多接收者证书基可搜索加密方案

刘 行 明 洋 王晨豪 赵 一
(长安大学信息工程学院 西安 710064)

摘 要 可搜索加密作为一种加密原语,允许用户在云存储服务器中搜索文件的同时确保原始文件的机密性.证书基可搜索加密在实现密文检索的基础上,解决了证书管理、密钥托管、安全信道等问题.然而,已有的证书基可搜索加密要么使用耗时的双线性映射操作,要么无法满足发送者匿名特性.同时其仅考虑单个接收者,致使多个接收者场景下效率低,不能满足现实需求.为解决上述不足,基于椭圆曲线密码学,利用密钥交换思想和数字签名技术,本文提出多接收者证书基可搜索加密方案.对于相同数据,方案中发送者仅仅执行一次加密,即可使得多个接收者能够同时进行搜索.同时,发送者使用自己的私钥和证书生成密文,导致敌手无法生成有效密文发动关键词猜测攻击,确保了搜索陷门的安全性.本文所提方案中搜索陷门仅由一个群元素组成,同时没有泄露发送者的身份信息实现了匿名性.安全性分析表明,在随机预言机模型中,基于计算性 Diffie-Hellman 假设,本文所提方案能够满足适应性选择关键词攻击的不可区分性和适应性关键词猜测攻击的不可区分性.性能分析表明,与相关方案相比,本文所提方案实现了低的计算代价和通信代价,更加适用于云存储环境下的多用户服务场景.

关键词 可搜索加密;证书基密码学;多接收者;可证明安全;云存储
中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.00544

Multi-Recipient Certificate-Based Searchable Encryption Scheme

LIU Hang MING Yang WANG Chen-Hao ZHAO Yi
(*School of Information Engineering, Chang'an University, Xi'an* 710064)

Abstract With the development of cloud computing, more and more data are outsourced to cloud servers for the purpose of freeing up local storage resources. Taking the privacy problem into account, the data are typically encrypted before outsourcing. However, the encryption operation will break the structure of underlying data, making the retrieval function limited. Searchable encryption (SE), as an encryption primitive, allows users to search encrypted files in cloud storage servers while ensuring the security of the original files. Although public-key encryption with keyword search (PEKS) solves the ciphertext retrieval problem in the public key scenario, it suffers from the inherent certificate management problem in the traditional public key infrastructure setting. Subsequently, scholars have solved this problem by combining PEKS with identity-based cryptography (IBC) or certificateless cryptography (CLC). However, IBC and CLC also have the key escrow or secure channel problem. The former means that the private keys of all users will be leaked once the private key generator in IBC is compromised. The latter implies that the (partial) private key of the user needs to be transmitted over a secure channel in IBC and CLS. Certificate-based searchable encryption (CBSE) solves the problems of certificate management, key escrow, and secure channel on the basis of realizing ciphertext retrieval. Nevertheless, existing CBSE schemes either use time-consuming bilinear pairing operations resulting in efficiency problems or use the

收稿日期:2023-01-12;在线发布日期:2023-12-25.本课题得到国家自然科学基金(62072054)、陕西省重点研发计划(2021GY-047,2022GY-032)、西安市科技计划(23ZDCYJSGG0009-2022)、中央高校基本科研业务费专项资金(300102242201)资助.**刘 行**,博士研究生,主要研究方向为公钥密码学、区块链技术.E-mail:2022024015@chd.edu.cn.**明 洋**(通信作者),博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为密码学、信息安全.E-mail:yangming@chd.edu.cn.**王晨豪**,博士研究生,主要研究方向为公钥密码学、数字孪生安全.**赵 一**,博士,讲师,主要研究方向为密码学、网络安全.

sender's identity information as part of the search trapdoor, which leads to the failure to meet the property of sender anonymity. At the same time, existing schemes only consider the situation where a single recipient performs the search function, which leads to inefficiency in the scenario of multiple recipients and does not meet the practical requirements. In order to solve the above problems, based on elliptic curve cryptography, the multi-recipient certificate-based searchable encryption (MRCBSE) scheme is put forward using the key exchange protocol and digital signature technology. In the proposed scheme, for the same data, the sender only needs to perform the encryption operation once to generate a ciphertext that can be searched by multiple recipients at the same time. Also, the sender generates the ciphertext using its own private key and certificate, such that the adversaries cannot produce a valid ciphertext to launch the keyword guessing attack, ensuring the security of the search trapdoor. The search trapdoor of the proposed scheme consists of only one group element and does not reveal the identity information of the sender, thus achieving the property of sender anonymity. The formal definition and the corresponding security model of MRCBSE are given. Subsequently, based on the computational Diffie-Hellman assumption, the proposed scheme is proved to satisfy the indistinguishability under adaptive chosen keyword attack and the indistinguishability under adaptive keyword guessing attack in random oracle. Performance analysis results show that, in comparison with the related schemes, the proposed scheme not only has obvious advantages in terms of computation cost and communication cost but also realizes more security features, meaning that it is more suitable for multi-user service scenarios in cloud storage environments.

Keywords　searchable encryption; certificate-based cryptography; multi-recipient; provable security; cloud storage

1　引　言

随着云计算技术[1]的快速发展，云存储为互联网上共享海量数据提供了便捷，实现了无处不在的按需访问. 如今，人们经常上传照片和视频等个人数据到云服务器中，在释放本地存储资源的同时还可以通过云存储的社交网络应用程序与朋友分享数据. 然而，云存储存在严重数据泄露的安全隐患[2-4]. 例如，2020 年 3 月，新浪微博发生数据外泄事件①；2021 年 8 月，阿里云擅自泄露用户隐私数据事件②. 数据泄露主要是由恶意攻击者或云服务运营商的不端行为所引起的. 直觉上解决该问题的方法是将数据上传到云服务器之前进行加密操作. 然而，如何对加密后的数据进行检索成为云存储服务的新难题. 可搜索加密(Searchable Encryption，SE)技术作为一种密码学原语，能够在保护用户数据隐私的同时，实现云存储中密文数据的检索.

可搜索加密分为对称可搜索加密[5](Searchable Symmetric Encryption，SSE)和公钥可搜索加密[6-7](Public-key Encryption with Keyword Search，PEKS). 由于对称加密固有的密钥分配问题，使得 SSE 仅仅局限于单用户模型难以扩展到多用户共享场景. 在 PEKS 中，发送者除了对共享的数据进行加密外，还使用接收者的公钥加密数据的关键词. 云服务器根据接收者生成的搜索陷门进行密文检索. PEKS 需要满足选择关键词攻击(Chosen Keyword Attack，CKA)和关键词猜测攻击(Keyword Guessing Attack，KGA)下的安全性. 前者保证了敌手在获得一个关键词的密文后，无法得知加密的关键词信息. 后者保证了敌手在获得一个搜索陷门后，无法猜测其对应的关键词.

虽然 PEKS 在不泄露明文信息的情况下使得云服务器能够对用户的密文进行检索，但是其在多用户场景中的效率并不理想. 在云存储环境下，用户往往需要将数据同时发送给多个接收者，即发送者需要为每一个接收者生成对应的关键词密文，导致发送者的计算开销和云服务器的存储代价增大，云服务器的检索效率降低.

