一种基于商密 SM9 的高效标识广播加密方案

赖建昌[1)] 黄欣沂[1)] 何德彪[2)]

[1)](福建师范大学数学与信息学院福建省网络安全与密码技术重点实验室福建省应用数学中心 福州 350007)

[2)](武汉大学网络安全学院空天信息安全与可信计算教育部重点实验室 武汉 430072)

摘 要 广播加密允许发送者为一组指定的用户同时加密数据,并通过公开信道传输密文.只有加密时指定的授权用户才能正确解密,非授权用户即使合谋也无法获得明文数据.得益于这些优点,广播加密被广泛用在云计算、物联网等应用中,实现多用户数据共享和秘密分享.SM9 标识加密算法是我国自主设计的商用密码,用于数据加密,保护数据隐私,但只适用于单用户的情形.本文结合我国商密 SM9 标识加密算法和广播加密,利用双线性对技术设计了第一个基于 SM9 的标识广播加密方案.方案的构造思想借鉴 Delerablée 标识广播加密方案(Asiacrypt 2007).所提方案中密文和用户私钥的长度是固定的,与接收者数量无关.密文由三个元素构成,用户私钥只包含一个群元素.与 SM9 标识加密算法相比,密文长度只增加了一个群元素.本文给出了标识广播加密的形式化定义和安全模型,并在随机谕言模型中证明了方案能够抵抗静态选择明文攻击.方案的安全性分析基于 q-type 的 GDDHE 困难问题假设.理论分析和实验仿真显示,方案的计算开销和通信开销与目前国际主流的标识广播加密方案相当.

关键词 广播加密;固定密文长度;SM9;标识密码;选择明文安全

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2021.00897

An Efficient Identity-Based Broadcast Encryption Scheme Based on SM9

LAI Jian-Chang[1)] HUANG Xin-Yi[1)] HE De-Biao[2)]

[1)](*Fujian Provincial Key Lab of Network Security and Cryptology, Center for Applied Mathematics of Fujian Province, College of Mathematics and Informatics, Fujian Normal University, Fuzhou* 350007)

[2)](*Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072)

Abstract Broadcast encryption allows a data sender to encrypt data to a group of specified users via a public channel. Only those authorized users can decrypt the ciphertext. Unauthorized users learn nothing about the encrypted data even they collude. Broadcast encryption has been widely used in real-world applications for multi-user data sharing or secret sharing due to its merits, such as cloud computing and Internet of things. While the SM9 identity-based encryption algorithm designed by China is a Chinese encryption standard for protecting data privacy. Nevertheless, SM9 encryption algorithm is designed for the scenarios where the receiver is one only. In this paper, we fuse SM9 identity-based encryption algorithm and broadcast encryption, and propose the first identity-based broadcast encryption (IBBE) scheme based on SM9 under pairings. The construction idea is derived from Delerablée's IBBE scheme (Asiacrypt 2007). The proposed scheme features constant-size ciphertexts and private keys, which is independent of the number of receivers. More precisely, the ciphertext consists of three elements and user private key has one group element only. Compared to SM9 identity-based encryption algorithm, the ciphertext

收稿日期:2020-03-01;在线发布日期:2021-01-15.本课题得到国家自然科学基金(61902191,62032005,61872089,61972294,61932016)、江苏省自然科学基金青年基金(BK20190696)、福建省自然科学基金(2020J02016)资助.**赖建昌**,博士,副教授,主要研究方向为公钥密码学、信息安全等.E-mail:jclai@fjnu.edu.cn.**黄欣沂**(通信作者),博士,教授,博士生导师,主要研究领域为密码学、信息安全等.E-mail:xyhuang@fjnu.edu.cn.**何德彪**,博士,教授,博士生导师,主要研究领域为密码学、信息安全等.

contains one additional group element. We give the definition of IBBE and corresponding security models, and formally analyze the security of the proposed scheme. The proposed scheme has been proved to be IND-sID-CPA secure in the random oracle model under a q-type GDDHE assumption. The theoretical analysis and demonstration show that the proposed scheme is comparable to the existing optimal IBBE schemes in terms of computational overheads and communication overheads.

Keywords broadcast encryption; constant-size ciphertexts; SM9; identity-based cryptosystem; CPA security

1 引 言

密码是保护数据安全的重要技术.为保证数据私密性,明文数据通常经过加密处理后,以密态形式存储和传输,只有授权用户才能解密.传统公钥加密体制需要第三方机构颁发证书,绑定用户公钥和身份,确保用户公钥的真实有效性.然而,证书的管理和维护过程繁琐,开销较大.为了有效解决证书问题,Shamir[1]于 1984 年提出标识密码(Identity-based Cryptosystem)的概念,也称为基于身份的密码系统.在标识密码系统中,用户的公钥可以是电话号码、邮箱地址等能够唯一标识用户的任意字符串,相应的私钥由系统中的密钥生成中心(Key Generation Center,KGC)计算.标识密码消除了证书,避免了传统公钥密码体制中证书的管理问题.自标识密码概念提出后,标识密码得到国内外学者积极的研究.但直到 2001 年,Boneh 和 Franklin[2]利用双线性对技术提出第一个实用的且可证明安全的标识加密方案.

虽然标识密码得到了大量的研究,取得了积极的进展[3-21],但从整体上看,标识密码研究大都围绕国外提出的算法开展.为实现密码自主可控,保障网络与信息安全,我国自主设计了包含数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法的 SM9 标识密码[22].2016 年 3 月,国家密码管理局正式发布《SM9 标识密码算法》GM/T 0044-2016 密码行业标准.2020 年 4 月,GB/T 38635.1-2020《信息安全技术 SM9 标识密码算法 第 1 部分:总则》、GB/T 38635.2-2020《信息安全技术 SM9 标识密码算法 第 2 部分:算法》两项国家标准获批发布,SM9 正式成为国家标准.随着 SM9 相关算法被陆续纳入 ISO/IEC 国际标准,SM9 标识密码算法在国内外的地位越来越重要.基础的标识加密只适用于单用户的情形.当数据需要同时安全发送给多个用户时,可通过重复调用加密算法,分别为每个用户加密数据.显然,该方法的计算代价和通信代价随着接收者数量线性增加,效率极低.

为提高多用户环境下数据安全共享的效率,Fiat 和 Naor 在 1993 年提出广播加密(Broadcast Encryption)[23]的概念,支持一个密文被多个用户解密.在广播加密中,数据发送者首先选择一组接收者,然后利用这一组接收者的公钥集合对数据进行加密,并通过公开信道传输密文.只有公钥属于集合里的用户(即授权用户)才能正确解密并获得明文数据,非授权用户即使合谋也不能得到加密数据的内容.这些优点使得广播加密具有重要的实用价值,在付费电视、云计算、物联网等应用中得到广泛使用.2007 年,Delerablée[6]与 Sakai 和 Furukawa[7]分别在各自的独立工作中结合标识加密和广播加密,提出标识广播加密(Identity-Based Broadcast Encryption,IBBE)的概念,通过公钥聚合的方法构造了第一个同时具有定长密文和用户私钥性质的标识广播加密方案.不足的是两个方案都只有静态选择明文安全性.Kim 等人[8]研究了具有自适应性安全性且定长密文的标识广播加密方案.随后,标识广播加密技术得到了进一步的研究和发展,实现了接收者隐私保护[9]、用户可撤销[10]、抗泄露[11]等功能.然而,现有标识广播加密方案以国外设计为主,缺乏由我国 SM9 商用密码扩展的标识广播加密方案.

