汉大学应用数学专业获得博士学位。现任武汉大学国家网络安全学院教授, 博士生导师。研究领域为公钥密码学、网络与信息安全。Email: hedebiao@whu.edu.cn

**程朝辉** 于 2007 年在英国密德萨斯大学密码学专业获得博士学位, 现就职于深圳奥联信息安全科技有限公司。主要研究方向为密码学、网络与信息安全。Email: chengzh@myibc.net