① http://tech.cnr.cn/techgd/20200324/t20200324_525028413.shtml
② https://www.ccdi.gov.cn/pl/202108/t20210825_248870.html

结合传统公钥密码学和身份基密码学(Identity-Based Cryptography,IBC),Gentry[8]提出了证书基密码学(Certificate-Based Cryptography,CBC).在CBC中,用户自己生成公钥和私钥并向证书权威申请相应的证书.在私钥和证书共同作用下,用户完成解密或签名.证书将用户身份和公钥绑定,提供了隐式的身份认证功能.用户不需要了解其他人的证书及状态简化了证书管理.证书权威仅仅知道用户的公钥信息解决了密钥托管.同时用户证书不需要通过安全信道进行传输.

通过结合CBC和SE技术,Lu等人[9-10]提出了证书基可搜索加密(Certificate-Based Searchable Encryption,CBSE)方案.在CBSE中,用户向认证权威注册获得证书成为合法用户,使用自己的私钥和证书生成合法的密文和搜索陷门.然而,方案[9]采用了耗时的双线性映射操作导致效率问题;发送者的身份信息作为部分搜索陷门,致使方案[10]的陷门信息泄露了发送者身份隐私.

当面对发送者向多个接收者同时发送相同数据的场景,如果应用方案[9-10]来实现多个接收者密文检索需求,发送者必须使用每一个接收者的公钥分别加密相同的关键词,导致了较高的计算代价和通信代价.

针对上述问题,本文提出了多接收者证书基可搜索加密方案.据作者所知,这是第一个实现多接收者密文检索的证书基可搜索加密方案.本文主要贡献如下:

(1)利用密钥交换思想[11]和数字签名技术[12],本文提出了多接收者证书基可搜索加密方案.所提方案中发送者能够直接为多个接收者生成可搜索的关键词密文,从而减少了发送者的计算代价和云服务器的存储代价,提高了云服务器的检索效率.此外,搜索陷门仅由一个群元素组成,并且没有泄露发送者的身份信息,实现了对发送者隐私信息的保护.

(2)本文给出了多接收者证书基可搜索加密的形式化定义和安全模型.安全性分析表明,在随机预言机模型中,基于计算性Diffie-Hellman假设,所提方案满足适应性选择关键词攻击的不可区分性和适应性关键词猜测攻击的不可区分性.

(3)理论和实验分析表明,所提方案在80比特的安全等级下,当接收者数量为100时,关键词加密时间约为110.06 ms;当关键词数量为100时,搜索陷门生成时间约为57.20 ms,密文匹配时间约为28.60 ms.与已有的证书基可搜索加密方案相比,所提方案具有最优的计算代价和通信代价.

2 相关工作

2004年,Boneh等人[6]利用身份基加密[13]首次提出了PEKS方案,解决了公钥场景中的密文检索问题.但是在文献[6]中,接收者需要通过安全信道将搜索陷门发送给云服务器,降低了PEKS的实用性.Baek等人[14]使用接收者和指定测试者的公钥对关键词进行加密,提出了无安全信道的公钥可搜索加密(Secure Channel Free PEKS,SCF-PEKS).Rhee等人[15]进一步优化了文献[14]的安全模型并构造了新的SCF-PEKS方案.

针对搜索陷门中的关键词隐私,Byun等人[16]提出了KGA,即攻击者在获得搜索陷门后能够找到对应的关键词.Xu等人[17]引入模糊函数对关键词进行模糊化处理从而抵抗KGA.Huang等人[18]将认证技术结合到PEKS中来抵抗KGA.但是,Noroozi等人[19]指出文献[17]在多用户下不能抵抗KGA.Chen等人[20]通过引入辅助服务器来抵抗KGA.然而,云存储服务器能够冒充正常用户和辅助服务器交互发起在线KGA.2020年,Zhao等人[21]通过使用损耗陷门函数[22],在服务器辅助框架下提出了能够抵抗在线KGA的一般性构造.

Abdalla等人[23]结合身份基密码学和PEKS提出身份基可搜索加密(Identity-Based Encryption with Keyword Search,IBEKS),解决了基于PKI下PEKS方案中复杂的证书管理问题.然而,IBEKS存在着内在密钥托管问题,即私钥生成中心拥有所有用户的私钥.针对该问题,学者们[24-31]提出了无证书可搜索加密(CertificateLess PEKS,CLPEKS).该方案中用户私钥由密钥产生中心生成的部分私钥和用户的秘密值组成,解决了密钥托管问题.但是,部分私钥需要通过安全信道分发给用户限制了实用性.

为了解决基于PKI下PEKS的证书管理问题,IBEKS的密钥托管问题以及CLPEKS的安全信道问题,Lu等人[9-10]将PEKS扩展到CBC中,分别基于双线性映射和椭圆曲线密码学构造了CBSE方案.尽管方案[10]构造了高效的无双线性映射的CBSE方案,但是其搜索陷门泄露了发送者的身份隐私信息.此外,方案[9-10]在多接收者场景下的计算代价和通信代价较大.

为了提高多接收者场景下的效率,Hwang等人[32]提出了多用户的支持连接关键词搜索的PEKS方案,显著降低了计算代价和通信代价.Lu

等人[33]利用多个接收者的身份信息构造多项式，提出了隐私保护的多接收者 CLPEKS 方案. 然而，该方案的搜索陷门泄露了发送者的身份隐私信息. 利用随机数重用的思想，Ma 等人[34]构造了支持连接关键词搜索的多接收者 CLPEKS 方案. 基于方案[33]，Yang 等人[35]在 PKI 场景下提出了高效的多接收者PEKS方案. 考虑到方案[34]无法抵抗 KGA，Chenam 等人[36]基于指定测试者和认证技术，构造了安全的多接收者 CLPEKS 方案. 然而，这些方案[32-36]存在着证书管理或安全信道问题.

3　预备知识

3.1　椭圆曲线密码学

Miller[37]提出椭圆曲线密码学，椭圆曲线定义如下：

令 p 为大素数，a,b 为有限域$\mathbb{F}_p$上的元素，$y^2=x^3+ax+b(\mathrm{mod}\ p)$在$\mathbb{F}_p$上确定了一条非奇异椭圆曲线 E. E 上所有的有理点(包括无穷远点 O)构成了素数 q 阶的加法循环群$\mathbb{G}$，其生成元记为 P，$kP=P+P+\cdots+P$(k 次)表示标量乘法操作. 本文使用仿射坐标系下的坐标表示方法，即点 G 的坐标表示为 $G=(x_G,y_G)$.

3.2　困难问题及假设

计算性 Diffie-Hellman (CDH) 问题[37]. 给定 $(P,aP,bP)\in\mathbb{G}$，其中$(a,b)\in\mathbb{Z}_q^*$ 且未知，求解 abP.

定义概率多项式时间算法$\mathcal{A}$解 CDH 问题的优势为

$$Adv_{\mathcal{A}}^{\mathrm{CDH}}=\Pr[\mathcal{A}(P,aP,bP)=abP].$$

计算性 Diffie-Hellman(CDH)假设[37]. 对于任何概率多项式时间算法$\mathcal{A}$，$Adv_{\mathcal{A}}^{\mathrm{CDH}}$是可忽略的.