1.1 本文贡献

面向密码技术自主先进、安全可控的战略需求,本文根据 SM9 标识加密算法的特点,结合 Delerablée 广播加密方案[6]的设计思路,提出了第一个基于我国 SM9 商用密码的标识广播加密方案.方案的设计只给出了密钥封装,即解密的结果是一个会话密钥.提出的方案最大化保留了 SM9 标识加密算法的结构,其中用户私钥生成算法与 SM9 中用户私钥生成算法相同,有助于与现有使用 SM9 的信息系统有效融合.方案中密文和用户私钥长度都是固定常数,与接收者数量无关.密文由三个元素组成,而用户私钥

只包含一个群元素. 与 SM9 标识加密(密钥封装)算法相比,密文只增加了一个群元素.

本文回顾了标识广播加密的定义和安全模型,在相应的安全模型中分析了方案的安全性并给出证明. 在随机谕言模型下证明方案可抵抗静态选择明文攻击. 方案的安全性基于 q-type GDDHE(General Decisional Diffie-Hellman Exponent)困难问题假设. 与目前最优的标识广播加密方案相比,基于我国 SM9 标识密码设计的新方案具有相当的计算效率和存储效率. 最后,对方案进行了编程仿真,当系统安全性设为 128 bits,接收者数量为 100 时,加密时间约为 72.92 ms,解密时间约为 135.89 ms.

1.2　相关工作

自 Fiat 和 Naor 提出广播加密[23]的概念后,广播加密得到了广泛的研究和应用. 广播加密最基本的安全要求是抗合谋攻击,即非授权用户合谋无法解密密文. Fiat 和 Naor 提出的广播加密方案只在有限个合谋者的情况下才是安全的. Naor 等人[24]随后提出了一个能够对除小部分撤销用户外完全抗合谋攻击的方案. Boneh 等人在文献[25]中提出第一个完全抗合谋攻击且具有定长密文和私钥的广播加密方案. 随后具有不同性质的广播加密方案被陆续提出[26-29].

Delerablée[6]与 Sakai 和 Furukawa[7]各自在他们的独立工作中提出标识广播加密的概念,并都采用用户公钥聚合方法构造了具有定长密文和私钥的标识广播加密方案. 在随机谕言模型下证明方案具有静态选择明文的安全性. 文献[8]采用对偶加密(Dual System Encryption)技术,提出一个在标准模型下具有适应性安全且固定密文长度的标识广播加密方案,但该设计中的系统公钥长度和私钥长度随接收者数量线性增长. 刘潇等人[12]结合 Delerablée 标识广播加密技术和 Boyen-Mei-Waters 方法,构造了具有定长密文和选择密文安全的标识广播加密方案.

Susilo 等人[13]研究如何在标识广播加密中,通过第三方撤销部分授权解密用户的解密权限,并提出接收者可撤销的标识广播加密方案. 第三方可以在不需要解密和知道明文的情况下,撤销部分接收者的解密权限. Xu 等人[14]基于云邮件应用,提出条件标识代理重加密的标识广播加密方案. 文献[11]研究了广播加密中抗泄露的问题,提出可抗持续泄露的标识广播加密方案. Lai 等人[15]结合广播加密和内积加密技术,提出一个内积型标识广播加密方案. 解密结果不再是明文,而是与明文和私钥相关的内积值,进一步保护数据隐私. 该研究在数据统计等特殊应用中有着重要的作用. 文献[10]提出具有用户撤销性质的标识广播加密方案. Jiang 等人[16]提出支持关键字搜索的标识广播加密方案,该方案能够抵抗内部攻击. Kim 等人[17]针对边缘计算提出具有外包解密性质的标识广播加密方案. 文献[18]提出用户私钥和密文长度都是常数的可问责标识广播加密方案. 标识广播加密中的用户隐私问题在文献[9,19-20]中得到了进一步的研究.

针对 SM9 标识密码的研究,Cheng[30]给出了 SM9 密钥协商协议和加密算法的正式安全性证明. 文献[31]研究了如何提高 SM9 数字签名计算性能,提出一种 SM9 数字签名及验证算法的快速实现方法,有效降低了算法运算的复杂度. 文献[32]提出一种关于 SM9 的可分离匿名分布式密钥产生分发方案,用户私钥生成是一个交互过程,该过程无双线性对运算且没有安全信道的要求. 文献[33]结合盲签名和 SM9 标识密码算法的特点,提出一种基于 SM9 的盲签名方案. 文献[34]以联盟链为基础,基于 SM9 提出一种可证明安全的区块链隐私防护方案,实现不可伪造、保证节点匿名和前向安全等性能. 综上所述,目前尚未发现基于 SM9 商用密码的标识广播加密公开研究成果.

1.3　本文组织结构

本文在第 2 节回顾双线性群、标识广播加密与安全模型的定义、困难问题假设等预备知识;第 3 节给出基于 SM9 的广播加密方案的具体构造;在第 4 节,根据安全模型证明方案的安全性,并在第 5 节对提出的方案进行性能分析和测试;第 6 节对本文进行总结.

2　预备知识

2.1　双线性群

假设 G_1,G_2,G_T 均是阶为大素数 N 的循环群,P,Q 分别是群 G_1,G_2 的生成元,双线性映射 e:$G_1\times G_2\rightarrow G_T$ 应满足以下 3 个条件:

(1) 双线性性. 对任意的生成元 $P\in G_1$,$Q\in G_2$ 和 a,$b\in Z_N$,都有 $e(aP,bQ)=e(P,Q)^{ab}$;

(2) 非退化性. 至少存在元素 $P_1\in G_1$,$P_2\in G_2$ 满足 $e(P_1,P_2)\neq 1$;

(3) 可计算性. 对于任意的 $P_1\in G_1$,$P_2\in G_2$,存在多项式时间算法高效计算 $e(P_1,P_2)$.

双线性群 BP 由以上五元组(G_1,G_2,G_T,e,N)组成. 若 $G_1=G_2$,则称该双线性群为对称双线性群,否则称为非对称双线性群. 此外,基于 Type II 的非对称双线性群中,存在有效的公开可计算同构映射 $\varphi:G_2\rightarrow G_1$,使得 $\varphi(Q)=P$. SM9 标识密码算法的构造基于 Type II 非对称双线性群.