3.3　密钥交换

密钥交换是由 Diffie 和 Hellman[11]提出的一种安全通信协议. 该协议使得通信双方协商一个会话密钥在不安全信道上进行安全通信. 具体如下：

令$\mathbb{G}$为非奇异椭圆曲线 E 上素数 q 阶的加法循环群，P 为其生成元. 用户 A 和用户 B 的公私钥对分别为$(PK_A=aP,SK_A=a)$和$(PK_B=bP,SK_B=b)$，其中$a,b\in\mathbb{Z}_q^*$. 那么A和B的会话密钥为$K_{AB}=a\cdot PK_B=abP=b\cdot PK_A=K_{BA}$.

3.4　数字签名

数字签名[12]是一种鉴别数字信息完整性的方法. 通过为数据信息附加上额外的不可伪造信息，使得接收方能够验证该数据信息完整性，同时发送方也不能否认自己的行为.

数字签名方案包含 3 个多项式时间算法.

(1) 密钥生成算法 KeyGen(λ)：该算法由发送方执行. 输入安全参数 λ，发送方生成私钥 SK 和公钥 PK.

(2) 签名生成算法 Sign(m,SK)：该算法由发送方执行. 输入消息 m 和私钥SK，发送方生成签名 σ.

(3) 签名验证算法 Verify(m,PK,σ)：该算法由接收方执行. 输入消息 m，公钥 PK 和签名 σ，如果 σ 是PK 下 m 的有效签名，接收方输出 1，否则输出 0.

3.5　系统模型

图 1 给出了多接收者证书基可搜索加密的系统模型，包含证书权威、发送者、多个接收者和云服务器.

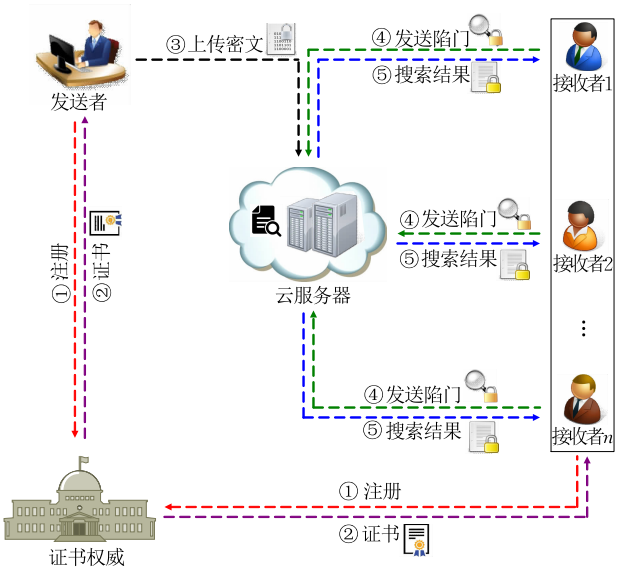

图 1　系统模型

(1) 证书权威：诚实好奇的实体，负责生成系统参数和用户注册.

(2) 发送者：生成数据密文和相应的关键词密文，并将其存储在云服务器中.

(3) 接收者：当从云服务器中检索数据时，生成关键词的搜索陷门发送给云服务器.

(4) 云服务器：诚实好奇的实体，负责存储密文和响应接收者的搜索请求.

3.6　多接收者证书基可搜索加密形式化定义

定义 1.　多接收者证书基可搜索加密方案包含 6 个多项式时间算法.

(1) 系统建立算法 Setup(λ)：该算法由证书权威执行. 输入安全参数 λ，证书权威生成系统参数 $params$ 和主私钥 msk.

(2) 用户密钥生成算法 UserKenGen($params$)：该算法由用户执行. 输入系统参数 $params$，用户生成私钥 SK_u和部分公钥 P_u.

(3) 证书生成算法 CertGen($params, msk, id_u, P_u$)：该算法由证书权威执行. 输入系统参数 $params$，主私钥 msk，用户身份 id_u 和用户部分公钥 P_u，证书权威生成用户证书 $cert_u$ 和用户公钥 PK_u.

(4) 关键词加密算法 KwEnc($params, id_s, SK_s, cert_s, \{id_1, \cdots, id_n\}, \{PK_1, \cdots, PK_n\}, w$)：该算法由发送者执行. 输入系统参数 $params$，发送者身份 id_s，私钥 SK_s，证书 $cert_s$，接收者身份 $\{id_1, \cdots, id_n\}$，公钥 $\{PK_1, \cdots, PK_n\}$ 和关键词 w，发送者输出密文 C_w.

(5) 搜索陷门生成算法 TrapGen($params, id_i, SK_i, cert_i, id_s, PK_s, w'$)：该算法由接收者执行. 输入系统参数 $params$，接收者身份 id_i，私钥 SK_i，证书 $cert_i$，发送者身份 id_s，公钥 PK_s 和关键词 w' 作为输入，接收者输出搜索陷门 $T_{w'}$.

(6) 密文匹配算法 Test($params, C_w, T_{w'}$)：该算法由云服务器执行. 输入系统参数 $params$，密文 C_w 和搜索陷门 $T_{w'}$，如果 C_w 和 $T_{w'}$ 匹配，云服务器输出 1，否则输出 0.

正确性：对于任意关键词 w 和 $id_i \in \{id_1, \cdots, id_n\}$，如果 $C_w \leftarrow$ KwEnc($params, id_s, SK_s, cert_s, \{id_1, \cdots, id_n\}, \{PK_1, \cdots, PK_n\}, w$)，$T_w \leftarrow$ TrapGen($params, id_i, SK_i, cert_i, id_s, PK_s, w$)，那么 $1 \leftarrow$ Test($params, C_w, T_w$).

3.7 安全模型

多接收者证书基可搜索加密的安全模型包含两种类型攻击者：类型 I 攻击者 $\mathcal{A}_{\mathrm{I}}$ 和类型 II 攻击者 $\mathcal{A}_{\mathrm{II}}$. $\mathcal{A}_{\mathrm{I}}$ 表示未经认证的外部敌手或诚实好奇的云服务器. $\mathcal{A}_{\mathrm{II}}$ 表示诚实好奇的证书权威.

多接收者证书基可搜索加密的安全性应该满足适应性选择关键词攻击的不可区分性(Indistinguishability under Adaptive Chosen Keyword Attack, IND-CKA)和适应性关键词猜测攻击的不可区分性(Indistinguishability under Adaptive Keyword Guessing Attack, IND-KGA). IND-CKA 和 IND-KGA 分别保证了密文和搜索陷门的隐私不被泄露.

多接收者证书基可搜索加密的安全模型由挑战者 $\mathcal{C}$ 与攻击者之间的交互游戏定义. 攻击者能够进行以下询问：

哈希询问：给定哈希询问，$\mathcal{C}$ 输出随机值.

创建用户询问：对 id_i 进行创建用户询问，$\mathcal{C}$ 返回 id_i 的公钥 PK_i.

私钥提取询问：对 id_i 进行私钥提取询问，$\mathcal{C}$ 返回 id_i 的私钥 SK_i.

证书提取询问：对 id_i 进行证书提取询问，$\mathcal{C}$ 返回 id_i 的证书 $cert_i$.

陷门询问：对 $\{id_s, id_r, w_i\}$ 进行陷门询问，$\mathcal{C}$ 返回搜索陷门 T_{w_i}.

游戏 IND-CKA-I：挑战者 $\mathcal{C}$ 和攻击者 $\mathcal{A}_{\mathrm{I}}$ 进行如下交互：

初始化阶段. $\mathcal{C}$ 运行算法 Setup(λ) 生成 $params$ 和 msk，将 $params$ 发送给 $\mathcal{A}_{\mathrm{I}}$.

阶段 1. $\mathcal{A}_{\mathrm{I}}$ 适应性地进行哈希询问、创建用户询问、私钥提取询问、证书提取询问和陷门询问.

挑战阶段. $\mathcal{A}_{\mathrm{I}}$ 选择两个关键词 w_0^* 和 w_1^*，以及发送者身份 id_s^* 和接收者身份 $\{id_1^*, \cdots, id_n^*\}$ 发送给 $\mathcal{C}$. $\mathcal{C}$ 随机选择 $\xi \in \{0,1\}$，运行算法 KwEnc($params, SK_s^*, cert_s^*, \{id_1^*, \cdots, id_n^*\}, \{PK_1^*, \cdots, PK_n^*\}, w_\xi^*$) 生成挑战密文 $C_{w_\xi^*}^*$ 发送给 $\mathcal{A}_{\mathrm{I}}$.

阶段 2. $\mathcal{A}_{\mathrm{I}}$ 进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^* \in \{id_s^*, id_1^*, \cdots, id_n^*\}$，$\mathcal{A}_{\mathrm{I}}$ 不能进行私钥提取询问和证书提取询问.

(2) 对于 $id^* \in \{id_1^*, \cdots, id_n^*\}$，$\mathcal{A}_{\mathrm{I}}$ 不能对 $\{id_s^*, id^*, w_0^*\}$ 和 $\{id_s^*, id^*, w_1^*\}$ 进行陷门询问.

猜测阶段. $\mathcal{A}_{\mathrm{I}}$ 输出猜测 $\xi' \in \{0,1\}$. 若 $\xi' = \xi$，则 $\mathcal{A}_{\mathrm{I}}$ 赢得游戏.

定义 $\mathcal{A}_{\mathrm{I}}$ 赢得游戏 IND-CKA-I 的优势为

$$Adv_{\mathcal{A}_{\mathrm{I}}}^{\text{IND-CKA-I}} = \left| \Pr[\xi' = \xi] - \frac{1}{2} \right|.$$

游戏 IND-CKA-II：挑战者 $\mathcal{C}$ 和攻击者 $\mathcal{A}_{\mathrm{II}}$ 进行如下交互：

初始化阶段. $\mathcal{C}$ 运行算法 Setup(λ) 生成 $params$ 和 msk，将 $\{params, msk\}$ 发送给 $\mathcal{A}_{\mathrm{II}}$.

阶段 1. $\mathcal{A}_{\mathrm{II}}$ 适应性地进行哈希询问、创建用户询问、私钥提取询问和陷门询问.

挑战阶段. 与游戏 IND-CKA-I 相同.

阶段 2. $\mathcal{A}_{\mathrm{II}}$ 进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^* \in \{id_s^*, id_1^*, \cdots, id_n^*\}$，$\mathcal{A}_{\mathrm{II}}$ 不能进行私钥提取询问.

(2) 对于 $id^* \in \{id_1^*, \cdots, id_n^*\}$，$\mathcal{A}_{\mathrm{II}}$ 不能对 $\{id_s^*, id^*, w_0^*\}$ 和 $\{id_s^*, id^*, w_1^*\}$ 进行陷门询问.

猜测阶段. 与游戏 IND-CKA-I 相同.

定义 $\mathcal{A}_{\mathrm{II}}$ 赢得游戏 IND-CKA-II 的优势为

$$Adv_{\mathcal{A}_{\mathrm{II}}}^{\text{IND-CKA-II}} = \left| \Pr[\xi' = \xi] - \frac{1}{2} \right|.$$

定义 2. 如果任何多项式时间攻击者赢得游戏 IND-CKA-I 和 IND-CKA-II 的优势 $Adv_{\mathcal{A}_{\mathrm{I}}}^{\text{IND-CKA-I}}$，

$Adv_{\mathcal{A}_{\mathrm{II}}}^{\text{IND-CKA-II}}$是可忽略的，那么本文所提方案是 IND-CKA 安全的.

游戏 IND-KGA-I：挑战者$\mathcal{C}$和攻击者$\mathcal{A}_{\mathrm{I}}$进行如下交互：

初始化阶段. 与游戏 IND-CKA-I 相同.

阶段 1. 与游戏 IND-CKA-I 相同.

挑战阶段. $\mathcal{A}_{\mathrm{I}}$选择两个关键词 w_0^*和 w_1^*，以及发送者身份id_s^*和接收者身份 id_r^* 发送给$\mathcal{C}$. $\mathcal{C}$随机选择 $\xi\in\{0,1\}$，运行算法 TrapGen($params, id_r^*, SK_r^*, cert_r^*, id_s^*, PK_s^*, w_\xi^*$)生成挑战陷门 $T_{w_\xi^*}^*$发送给$\mathcal{A}_{\mathrm{I}}$.

阶段 2. $\mathcal{A}_{\mathrm{I}}$进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^*\in\{id_s^*, id_r^*\}$，$\mathcal{A}_{\mathrm{I}}$不能进行私钥提取询问和证书提取询问.

(2) $\mathcal{A}_{\mathrm{I}}$不能对$\{id_s^*, id_r^*, w_0^*\}$和$\{id_s^*, id_r^*, w_1^*\}$进行陷门询问.

猜测阶段. 与游戏 IND-CKA-I 相同.

定义$\mathcal{A}_{\mathrm{I}}$赢得游戏 IND-KGA-I 的优势为

$$Adv_{\mathcal{A}_{\mathrm{I}}}^{\text{IND-KGA-I}}=\left|\Pr[\xi'=\xi]-\frac{1}{2}\right|.$$

游戏 IND-KGA-II：挑战者$\mathcal{C}$和攻击者$\mathcal{A}_{\mathrm{II}}$进行如下交互：

初始化阶段. 与游戏 IND-CKA-II 相同.

阶段 1. 与游戏 IND-CKA-II 相同.

挑战阶段. 与游戏 IND-KGA-I 相同.

阶段 2. $\mathcal{A}_{\mathrm{II}}$进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^*\in\{id_s^*, id_r^*\}$，$\mathcal{A}_{\mathrm{II}}$不能进行私钥提取询问.

(2) $\mathcal{A}_{\mathrm{II}}$不能对$\{id_s^*, id_r^*, w_0^*\}$和$\{id_s^*, id_r^*, w_1^*\}$进行陷门询问.

猜测阶段. 与游戏 IND-CKA-I 相同.