2.2 标识广播加密形式化定义

一个标识广播加密方案由以下四个多项式时间算法构成.

(1) $Setup(\lambda,m)$. 以系统安全参数 λ 和系统支持的最大广播人数 m (整数)为输入,系统建立算法 $Setup$ 输出系统主公钥 mpk 和主私钥 msk. 该算法由密钥生成中心(KGC)运行.

(2) $KeyGen(mpk,msk,ID)$. 以系统主公钥 mpk,系统主私钥 msk 和用户标识 ID 为输入,用户私钥生成算法 $KeyGen$ 输出用户标识 ID 所对应的私钥 sk_{ID}. 该算法由 KGC 运行.

(3) $Encrypt(mpk,S)$. 以系统主公钥 mpk 和接收者标识集合 $S=(ID_1,ID_2,\cdots,ID_n)$ 为输入,其中 $n\leq m$,加密算法 $Encrypt$ 输出(C,K),其中 C 为封装密文(广播数据头),K 为封装密钥(会话密钥). 接收者标识集合 S 通常包含在封装密文 C 内.

当加密者(发送者)需要把数据 M 广播给用户集合 S 时,加密者首先通过 $Encrypt(mpk,S)$算法生成(C,K),然后选择安全的数据加密方案利用封装的会话密钥 K 产生数据 M 的密文 C_M,最后通过公共信道广播(C,C_M). 该算法由加密用户运行. 本文忽略数据加密算法的描述.

(4) $Decrypt(mpk,C,ID,S,sk_{ID})$: 以系统主公钥 mpk、封装密文 C、接收者标识 ID 以及 ID 对应的私钥 sk_{ID} 为输入,解密算法 $Decrypt$ 输出 K 或者 $\perp$. 如果解密算法输出的是 K,接收者通过数据加密方案的解密算法,利用 K 解密密文 C_M,恢复明文数据 M. 该算法由解密者执行.

标识广播加密方案的正确性要求对任意的 $(mpk,msk)\leftarrow Setup(\lambda,m)$, $sk_{ID}\leftarrow KeyGen(mpk,msk,ID)$和$(C,K)\leftarrow Encrypt(mpk,S)$,

$$Decrypt(mpk,C,ID,S,sk_{ID})=\begin{cases}K, & \text{如果 } ID\in S\\ \perp, & \text{其他}\end{cases}.$$

2.3 安全模型

根据文献[6],本节回顾标识广播加密的常见安全模型:在静态选择密文攻击下的密文不可区分性(Indistinguishability against selective Identity Chosen Ciphertext Attacks, IND-sID-CCA). 该安全模型通过攻击者和挑战者之间的游戏进行定义,包含以下几个阶段. 假设攻击者和挑战者都以最大广播人数 m 为输入.

初始化阶段. 攻击者首先给出一个挑战标识集合 $S^*=(ID_1^*,ID_2^*,\cdots,ID_{s^*}^*)$,其中 $s^*\leq m$.

系统建立阶段. 对于给定的安全参数 λ 和 m,挑战者运行算法 $Setup(\lambda,m)$,生成系统主公钥 mpk 和主私钥 msk,并发送生成的系统主公钥 mpk 给攻击者.

询问阶段 1. 在这一阶段,攻击者可以根据自己的需求适应性地向挑战者发起以下询问.

(1) 私钥生成询问. 攻击者可以询问任意标识 ID 对应的私钥,其中 $ID\notin S^*$. 挑战者运行用户私钥生成算法 $KeyGen$ 生成对应的私钥 sk_{ID},并把 sk_{ID} 发送给攻击者.

(2) 密文解密询问. 攻击者可以询问任意密文(C,S)的解密. 挑战者首先选择一个标识 $ID\in S$,运行用户私钥生成算法 $KeyGen$ 生成对应的私钥 sk_{ID},然后以 sk_{ID} 和 C 作为输入,运行解密算法 $Decrypt$,并把解密结果发送给攻击者.

挑战阶段. 当攻击者确定询问阶段 1 结束后,挑战者运行加密算法 $Encrypt(mpk,S^*)$生成挑战封装密文 C^* 和封装密钥 K^*. 接着挑战者随机选择一个比特 $\mu\in\{0,1\}$并设 $K_\mu=K^*$,并从对应的封装密钥空间中选择一个随机值并设为 $K_{1-\mu}$. 最后,挑战者发送(C^*,K_0,K_1)给攻击者.

询问阶段 2. 在这一阶段,攻击者可以根据自己的需求继续向挑战者发起私钥生成询问和密文解密询问. 但要求攻击者不能发起挑战封装密文 C^* 的解密询问. 挑战者根据询问阶段 1 回复攻击者.

猜测阶段. 最后,攻击者输出对 μ 的猜测 $\mu'\in\{0,1\}$. 如果 $\mu'=\mu$,则称攻击者获胜. 定义攻击者 A 获胜的优势为

$$Adv_A^{\mathrm{IBBE}}(\lambda)=\left|\Pr[\mu'=\mu]-\frac{1}{2}\right|.$$

定义 1. 在 IND-sID-CCA 安全模型中,如果对于任意的多项式时间攻击者 A,$Adv_A^{\mathrm{IBBE}}(\lambda)$都是可忽略的,那么称该方案是 IND-sID-CCA 安全的.

在 IND-sID-CCA 安全模型中,如果不允许攻击者在询问阶段 1 和询问阶段 2 中发起密文解密询问,则称该模型为静态选择明文安全模型,记为 IND-sID-CPA(Indistinguishability against selective Identity Chosen Plaintext Attacks). 本文方案的安全性分析基于该安全模型.

2.4　困难问题假设

本节对文献[6]中的困难问题进行修改，定义一个通用指数 Diffie-Hellman 困难问题假设，记为 (f,g)-GDDHE 假设，并在通用群模型(Generic Group Model)下分析了该假设的合理性. 本文提出的方案安全性依赖 (f,g)-GDDHE 问题的困难性. (f,g)-GDDHE 问题的描述如下：

(f,g)-GDDHE 问题. 假设 $BP=(G_1,G_2,G_T,e,N)$是与安全参数 λ 相关的非对称双线性群，f 和 g 是两个互质、阶分别为 t 和 m 的多项式，且根各不相同. 令 H_0 和 P_0 分别是群 G_1 和 G_2 的生成元，则 (f,g)-GDDHE 问题为：已知

$$\alpha P_0,\alpha^2 P_0,\cdots,\alpha^t P_0,\alpha^2 f(\alpha)P_0,k\alpha^2 f(\alpha)P_0,$$
$$H_0,\alpha H_0,\alpha^2 H_0,\cdots,\alpha^{2m}H_0,kg(\alpha)H_0,$$

和群 G_T 中的一个元素 T，判断 T 是否等于 $e(H_0,P_0)^{k\alpha f(\alpha)}$ 或者为 G_T 中的一个随机元素，α 是未知的.