定义$\mathcal{A}_{\mathrm{II}}$赢得游戏 IND-KGA-II 的优势为

$$Adv_{\mathcal{A}_{\mathrm{II}}}^{\text{IND-KGA-II}}=\left|\Pr[\xi'=\xi]-\frac{1}{2}\right|.$$

定义 3.　如果任何多项式时间攻击者赢得游戏IND-KGA-I和IND-KGA-II 的优势$Adv_{\mathcal{A}_{\mathrm{I}}}^{\text{IND-KGA-I}}$，$Adv_{\mathcal{A}_{\mathrm{II}}}^{\text{IND-KGA-II}}$是可忽略的，那么本文所提方案是 IND-KGA 安全的.

4　方案构造

本节给出了多接收者证书基可搜索加密方案的具体构造. 表 1 列出了本文所提方案使用的符号及其含义.

表 1　符号定义

符号	含义
$params$	系统参数
id_s	发送者的身份
$(SK_s, P_s, PK_s, cert_S)$	发送者的私钥、部分公钥、公钥和证书
id_i	第 i 个接收者的身份
$(SK_i, P_i, PK_i, cert_i)$	第 i 个接收者的私钥、部分公钥、公钥和证书
w	发送者加密的关键词
C_w	关键词 w 的密文
w'	接收者搜索的关键词
$T_{w'}$	关键词 w'的搜索陷门

4.1　方　案

(1) 系统建立算法 Setup：给定安全参数 λ，证书权威随机选择大素数 p，以及 $a,b\in\mathbb{F}_p$，椭圆曲线 $E: y^2=x^3+ax+b(\mathrm{mod}p)$，生成素数 q 阶循环群$\mathbb{G}$. 证书权威随机选择 $s\in\mathbb{Z}_q^*$ 作为主私钥，$P\in\mathbb{G}$为生成元，计算 $P_{\text{pub}}=sP$. 证书权威选择三个安全哈希函数 $H_1:\{0,1\}^*\to\mathbb{Z}_q^*$, $H_2:\{0,1\}^*\to\mathbb{Z}_q^*$, $H_3:\{0,1\}^*\to\mathbb{Z}_q^*$. 证书权威输出系统参数 $params=\{E,a,b,p,q,\mathbb{G},P,P_{\text{pub}},H_1,H_2,H_3\}$.

(2) 用户密钥生成算法 UserKeyGen：用户随机选择 $d_u\in\mathbb{Z}_q^*$，计算 $P_u=d_uP$. 则用户私钥为 $SK_u=d_u$，部分公钥为 P_u.

(3) 证书生成算法 CertGen：给定用户身份 id_u 和部分公钥 P_u，证书权威随机选择 $r_u\in\mathbb{Z}_q^*$，计算 $R_u=r_uP$, $e_u=H_1(id_u\|x_{R_u}\|y_{R_u}\|x_{P_u}\|y_{P_u})$，若 $e_u=0$，则重新选择 r_u. 证书权威计算 $cert_u=r_u-e_u\cdot s$. 若 $cert_u=0$，则重新选择 r_u. 最后，证书权威输出用户证书 $cert_u$和用户公钥 $PK_u=\{P_u,R_u\}$.

(4) 关键词加密算法 KwEnc：给定发送者身份 id_s，私钥 SK_s，证书 $cert_s$，接收者身份$\{id_1,\cdots,id_n\}$，公钥$\{PK_1,\cdots,PK_n\}$和关键词 w，发送者随机选择 $t\in\mathbb{Z}_q^*$，计算 $C_1=t\cdot P$，对于每个 $j=1,\cdots,n$，计算

$$\begin{aligned}
&e_j=H_1(id_j\|x_{R_j}\|y_{R_j}\|x_{P_j}\|y_{P_j}),\\
&K_{sj}=(cert_s+d_s)\cdot P_j,\\
&V_{sj}=t\cdot H_2(x_{K_{sj}}\|y_{K_{sj}}\|id_s\|id_j\|w)\cdot P_j+\\
&\qquad t\cdot x_{K_{sj}}\cdot(R_j-e_j\cdot P_{\text{pub}}),\\
&C_{2,j}=H_3(x_{C_1}\|y_{C_1}\|x_{V_{sj}}\|y_{V_{sj}}),
\end{aligned}$$

则关键词 w 的密文为 $C_w=\{C_1,C_{2,1},\cdots,C_{2,n}\}$.

(5) 搜索陷门生成算法 TrapGen：给定接收者身份 id_i，私钥 SK_i，证书 $cert_i$，发送者身份 id_s，公钥 PK_s和关键词 w'，接收者计算

$$\begin{aligned}
&e_s=H_1(id_s\|x_{R_s}\|y_{R_s}\|x_{P_s}\|y_{P_s}),\\
&K'_{si}=d_i\cdot(R_s-e_s\cdot P_{\text{pub}}+P_s),\\
&T_{w'}=cert_i\cdot x_{K'_{si}}+d_i\cdot H_2(x_{K'_{si}}\|y_{K'_{si}}\|id_s\|id_i\|w'),
\end{aligned}$$

则关键词 w'的搜索陷门为 $T_{w'}$.

(6) 密文匹配算法 Test：给定密文 C_w 和搜索陷门 $T_{w'}$，云服务器计算 $V'_{si}=T_{w'}\cdot C_1$，对于每个 $j=1,\cdots,n$，检查 $H_3(x_{C_1}\|y_{C_1}\|x_{V'_{si}}\|y_{V'_{si}})=C_{2,j}$ 是否成立. 如果成立，云服务器输出 1，否则输出 0.

正确性：

$$\begin{aligned}K'_{si}&=d_i\cdot(R_s-e_s\cdot P_{\text{pub}}+d_s\cdot P)\\&=(r_s-e_s\cdot s+d_s)\cdot d_i\cdot P\\&=(cert_s+d_s)\cdot P_i\\V'_{si}&=T_{w'}\cdot C_1\\&=(cert_i\cdot x_{K'_{si}}+d_i\cdot H_2(x_{K'_{si}}\|y_{K'_{si}}\|id_s\|id_i\|w'))\cdot tP\\&=t\cdot H_2(x_{K'_{si}}\|y_{K'_{si}}\|id_s\|id_{ri}\|w')\cdot P_i+\\&\quad t\cdot x_{K'_{si}}\cdot(R_i-e_i\cdot P_{\text{pub}}).\end{aligned}$$

若 $w'=w$，$j=i$，那么 $K'_{si}=K_{sj}$，$V'_{si}=V_{sj}$，则等式 $H_3(x_{C_1}\|y_{C_1}\|x_{V'_{si}}\|y_{V'_{si}})=C_{2,j}$ 成立.

4.2 安全性

定理 1. 如果 CDH 假设成立，则本文所提方案是 IND-CKA 安全的.

证明. 该定理由引理 1 和引理 2 证明.

引理 1. 如果类型 I 攻击者 $\mathcal{A}_1$ 能够以不可忽略的优势 ϵ 攻破本文所提方案的 IND-CKA，则可以构造算法 $\mathcal{B}$ 以优势 $\epsilon'\geq(2\epsilon/nq_3)\cdot(1-1/q_u)^{q_c+q_t}\cdot(1/q_u)$ 解 CDH 问题，其中 q_3,q_u,q_c,q_t 分别表示 $\mathcal{A}_1$ 进行 H_3 询问、创建用户询问、证书提取询问和陷门询问的最大次数.