令 I 是 (f,g)-GDDHE 困难问题实例的输入，事件 true 为 $T=e(H_0,P_0)^{k\alpha f(\alpha)}$，事件 false 为 $T\neq e(H_0,P_0)^{k\alpha f(\alpha)}$. 定义算法 D 解决 (f,g)-GDDHE 问题的优势为

$$Adv_D^{(f,g)\text{-GDDHE}}(\lambda)=$$
$$|\Pr[D(I)=1|\text{true}]-\Pr[D(I)=1|\text{false}]|.$$

定理 1.　(f,g)-GDDHE 假设. 在通用群模型中，不存在具有不可忽略优势的多项式时间算法 D 解决 (f,g)-GDDHE 困难问题.

在不影响困难性的前提下，本文在对称双线性群中分析 (f,g)-GDDHE 问题的困难性.

证明.　定理证明的思路与文献[8]中困难问题的证明方法类似. 不妨设 $H_0=P_0^{\beta}$，则 (f,g)-GDDHE 困难问题可重新阐述为

$$P=(\alpha,\alpha^2,\cdots,\alpha^t,\alpha^2 f(\alpha),k\alpha^2 f(\alpha),$$
$$\beta,\beta\alpha,\beta\alpha^2,\cdots,\beta\alpha^{2m},\beta kg(\alpha)),$$
$$Q=1,$$
$$F=k\alpha\beta f(\alpha).$$

根据文献[35]，需要证明 F 与 (P,Q) 无关，即不存在不是所有都为零的系数 $\{x_{i,j}\}$ 和 y_1 使得

$$k\alpha\beta f(\alpha)=F=\sum x_{i,j}d_i d_j+y_1,$$

其中 $d_i,d_j\in P$. 为了满足以上等式，任意两个 P 中元素的乘积必须包含 $k\alpha\beta$. 因此，可列出所有可能的乘积集合

$$P'=(k\beta\alpha^2 f(\alpha),k\beta\alpha^3 f(\alpha),\cdots,k\beta\alpha^{2m+2}f(\alpha),k\beta\alpha g(\alpha),$$
$$k\beta\alpha^2 g(\alpha),\cdots,k\beta\alpha^t g(\alpha),k\beta\alpha^2 f(\alpha)g(\alpha)).$$

由于 $k\beta\alpha^2 f(\alpha)g(\alpha)$ 可以通过 P' 中第一行线性表示，删除 $k\alpha\beta$ 后，P' 可以简化为

$$(\alpha f(\alpha),\alpha^2 f(\alpha),\cdots,\alpha^{2m+1}f(\alpha),$$
$$g(\alpha),\alpha g(\alpha),\cdots,\alpha^{t-1}g(\alpha)).$$

因此，

$$f(\alpha)=A(\alpha)f(\alpha)+B(\alpha)g(\alpha),$$

其中 $A(\alpha)$ 和 $B(\alpha)$ 都是多项式，满足 $A(0)=0$，$A(\alpha)$ 的阶小于 $2m+1$，$B(\alpha)$ 的阶小于 $t-1$. 又多项式 $f(\alpha)$ 和 $g(\alpha)$ 是互质的多项式，有 $f(\alpha)|B(\alpha)$. 由于 $f(\alpha)$ 的阶为 t，可以得出 $B(\alpha)=0$，即 $A(\alpha)=1$，这与 $A(0)=0$ 矛盾.　证毕.

3　方案构造

3.1　方案描述

为了方便与 SM9 信息系统有效融合，本节采用 SM9 标识加密算法中的符号描述方案.

(1) Setup. 给定安全参数 λ 和加密算法中允许最大接收者的数量 m，首先选择一个双线性群 $BP=(G_1,G_2,G_T,e,N)$，其中 G_1 和 G_2 的生成元分别为 P_1 和 P_2. 选择随机数 $\alpha\in\{1,N-1\}$，密码哈希函数 $H_1:\{0,1\}^*\to Z_N^*$，密钥派生函数 $KDF:\{0,1\}^*\to klen$，其中 $klen$ 为封装会话密钥的长度. 计算群 G_1 中的元素 $P_{pub}=(\alpha P_1,\alpha^2 P_1,\alpha^3 P_1,\cdots,\alpha^m P_1)$，计算群 G_2 中的元素 $u=\alpha^2 P_2$，计算群 G_T 中的元素 $g=e(P_1,P_2)^{\alpha}$. 接着选择用一个字节表示的加密私钥生成函数识别符 hid，设系统的主公钥为 $mpk=(u,g,P_1,P_{pub},H_1,hid,KDF)$，系统主私钥为 $msk=(\alpha,P_2)$.

(2) KeyGen. 给定用户的标识 ID，首先在有限域 F_N 上计算 $t_1=H_1(ID\|hid,N)+\alpha$，若 $t_1=0$，则需重新产生主公钥，计算和公开主公钥，并更新已有接收者的解密私钥；否则计算 $t_2=\alpha\cdot t_1^{-1}$，然后计算 $sk_{ID}=t_2\cdot P_2$，把 sk_{ID} 作为用户的解密私钥.

(3) Encrypt. 为了封装比特长度为 $klen$ 的密钥给用户集合 $S=(ID_1,ID_2,\cdots,ID_n)$，选取随机数 $r\in\{1,N-1\}$，计算 $C_1=-r\cdot u$，$w=g^r$，

$$C_2=r\cdot\prod_{i=1}^{n}(H_1(ID_i\|hid,N)+\alpha)\cdot P_1,$$
$$K=KDF(C_1\|C_2\|w\|S,klen).$$

输出 (K,C_1,C_2)，其中 K 是被封装的会话密钥，(C_1,C_2) 为封装密文. 根据算法描述，r,ID_i,hid 都是已知的，

$$C_2=r\cdot\prod_{i=1}^{n}(H_1(ID_i\|hid,N)+\alpha)\cdot P_1=r\cdot\sum_{j=0}^{n}z_i(\alpha^i P_1),$$

其中 z_i 是可计算的多项式系数. 又因为对任意 $i\in[1,m]$,$\alpha^i P_1$ 属于系统主公钥,因此 C_2 是可计算的.

(4) Decrypt. 假设接收者的标识为 ID_i,收到封装密文 (C_1,C_2) 后,计算

$$w'=(e(f_i(\alpha)\cdot P_1,C_1)\cdot e(C_2,sk_{ID_i}))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)}},$$

其中

$$f_i(\alpha)=\frac{1}{\alpha}\cdot\Big(\prod_{j=1,j\neq i}^{n}(H_1(ID_j\|hid,N)+\alpha)-\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)\Big),$$

并计算 $K'=KDF(C_1\|C_2\|w'\|S,klen)$,接收者最后输出 K'.