证明. 给定CDH问题的一个实例 (P,aP,bP)，算法 $\mathcal{B}$ 可以通过将 $\mathcal{A}_1$ 作为子程序调用来计算 abP.

初始化阶段. $\mathcal{B}$ 随机选择 $id_r(1\leq r\leq q_u)$ 作为挑战身份，令 $P_{\text{pub}}=aP$，运行系统建立算法返回 *params* 给 $\mathcal{A}_1$.

为了快速响应询问，$\mathcal{B}$ 维护以下初始化为空的列表：

L_{H_1}：由元组 (id_i,PK_i,e_i) 组成.

L_{H_2}：由元组 $(K_{ij},id_i,id_j,w_k,\pi_{ijk})$ 组成.

L_{H_3}：由元组 (C_1,V_{ijk},τ_{ijk}) 组成.

L_{user}：由元组 $(id_i,SK_i,r_i,e_i,cert_i,PK_i)$ 组成.

阶段 1. $\mathcal{A}_1$ 适应性地进行以下询问：

(1) H_1 询问：当 $\mathcal{A}_1$ 对 (id_i,PK_i) 进行哈希 H_1 询问时，如果 (id_i,PK_i,e_i) 已经存在于 L_{H_1} 中，$\mathcal{B}$ 返回相应的 e_i. 否则，$\mathcal{B}$ 随机选择 $e_i\in\mathbb{Z}_q^*$，将 (id_i,PK_i,e_i) 插入到 L_{H_1} 中并返回 e_i 给 $\mathcal{A}_1$.

(2) H_2 询问：当 $\mathcal{A}_1$ 对 (K_{ij},id_i,id_j,w_k) 进行哈希 H_2 询问时，如果 $(K_{ij},id_i,id_j,w_k,\pi_{ijk})$ 已经存在于 L_{H_2} 中，$\mathcal{B}$ 返回相应的 π_{ijk}. 否则，$\mathcal{B}$ 随机选择 $\pi_{ijk}\in\mathbb{Z}_q^*$，将 $(K_{ij},id_i,id_j,w_k,\pi_{ijk})$ 插入到 L_{H_2} 中并返回 π_{ijk} 给 $\mathcal{A}_1$.

(3) H_3 询问：当 $\mathcal{A}_1$ 对 (C_1,V_{ijk}) 进行哈希 H_3 询问时，如果 (C_1,V_{ijk},τ_{ijk}) 已经存在于 L_{H_3} 中，$\mathcal{B}$ 返回相应的 τ_{ijk}. 否则，$\mathcal{B}$ 随机选择 $\tau_{ijk}\in\mathbb{Z}_q^*$，将 (C_1,V_{ijk},τ_{ijk}) 插入到 L_{H_4} 中并返回 τ_{ijk} 给 $\mathcal{A}_1$.

(4) 创建用户询问：当 $\mathcal{A}_1$ 对 id_i 进行创建用户询问时，$\mathcal{B}$ 执行：

① 如果 $(id_i,SK_i,r_i,e_i,cert_i,PK_i)$ 已经存在于 L_{user} 中，$\mathcal{B}$ 返回 PK_i 给 $\mathcal{A}_1$.

② 如果 $id_i=id_r$，$\mathcal{B}$ 随机选择 $d_i,r_i,e_i\in\mathbb{Z}_q^*$，令 $SK_i=d_i$，$cert_i=\perp$，$PK_i=\{d_iP,r_iP\}$，分别插入 $(id_i,SK_i,r_i,e_i,cert_i,PK_i)$ 和 (id_i,PK_i,e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_1$.

③ 如果 $id_i\neq id_r$，$\mathcal{B}$ 随机选择 $d_i,e_i,\alpha_i\in\mathbb{Z}_q^*$，令 $SK_i=d_i$，$cert_i=\alpha_i$，$PK_i=\{d_iP,\alpha_iP+e_iP_{\text{pub}}\}$，分别插入 $(id_i,SK_i,\perp,e_i,cert_i,PK_i)$ 和 (id_i,PK_i,e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_1$.

(5) 私钥提取询问：当 $\mathcal{A}_1$ 对 id_i 进行私钥提取询问时，$\mathcal{B}$ 检查 $(id_i,SK_i,r_i,e_i,cert_i,PK_i)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i 进行创建用户询问. 最后，$\mathcal{B}$ 返回 SK_i 给 $\mathcal{A}_1$.

(6) 证书提取询问：当 $\mathcal{A}_1$ 对 id_i 进行证书提取询问时，$\mathcal{B}$ 检查 $(id_i,SK_i,r_i,e_i,cert_i,PK_i)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i 进行创建用户询问. $\mathcal{B}$ 执行：

① 如果 $id_i=id_r$，$\mathcal{B}$ 终止模拟.

② 如果 $id_i\neq id_r$，$\mathcal{B}$ 返回 $cert_i$ 给 $\mathcal{A}_1$.

(7) 陷门询问：当 $\mathcal{A}_1$ 对 (id_i,id_j,w_k) 进行陷门询问时，$\mathcal{B}$ 检查 $(id_i,SK_i,r_i,e_i,cert_i,PK_i)$ 和 $(id_j,SK_j,r_j,e_j,cert_j,PK_j)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i,id_j 进行创建用户询问. $\mathcal{B}$ 执行：

① 如果 $id_j=id_r$，$\mathcal{B}$ 终止模拟.

② 如果 $id_j\neq id_r$，$\mathcal{B}$ 计算 $K'_{ij}=d_j\cdot(R_i-e_i\cdot P_{\text{pub}}+P_i)$，检查 $(K'_{ij},id_i,id_j,w_k,\pi_{ijk})$ 是否存在于 L_{H_2} 中. 如果不存在，$\mathcal{B}$ 对 (K'_{ij},id_i,id_j,w_k) 进行哈希 H_2 询问得到 π_{ijk}. 最后，$\mathcal{B}$ 返回陷门 $T_{w_k}=cert_j\cdot x_{K'_{ij}}+d_j\cdot\pi_{ijk}$ 给 $\mathcal{A}_1$.

挑战阶段. 当阶段 1 结束后，$\mathcal{A}_1$ 选择两个关键词 w_0^*,w_1^*，以及发送者的身份 id_s^* 和接收者的身份 $\{id_1^*,\cdots,id_n^*\}$ 发送给 $\mathcal{B}$. 对于每个 $id^*\in\{id_s^*,id_1^*,\cdots,id_n^*\}$，$\mathcal{B}$ 检查 $(id^*,SK^*,r^*,e^*,cert^*,PK^*)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id^* 进行创建用户询问. $\mathcal{B}$ 执行：

(1) 如果 $id_r\notin\{id_1^*,\cdots,id_n^*\}$，$\mathcal{B}$ 终止模拟.

(2) 如果 $id_r \in \{id_1^*, \cdots, id_n^*\}$，$\mathcal{B}$ 随机选择 $\xi \in \{0,1\}$，令 $C_1^* = bP$，随机选择 $C_{21}^*, \cdots, C_{2n}^* \in \mathbb{Z}_q^*$. 最后，$\mathcal{B}$ 返回挑战密文 $C_{w_\xi^*}^* = \{C_1^*, C_{2,1}^*, \cdots, C_{2,n}^*\}$ 给 $\mathcal{A}_{\mathrm{I}}$.

阶段 2. $\mathcal{A}_{\mathrm{I}}$ 进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^* \in \{id_s^*, id_1^*, \cdots, id_n^*\}$，$\mathcal{A}_{\mathrm{I}}$ 不能进行私钥询问和证书询问.

(2) 对于 $id^* \in \{id_1^*, \cdots, id_n^*\}$，$\mathcal{A}_{\mathrm{I}}$ 不能对 $\{id_s^*, id^*, w_0^*\}$ 和 $\{id_s^*, id^*, w_1^*\}$ 进行陷门询问.

猜测阶段. 最后，$\mathcal{A}_{\mathrm{I}}$ 输出 $\xi' \in \{0,1\}$. $\mathcal{B}$ 忽略 $\mathcal{A}_{\mathrm{I}}$ 的输出，从 L_{H_3} 中选择 $(C_1^*, V_{sr\xi}^*, \tau_{sr\xi}^*)$，计算 $T = e_r^{-1} \cdot (r_r \cdot bP + x_{K_{si}}^{-1} \cdot (H_2(x_{K_{sr}} \| y_{K_{sr}} \| id_s^* \| id_r \| w_\xi) \cdot d_r \cdot bP - V_{sr\xi}^*))$ 作为 CDH 问题的解.

由于 $P_{\mathrm{pub}} = aP, C_1^* = bP$，则

$$\begin{aligned} V_{sr\xi}^* &= b \cdot H_2(x_{K_{sr}} \| y_{K_{sr}} \| id_s^* \| id_r \| w_\xi) \cdot P_r + \\ &\quad x_{K_{sr}} \cdot b \cdot (R_r - e_r \cdot aP) \\ &= H_2(x_{K_{sr}} \| y_{K_{sr}} \| id_s^* \| id_r \| w_\xi) \cdot d_r \cdot bP + \\ &\quad x_{K_{sr}} \cdot (r_r \cdot bP - e_r \cdot abP), \\ T &= e_r^{-1} \cdot (r_r \cdot bP + x_{K_{si}}^{-1} \cdot (H_2(x_{K_{sr}} \| y_{K_{sr}} \| id_s^* \| id_r \| w_\xi) \cdot \\ &\quad d_r \cdot bP - V_{sr\xi}^*)) \\ &= abP. \end{aligned}$$

定义事件 Θ 为 $\mathcal{A}_{\mathrm{I}}$ 对 $V_{si\xi}^* = x_{K_{si}} \cdot b \cdot H_2(x_{K_{si}} \| y_{K_{si}} \| id_s^* \| id_i^* \| w_\xi) \cdot (R_i^* - e_i^* \cdot aP + P_i^*)$ 已经进行哈希 H_3 询问，其中 $id_i^* \in \{id_1^*, \cdots, id_n^*\}$；事件 Θ' 为 $\mathcal{A}_{\mathrm{I}}$ 对 $V_{sr\xi}^* = x_{K_{sr}} \cdot b \cdot H_2(x_{K_{sr}} \| y_{K_{sr}} \| id_s^* \| id_r \| w_\xi) \cdot (R_r - e_r \cdot aP + P_r)$ 已经进行哈希 H_3 询问，易知 $n \cdot \Pr[\Theta'] \geq \Pr[\Theta]$.

定义 $\mathcal{B}$ 在上述游戏中终止模拟事件如下：

(1) $\mathcal{F}_1$：证书提取询问中终止.

(2) $\mathcal{F}_2$：陷门询问中终止.

(3) $\mathcal{F}_3$：挑战阶段中终止.

$\mathcal{B}$ 模拟过程中不终止的概率为 $\Pr[\overline{\mathcal{F}}] = \Pr[\overline{\mathcal{F}}_1 \wedge \overline{\mathcal{F}}_2 \wedge \overline{\mathcal{F}}_3] = (1-1/q_u)^{q_c+q_t}(1/q_u)$.

定义事件 $E = \Theta | \overline{\mathcal{F}}$. 如果 E 不发生，则 $\mathcal{A}_{\mathrm{I}}$ 猜测正确 ξ 的概率不超过 1/2，即 $\Pr[\xi' = \xi | \overline{E}] = 1/2$.

因此，

$$\begin{aligned} \Pr[\xi' = \xi] &= \Pr[\xi' = \xi | \overline{E}] \cdot \Pr[\overline{E}] + \\ &\quad \Pr[\xi' = \xi | E] \cdot \Pr[E] \\ &\leq \Pr[\overline{E}]/2 + \Pr[E] \\ &= 1/2 + \Pr[E]/2. \end{aligned}$$

从而可得 $\Pr[E] \geq 2|\Pr[\xi' = \xi] - 1/2|$. 由于 $\mathcal{A}_{\mathrm{I}}$ 赢得上述游戏的优势为 ϵ，则

$$2\epsilon \leq \Pr[E] = \frac{\Pr[\Theta, \overline{\mathcal{F}}]}{\Pr[\overline{\mathcal{F}}]} \leq \frac{\Pr[\Theta]}{\Pr[\overline{\mathcal{F}}]},$$

因此，$\Pr[\Theta] \geq 2\epsilon \Pr[\overline{\mathcal{F}}]$，则 $\Pr[\Theta'] \geq (2\epsilon/n)\Pr[\overline{\mathcal{F}}]$.

如果事件 Θ' 发生，$\mathcal{B}$ 就能够以 $1/q_3$ 的概率找到正确的 $(C_1^*, V_{sr\xi}^*, \tau_{sr\xi}^*)$. 因此，$\mathcal{B}$ 解 CDH 问题的优势为

$$\begin{aligned} \epsilon' &\geq (1/q_3)\Pr[\Theta'] \geq (2\epsilon/nq_3)\Pr[\overline{\mathcal{F}}] \\ &= (2\epsilon/nq_3) \cdot (1-1/q_u)^{q_c+q_t} \cdot (1/q_u). \end{aligned}$$

证毕.

引理 2. 如果类型 II 攻击者 $\mathcal{A}_{\mathrm{II}}$ 能够以不可忽略的优势 ϵ 攻破本文所提方案的 IND-CKA，则可以构造算法 $\mathcal{B}$ 以优势 $\epsilon' \geq (2\epsilon/nq_3) \cdot (1-1/q_u)^{q_s+q_t} \cdot (1/q_u)$ 解 CDH 问题，其中 q_3, q_u, q_s, q_t 分别表示 $\mathcal{A}_{\mathrm{II}}$ 进行 H_3 询问，创建用户询问，私钥提取询问和陷门询问的最大次数.

证明. 给定CDH问题的一个实例 (P, aP, bP)，算法 $\mathcal{B}$ 可以通过将 $\mathcal{A}_{\mathrm{II}}$ 作为子程序调用来计算 abP.