3.2 方案正确性分析

假设 $ID_i\in S$,则 $w'=w$,$K'=K$,其具体计算过程如下:

$$\begin{aligned}
w'&=(e(f_i(\alpha)\cdot P_1,C_1)\cdot e(C_2,sk_{ID_i}))^{\frac{1}{\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)}}\\
&=\Big(e\Big(\alpha^{-1}\Big(\prod_{j=1,j\neq i}^{n}(H_1(ID_j\|hid,N)+\alpha)-\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)\Big)\cdot P_1,-r\cdot\alpha^2\cdot P_2\Big)\cdot\\
&\quad e\Big(r\cdot\prod_{j=1}^{n}(H_1(ID_j\|hid,N)+\alpha)\cdot P_1,\\
&\quad \alpha\cdot(H_1(ID_j\|hid,N)+\alpha)^{-1}\cdot P_2\Big)\Big)^{\frac{1}{\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)}}\\
&=\Big(e\cdot\Big(\Big(\prod_{j=1,j\neq i}^{n}(H_1(ID_j\|hid,N)+\alpha)-\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)\Big)\cdot P_1,-r\cdot\alpha\cdot P_2\Big)\cdot\\
&\quad e\Big(\prod_{j=1,j\neq i}^{n}(H_1(ID_j\|hid,N)+\alpha)\cdot P_1,r\cdot\alpha\cdot P_2\Big)\Big)^{\frac{1}{\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)}}\\
&=e\Big(\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)\cdot P_1,r\cdot\alpha\cdot P_2\Big)^{\frac{1}{\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,N)}}\\
&=e(P_1,\alpha\cdot P_2)^r\\
&=g^r\\
&=w.
\end{aligned}$$

4 安全性分析

本节详细分析所提方案的安全性. 方案设计基于 SM9 标识加密算法的构造,实现多用户高效数据共享,其中用户私钥生成算法与 SM9 标识加密中的用户私钥生成算法完全一致. SM9 标识加密算法的安全性依赖于密码杂凑函数、密钥派生函数和随机数发生器等辅助函数. 这些辅助函数的强弱直接影响 SM9 标识加密算法的安全性. 本方案的设计也用到了 SM9 中的密码杂凑函数、密钥派生函数和随机数发生器等辅助函数. 因此,本文假设方案构造中涉及到的密码杂凑函数、密钥派生函数和随机数发生器等辅助函数都是安全的,在方案的证明中不考虑这些辅助函数的安全性. 但新方案的安全性证明与 SM9 加密算法的安全性证明[30]完全不同. 本文借鉴文献[6]中安全性证明的技巧分析方案的安全性,并得到定理 2.

定理 2. 令密码哈希函数 H_1 为随机谕言器. 如果 (f,g)-GDDHE 假设成立,则本文提出的方案是 IND-sID-CPA 安全的.

证明. 若存在一个 IND-sID-CPA 攻击算法 A 能够以不可忽略的优势 ε 攻破本文提出的方案,则我们可以构造一个模拟算法 B 通过与 A 交互,以 ε 的优势解决 (f,g)-GDDHE 困难问题.

令一次加密最大的接收者个数为 m,密钥询问次数和谕言器询问次数的总和为 t. 攻击算法 A 和模拟算法 B 都以 m,t 为输入,且模拟算法 B 给定 (f,g)-GDDHE 困难问题实例

$$\alpha P_0,\alpha^2 P_0,\cdots,\alpha^t P_0,\alpha^2 f(\alpha)P_0,k\alpha^2 f(\alpha)P_0 \quad (1)$$

$$H_0,\alpha H_0,\alpha^2 H_0,\cdots,\alpha^{2m}H_0,kg(\alpha)H_0 \quad (2)$$

和群 G_T 中的一个元素 T,判断 T 是否等于 $e(H_0,P_0)^{k\alpha f(\alpha)}$ 或者为 G_T 中的一个随机元素. 其中 $f(x)$ 和 $g(x)$ 是次数为 t 和 m 的互质多项式,对应群的阶为大素数 N,不失一般性,设

$$f(x)=\prod_{i=1}^{t}(x+x_i),\ g(x)=\prod_{i=t+1}^{t+m}(x+x_i),$$

对任意的 $i\in\{1,t\}$,定义 $f_i(x)=\frac{f(x)}{x+x_i}$. 对于任意的 $i\in\{t+1,t+m\}$,定义 $g_i(x)=\frac{g(x)}{x+x_i}$.

初始化阶段. 攻击算法 A 输出要攻击的挑战标识集合 $S^*=(ID_1^*,ID_2^*,\cdots,ID_{s^*}^*)$,其中 $s^*\leq m$.

系统建立阶段. 模拟算法 B 通过以下方法生成系统主公钥. 首先隐含地设置 $P_2=f(\alpha)P_0$,但是并不知道 P_2 的值. 随后,模拟算法 B 设置

$$P_1=\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)H_0,\ u=\alpha^2 P_2=\alpha^2 f(\alpha)P_0,$$

$$\alpha^j P_1=\alpha^j\cdot\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)H_0,\ j\in[1,m],$$

$$g=e(P_1,P_2)^{\alpha}=e(H_0,P_0)^{\alpha\cdot f(\alpha)\cdot\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)}.$$

不难看出，$P_1,\alpha^jP_1,j\in[1,m]$可以通过困难问题实例中(2)计算得到，$u$ 可以通过困难问题实例中(1)计算得到，g 可以通过困难问题实例中(1)和(2)计算得到. 最后，模拟算法 B 选择用一个字节表示的加密私钥生成函数识别符 hid，密钥派生函数 $KDF:\{0,1\}^*\rightarrow klen$，并定义

$$mpk=(u,g,P_1,P_{pub},hid,KDF),$$

其中 H_1 被看作是谕言器，由模拟算法 B 控制. 为方便描述，在 H_1 中省略 hid 和 N 的输入.

哈希询问阶段. 在任何时候，攻击算法 A 都可以向谕言器询问任意标识 ID_i 的哈希值 $H_1(ID_i\|hid,N)$. 不妨设攻击算法 A 发起私钥询问的次数为 q，则其最多询问 t-q 次的哈希值. 为应答这些询问，模拟算法 B 首先建立一个列表 L，列表 L 中存储数据是个三元组(ID_i,x_i,sk_{ID_i})，并设置初始状态为

$$\{(*,x_i,*)\}_{i=1}^{t},\ \{(ID_i,x_i,*)\}_{i=t+1}^{t+s^*},$$

其中“*”代表空. 当攻击算法 A 询问第 i 个标识 ID_i 的 H_1 哈希值时，模拟算法 B 按如下步骤回应：

(1) 若 ID_i 对应的三元组在列表 L 中，回复相应的 x_i.

(2) 否则，设 $H_1(ID_i\|hid,N)=x_i$，并更新列表 L 中的元组$(ID_i,x_i,*)$且发送 x_i 给 A.

询问阶段 1. 在这一阶段，攻击算法 A 可以适应性的向模拟算法 B 询问任意标识 $ID_i\notin S^*$ 对应的私钥，B 首先查询列表 L，并根据以下规则回复 A.

1. 若已询问过 ID_i 的私钥，则回复列表中相应的 sk_{ID_i}.

2. 否则，如果询问过 ID_i 的 H_1 哈希值，则获取相应的哈希值 x_i，计算

$$sk_{ID_i}=\alpha\cdot f_i(\alpha)P_0=\alpha\cdot\frac{1}{H_1(ID_i\|hid,N)+\alpha}P_2,$$

并把计算结果发送给 A. 不难看出，sk_{ID_i} 可以通过困难问题实例中(1)计算得到.

3. 否则执行 ID_i 的哈希 H_1 询问获取对应的哈希值 x_i，然后按步骤 2 生成对应的私钥 sk_{ID_i}，并发送 sk_{ID_i} 给 A.

挑战阶段. 当 A 决定询问阶段 1 结束后，B 计算

$$C_1^*=-k\alpha^2f(\alpha)P_0,\ C_2^*=kg(\alpha)H_0,$$

$$w^*=T^{\prod_{i=t+s^*+1}^{t+m}x_i}\cdot e\Big(\frac{1}{\alpha}\cdot\Big(\prod_{t+s^*+1}^{t+m}(\alpha+x_i)-\prod_{i=t+s^*+1}^{t+m}x_i\Big)H_0,k\alpha^2f(\alpha)P_0\Big).$$

最后计算 $K^*=KDF(C_1^*\|C_2^*\|w^*\|S^*,klen)$，并输出挑战封装密文$(C_1^*,C_2^*)$.

假设 $r^*=k$，容易验证得到

$$C_1^*=-k\alpha^2f(\alpha)P_0=-r^*\cdot u,$$

$$C_2^*=kg(\alpha)H_0=r^*\cdot\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)\cdot\prod_{i=t+1}^{t+s^*}(\alpha+x_i)H_0=r^*\cdot\prod_{i=t+1}^{t+s^*}(\alpha+H_1(ID_i^*\|hid,N))\cdot P_1.$$

如果 $T=e(H_0,P_0)^{k\alpha f(\alpha)}$，则

$$w^*=T^{\prod_{i=t+s^*+1}^{t+m}x_i}\cdot e\Big(\frac{1}{\alpha}\cdot\Big(\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)-\prod_{i=t+s^*+1}^{t+m}x_i\Big)H_0,k\alpha^2f(\alpha)P_0\Big)$$

$$=e(H_0,P_0)^{k\alpha f(\alpha)\cdot\prod_{i=t+s^*+1}^{t+m}x_i}\cdot e\Big(\Big(\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)-\prod_{i=t+s^*+1}^{t+m}x_i\Big)H_0,k\alpha f(\alpha)P_0\Big)$$

$$=e(H_0,P_0)^{k\alpha f(\alpha)\cdot\prod_{i=t+s^*+1}^{t+m}(\alpha+x_i)}=g^{r^*}.$$

因此，当 $T=e(H_0,P_0)^{k\alpha f(\alpha)}$ 时，挑战密文(C_1^*,C_2^*)是正确的封装密文.

询问阶段 2. 在这一阶段，攻击算法 A 可以继续发起用户私钥询问，模拟算法 B 按照询问阶段 1 的方法回复询问.

猜测阶段. 最后攻击算法 A 输出它的猜测 $\mu'\in\{0,1\}$. 如果 $\mu'=\mu$，模拟算法 B 输出 1 作为给定 (f,g)-GDDHE 困难问题实例的答案，意味着 $T=e(H_0,P_0)^{k\alpha f(\alpha)}$，否则输出 0，意味着 $T\neq e(H_0,P_0)^{k\alpha f(\alpha)}$.

接下来分析模拟算法 B 解决困难问题的优势. 不难得到

$$Adv_B^{(f,g)\text{-GDDHE}}(\lambda)=|\Pr[B(I)=1|\text{true}]-\Pr[B(I)=1|\text{false}]|=|\Pr[\mu=\mu'|\text{true}]-\Pr[\mu=\mu'|\text{false}]|.$$

从上述证明可知，当事件 true 发生时，对于攻击算法 A，模拟和真实攻击是不可区分的. 根据假设，攻击算法有 ε 的优势攻破方案，则在这种情况下，

$$\Pr[\mu=\mu'|\text{true}]=\frac{1}{2}+\varepsilon.$$

当 T 属于事件 false 时，T 是群 G_T 中的随机元素，且不等于 $e(H_0,P_0)^{k\alpha f(\alpha)}$. 在这种情况下，对于攻击算法，$w^*$ 是随机的，与 C_1^*,C_2^* 无关. 因此我们有 $\Pr[\mu=\mu'|\text{false}]=\frac{1}{2}$. 综上有，

$$Adv_B^{(f,g)\text{-GDDHE}}(\lambda)$$
$$=|\Pr[B(I)=1|\text{true}]-\Pr[B(I)=1|\text{false}]|$$
$$=|\Pr[\mu=\mu'|\text{true}]-\Pr[\mu=\mu'|\text{false}]|$$
$$=\left|\frac{1}{2}+\varepsilon-\frac{1}{2}\right|$$
$$=\varepsilon.$$ 证毕.

方案的安全性证明在随机谕言模型中完成,因此,方案可以利用 FO[35]转化技术实现 CCA 安全性.也可以与一次性签名技术(One-time signature)结合,实现 CCA 安全性,代价是增加存储开销或者计算开销.

5 方案性能分析

本节对基于 SM9 的广播加密方案进行性能分析,包括方案中各算法的计算效率和通信效率.2007 年 Delerablée 在文献[6]中提出具有定长密文和私钥的标识广播加密方案,密文和私钥长度与接收者的数量无关,在计算和通信效率上基本达到最优.后续标识广播加密的研究主要以实现不同功能和安全性为主,包括匿名性[9]、用户可撤销[10]、抗泄露[11]、选择密文安全[12]等.

5.1 理论分析

本小节首先从理论上对方案的通信效率和计算效率与文献[6]和文献[12]中提出的方案进行比较.通信效率的对比结果见表 1,其中$|G_1|$,$|G_2|$和$|G_T|$分别表示群 G_1,G_2和 G_T中元素的大小,m 是系统中一次加密允许的最大接收者数量,$|K|$表示数据加密密钥的大小,ROM(Random Oracle Model)表示随机谕言模型.从表 1 可以看出,本方案和文献[6]、文献[12]中的方案都具有定长的密文和私钥.密文都由三个元素组成,用户私钥都只有一个群元素.系统主公钥长度随最大接收者数量线性增长.由表 1 可知,方案在系统主公钥、用户私钥和密文的通信效率上和文献[6]、文献[12]相当.

表 1 方案通信效率比较

方案	公钥长度	私钥长度	密文长度
文献[6]	$\|G_T\|+\|G_1\|+(m+1)\|G_2\|$	$\|G_1\|$	$\|G_T\|+\|G_1\|+\|G_2\|$
文献[12]	$\|G_T\|+\|G_1\|+(m+1)\|G_2\|$	$\|G_1\|$	$\|G_T\|+\|G_1\|+\|G_2\|$
本方案	$\|G_T\|+\|G_2\|+(m+1)\|G_1\|$	$\|G_2\|$	$\|G_1\|+\|G_2\|+\|K\|$

计算效率的对比结果见表 2.三个方案都基于非对称双线性群设计,生成双线性群的操作可以预先完成,所以本文忽略这部分的计算开销.文献[6]和文献[12]中的方案设计采用乘法群表示,本文使用加法群表示.为方便比较,本文统一在加法群下统计计算开销并定义如下符号:SM_1表示群 G_1中的标量乘运算,SM_2表示群 G_2中的标量乘运算,p 表示双线性对运算,Et 表示群 G_T中的指数运算,m 是系统中一次加密允许的最大接收者数量,n 为加密算法中实际的接收者数量.表 2 表明,本方案中的各个算法在计算开销和目前最优的标识广播加密方案[6]相当.系统主公钥的计算开销为 $O(m)$,加密和解密的开销为 $O(n)$.虽然文献[12]中的方案具有选择密文安全性(CCA),但增加了约 2 倍的加密和解密的计算开销.

表 2 方案计算效率和安全性比较

方案	公钥生成	私钥生成	加密	解密	安全性	安全模型
文献[6]	mSM_2+SM_1+p	SM_1	$SM_1+(n+1)SM_2+Et$	$2p+(n-1)SM_2+Et$	IND-sID-CPA	ROM
文献[12]	$(m+1)SM_2+SM_1+p$	SM_1	$SM_1+(n+2)SM_2+Et$	$4p+2nSM_2+Et$	IND-sID-CCA	ROM
本方案	mSM_1+SM_2+p	SM_2	$(n+1)SM_1+SM_2+Et$	$2p+(n-1)SM_1+Et$	IND-sID-CPA	ROM

5.2 实验仿真

本小节对方案进行编程仿真,测试方案中各个算法的运行时间,并与文献[6]和文献[12]中的方案相比较.为测试方便,本文使用 PBC(Pairing-Based Cryptography)库,采用的椭圆曲线为 Type F,测试系统安全等级达到 128 bits($|G_1|=256$ bits)时方案的效率.测试环境中所用的设备是一台内存为 16.0 GB 的笔记本电脑,操作系统为 64 位的 Windows 10,CPU为Intel(R) Core(TM) i7-8558U@1.80 Hz 2.00 GHz,使用的编程语言为 C++.测试的结果如表 3 所示.在仿真中,假设最大用户数量和实际接收者数量是相等的且设为 100,即 $m=n=100$,结果取 100 次测试的平均值.从表 3 可以看出,当接收者数量为 100 时,本文提出的方案的加密时间约为 72.92 ms,解密时间约为 135.89 ms,在实际应用中是可行的.实验结果与理论分析一致.

表 3 方案算法仿真时间比较($m=n=100$)

方案	系统建立/ms	私钥生成/ms	加密/ms	解密/ms
文献[6]	192.59	0.66	157.43	215.00
文献[12]	191.23	0.68	160.52	437.32
本方案	113.54	1.43	72.92	135.89

6 总　结

本文基于我国商用密码 SM9 标识加密算法，设计了首个基于 SM9 的高效标识广播加密方案. 方案最大化地保留了 SM9 标识加密算法的结构，并支持多用户解密. 密文长度和用户私钥长度都是固定的，与接收者的数量无关. 在随机谕言模型下，我们证明方案能够抵抗静态选择明文攻击. 方案的安全性依赖于 q-type 的 GDDHE 困难假设. 实验仿真显示，新方案的计算开销和通信开销与目前国际主流的标识广播加密方案相当. 未来工作将在本文基础上增加新功能并对解密算法进行优化，实现快速解密.

参　考　文　献

[1] Shamir A. Identity-based cryptosystems and signature schemes //Proceedings of the 4th Annual International Cryptology Conference (CRYPTO 1984). Santa Barbara, USA, 1985: 47-53

[2] Boneh D, Franklin M K. Identity-based encryption from the Weil pairing//Proceedings of the 21st Annual International Cryptology Conference (CRYPTO 2001). Santa Barbara, USA, 2001: 213-229

[3] Hofheinz D, Jia Dingding, Pan Jiaxin. Identity-based encryption tightly secure under chosen-ciphertext attacks//Proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2018). Brisbane, Australia, 2018: 190-220

[4] Tseng Yuh-Min, Tsai Tung-Tso, Huang Sen-Shan, Huang Chung-Peng. Identity-based encryption with cloud revocation authority and its applications. IEEE Transactions on Cloud Computing, 2018, 6(4): 1041-1053

[5] Nishimaki R, Yamakawa T. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio//Proceedings of the 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2019). Beijing, China, 2019: 466-495

[6] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys//Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007). Kuching, Malaysia, 2007: 200-215

[7] Sakai R, Furukawa J. Identity-based broadcast encryption. IACR Cryptology ePrint Archive 2007: 217

[8] Kim J, Susilo W, Au M H, Seberry J. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 679-693

[9] He Kai, Weng Jian, Liu Jia-Nan, et al. Anonymous identity-based broadcast encryption with chosen-ciphertext security//Proceedings of the 11th Asia Conference on Computer and Communications Security (AsiaCCS 2016). Xi'an, China, 2016: 247-255

[10] Ge Aijun, Wei Puwen. Identity-based broadcast encryption with efficient revocation//Proceedings of the 22nd International Conference on Practice and Theory of Public Key Cryptography (PKC 2019). Beijing, China, 2019: 405-435

[11] Li Jiguo, Yu Qihong, Zhang Yichen. Identity-based broadcast encryption with continuous leakage resilience. Information Sciences, 2018, 429: 177-193

[12] Liu Xiao, Liu Wei-Ran, Wu Qian-Hong, Liu Jian-Wei. Chosen ciphertext secure identity-based broadcast encryption. Journal of Cryptography, 2015, 2(1): 66-76(in Chinese)
(刘潇，刘魏然，伍前红，刘建伟. 选择密文安全的基于身份的广播加密方案. 密码学报，2015，2(1)：66-76)

[13] Susilo W, Chen Rongmao, Guo Fuchun, et al. Recipient revocable identity-based broadcast encryption: How to revoke some recipients in IBBE without knowledge of the plaintext//Proceedings of the 11th on Asia Conference on Computer and Communications Security (AsiaCCS 2016). Xi'an, China, 2016: 201-210

[14] Xu Peng, Jiao Tengfei, Wu Qianhong, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. IEEE Transactions on Computers, 2016, 65(1): 66-79

[15] Lai Jianchang, Mu Yi, Guo Fuchun, et al. Identity-based broadcast encryption for inner products. The Computer Journal, 2018, 61(8): 1240-1251

[16] Jiang Peng, Guo Fuchun, Mu Yi. Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems. Theoretical Computer Science, 2019, 767: 51-72

[17] Kim J, Camtepe S, Susilo W, et al. Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing//Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. Auckland, New Zealand, 2019: 55-66

[18] Zhao Zhen, Guo Fuchun, Lai Jianchang, et al. Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. Theoretical Computer Science, 2020, 809: 73-87

[19] Zhang Leyou, Wu Qing, Mu Yi. Anonymous identity-based broadcast encryption with adaptive security//Proceedings of the 5th International Symposium on Cyberspace Safety and Security. Zhangjiajie, China, 2013: 258-271

[20] Xu Peng, Li Jingnan, Wang Wei, Jin Hai. Anonymous identity-based broadcast encryption with constant decryption complexity and strong security//Proceedings of the 11th on Asia Conference on Computer and Communications Security (AsiaCCS 2016). Xi'an, China, 2016: 223-233

[21] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext. IACR Cryptology ePrint Archive 2005: 15

[22] GM/T0044-2016. SM9 标识密码算法. 国家密码管理局. http://www.gmbz.org.cn/main/viewfile/20180110024736330 53.html

[23] Fiat A, Naor M. Broadcast encryption//Proceedings of the 13th Annual International Cryptology Conference (CRYPTO 1993). Santa Barbara, USA, 1994: 480-491

[24] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers//Proceedings of the 21st Annual International Cryptology Conference (CRYPTO 2001). Santa Barbara, USA, 2001: 41-62

[25] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys//Proceedings of the 25th Annual International Cryptology Conference (CRYPTO 2005). Santa Barbara, USA, 2005: 258-275

[26] Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts)//Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2009). Cologne, German, 2009: 171-188

[27] Libert B, Paterson K G, Quaglia E A. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model//Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography (PKC 2012). Darmstadt, Germany, 2012: 206-224

[28] Wu Qianhong, Qin Bo, Zhang Lei, et al. Contributory broadcast encryption with efficient encryption and short ciphertexts. IEEE Transactions on Computers, 2016, 65(2): 466-479

[29] Li Jiguo, Chen Liqing, Lu Yang, Zhang Yichen. Anonymous certificate-based broadcast encryption with constant decryption cost. Information Sciences, 2018, 454-455: 110-127

[30] Cheng Zhaohui. Security analysis of SM9 key agreement and encryption//Proceedings of the 14th International Conference on Information Security and Cryptology. Fuzhou, China, 2018: 3-25

[31] Wang Song, Fang Li-Guo, Han Lian-Bing, Liu Hong-Bo. Fast implementation of SM9 digital signature and verification algorithms. Communications Technology, 2019, 52(10): 2524-2527(in Chinese)
(王松, 房利国, 韩炼冰, 刘鸿博. 一种 SM9 数字签名及验证算法的快速实现方法. 通信技术, 2019, 52(10): 2524-2527)

[32] Xu Sheng-Wei, Ren Xiong-Peng, Yuan Feng, et al. A secure key issuing scheme of SM9. Computer Applications and Software, 2020, 37(1): 314-319(in Chinese)
(许盛伟, 任雄鹏, 袁峰等. 一种关于 SM9 的安全密钥分发方案. 计算机应用与软件, 2020, 37(1): 314-319)

[33] Zhang Xue-Feng, Peng Hua. Blind signature scheme based on SM9 algorithm. Netinfo Security, 2019, 19(8): 61-67(in Chinese)
(张雪锋, 彭华. 一种基于 SM9 算法的盲签名方案研究. 信息网络安全, 2019, 19(8): 61-67)

[34] Yang Ya-Tao, Cai Ju-Liang, Zhang Xiao-Wei, Yuan Zheng. Privacy preserving scheme in blockchain with provably secure based on SM9 algorithm. Journal of Software, 2019, 30(6): 1692-1704(in Chinese)
(杨亚涛, 蔡居良, 张筱薇, 袁征. 基于 SM9 算法可证明安全的区块链隐私保护方案. 软件学报, 2019, 30(6): 1692-1704)

[35] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes//Proceedings of the 19th Annual International Cryptology Conference (CRYPTO'99). Santa Barbara, USA, 1999: 537-554

LAI Jian-Chang, Ph. D., associate professor. His current major research interest is public-key cryptography and information security.

HUANG Xin-Yi, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

HE De-Biao, Ph. D., professor, Ph. D. supervisor. His main research interests include cryptography and information security.

Background

Date encryption has been regarded as one of the most promising approaches to protect data security and privacy. Traditional public-key encryption system requires a certificate for each user to guarantee the validity of user public key. While the verification of certificates is usually cost and the management of certificates is complex. To address this issue, Shamir introduced identity-based cryptosystem (IBC) in 1984, where user public keys can be an arbitrary string that identifies the user uniquely, such as phone number, email address. Du to these merits, IBC has received extensive attention. However, almost twenty years later, Boneh and Franklin proposed the first practical and provable secure

identity-based encryption (IBE) scheme under pairings in 2001. Since the pioneering work of Boneh and Franklin, IBE has been studied extensively and used to construct various schemes to satisfy new applications. Nevertheless, most of practical IBE schemes were designed by the foreigner. In this situation, our country designed a series of identity-based algorithms, called SM9, including digital signature, key exchange protocol, key encapsulation mechanism (KEM) and public key encryption, and later SM9 has become a cryptographic industry standard. But, the encryption algorithm is designed for single user only. It is inefficient when a data needs to be sent to multi-user simultaneously. In order to address this issue, the concept of broadcast encryption was introduced, which allows a sender to encrypt a data for a group of specified users. However, there does not exist any broadcast encryption construction based on SM9.

In this paper, we fill this gap by proposing the first identity-based broadcast encryption scheme based on SM9. The construction is built on SM9 KEM and allows a data to be shared with multi-user. The proposed scheme has constant size ciphertexts as well as private keys, which is independent of the number of receivers. More precisely, the ciphertexts consist of three elements and private key is composed of one group element only. The price to pay is an increase of public keys. We give the definition of identity-based broadcast encryption and its security models. We formally analyze the security of the proposed scheme and prove that the proposed scheme is secure against selective chosen-plaintext attacks under a q-type GDDHE assumption. The security is completed in the random oracle model. The theoretical analysis and demonstration show that the proposed scheme is comparable to the existing optimal IBBE schemes in terms of computational overheads and communication overheads.

This work is supported in part by the National Natural Science Foundation of China under Grant Nos. 61902191, 62032005, 61872089, 61972294, 61932016), in part by the Natural Science Foundation of Jiangsu Province under Grant No. BK20190696, and in part by the Natural Science Foundation of Fujian Province under Grant No. 2020J02016.