初始化阶段. $\mathcal{B}$ 随机选择 $id_r (1 \leq r \leq q_u)$ 作为挑战身份，随机选择 $s \in \mathbb{Z}_q^*$，计算 $P_{\mathrm{pub}} = sP$，运行系统建立算法返回 $\{params, s\}$ 给 $\mathcal{A}_{\mathrm{II}}$.

阶段 1. $\mathcal{A}_{\mathrm{II}}$ 适应性地进行以下询问：

(1) H_1 询问：与引理 1 相同.

(2) H_2 询问：与引理 1 相同.

(3) H_3 询问：与引理 1 相同.

(4) 创建用户询问：当 $\mathcal{A}_{\mathrm{II}}$ 对 id_i 进行创建用户询问时，$\mathcal{B}$ 执行：

① 如果 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 已经存在于 L_{user} 中，$\mathcal{B}$ 返回 PK_i 给 $\mathcal{A}_{\mathrm{II}}$.

② 如果 $id_i = id_r$，$\mathcal{B}$ 随机选择 $r_i, e_i \in \mathbb{Z}_q^*$，令 $SK_i = \perp$，$cert_i = r_i - e_i \cdot s$，$PK_i = \{aP, r_iP\}$，分别插入 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 和 (id_i, PK_i, e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_{\mathrm{II}}$.

③ 如果 $id_i \neq id_r$，$\mathcal{B}$ 随机选择 $d_i, r_i, e_i \in \mathbb{Z}_q^*$，令 $SK_i = d_i$，$cert_i = r_i - e_i \cdot s$，$PK_i = \{d_iP, r_iP\}$，分别插入 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 和 (id_i, PK_i, e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_{\mathrm{II}}$.

(5) 私钥提取询问：当 $\mathcal{A}_{\mathrm{II}}$ 对 id_i 进行私钥提取询问时，$\mathcal{B}$ 检查 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i 进行创建用户询问. $\mathcal{B}$ 执行：

① 如果 $id_i = id_r$，$\mathcal{B}$ 终止模拟.

② 如果 $id_i \neq id_r$，$\mathcal{B}$ 返回 SK_i 给 $\mathcal{A}_{\mathrm{II}}$.

(6) 陷门询问：与引理 1 相同.

挑战阶段. 当阶段 1 结束后，$\mathcal{A}_{\mathrm{II}}$ 选择两个关键词 w_0^*, w_1^*，以及发送者的身份 id_s^* 和接收者的身份 $\{id_1^*, \cdots, id_n^*\}$ 发送给 $\mathcal{B}$. 对于每个 $id^* \in \{id_s^*, id_1^*, \cdots, id_n^*\}$，$\mathcal{B}$ 检查 $(id^*, SK^*, r^*, e^*, cert^*, PK^*)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id^* 进行创建用户询

问.$\mathcal{B}$执行:

(1)如果 $id_r \notin \{id_1^*,\cdots,id_n^*\}$,$\mathcal{B}$终止模拟.

(2)如果 $id_r \in \{id_1^*,\cdots,id_n^*\}$,$\mathcal{B}$随机选择 $\xi \in \{0,1\}$,令 $C_1^*=bP$,随机选择 $C_{21}^*,\cdots,C_{2n}^* \in \mathbb{Z}_q^*$.最后,$\mathcal{B}$返回挑战密文 $C_{w_\xi^*}^*=\{C_1^*,C_{2,1}^*,\cdots,C_{2,n}^*\}$给 $\mathcal{A}_{\mathrm{II}}$.

阶段 2. $\mathcal{A}_{\mathrm{II}}$继续进行阶段 1 中的询问,但是存在以下限制:

(1)对于 $id^* \in \{id_s^*,id_1^*,\cdots,id_n^*\}$,$\mathcal{A}_{\mathrm{II}}$不能进行私钥提取询问.

(2)对于 $id^* \in \{id_1^*,\cdots,id_n^*\}$,$\mathcal{A}_{\mathrm{II}}$不能对$\{id_s^*,id^*,w_0^*\}$和$\{id_s^*,id^*,w_1^*\}$进行陷门询问.

猜测阶段.最后,$\mathcal{A}_{\mathrm{II}}$输出 $\xi' \in \{0,1\}$.$\mathcal{B}$忽略$\mathcal{A}_{\mathrm{II}}$的输出,从$L_{H_3}$中选择$(C_1^*,V_{sr\xi}^*,\tau_{sr\xi}^*)$,计算$T=H_2(x_{K_{sr}}\|y_{K_{sr}}\|id_s^*\|id_r\|w_\xi)^{-1}\cdot(V_{sr\xi}^*-x_{K_{sr}}\cdot(r_r-e_r\cdot s)\cdot bP)$作为 CDH 问题的解.

由于 $P_r=aP$,$C_1^*=bP$,则

$$\begin{aligned}V_{sr\xi}^* &= b\cdot H_2(x_{K_{sr}}\|y_{K_{sr}}\|id_s^*\|id_r\|w_\xi)\cdot aP+\\ &\quad x_{K_{sr}}\cdot b\cdot(R_r-e_rP_{\mathrm{pub}})\\ &= H_2(x_{K_{sr}}\|y_{K_{sr}}\|id_s^*\|id_r\|w_\xi)\cdot abP+\\ &\quad x_{K_{sr}}\cdot(r_r-e_r\cdot s)\cdot bP,\\ T &= H_2(x_{K_{sr}}\|y_{K_{sr}}\|id_s^*\|id_r\|w_\xi)^{-1}\cdot\\ &\quad (V_{sr\xi}^*-x_{K_{sr}}\cdot(r_r-e_r\cdot s)\cdot bP)\\ &= abP.\end{aligned}$$

类似于引理 1 的分析方法,$\mathcal{B}$解 CDH 问题的优势为 $\epsilon'=(2\epsilon/nq_3)\cdot(1-1/q_u)^{q_s+q_t}\cdot(1/q_u)$.

证毕.

定理 2. 如果 CDH 假设成立,则本文所提方案是 IND-KGA 安全的.

证明. 该定理由引理 3 和引理 4 证明.

引理 3. 如果类型 I 攻击者$\mathcal{A}_1$能够以不可忽略的优势 ϵ 攻破本文所提方案的 IND-KGA,则可以构造算法$\mathcal{B}$以优势 $\epsilon' \geq (2\epsilon/q_2)\cdot(1/q_u(q_u-1))\cdot(1-1/q_u)^{q_s+q_c}\cdot(1-2/q_u)^{q_t}$解CDH 问题,其中 q_2,q_u,q_s,q_c,q_t分别表示$\mathcal{A}_1$进行 H_2 询问,创建用户询问,私钥提取询问,证书提取询问和陷门询问的最大次数.

证明. 给定 CDH 问题的一个实例(P,aP,bP),算法$\mathcal{B}$可以通过将$\mathcal{A}_1$作为子程序调用来计算 abP.

初始化阶段.$\mathcal{B}$随机选择$\{id_s,id_r\}(1\leq s\leq r\leq q_u)$作为挑战身份,令 $P_{\mathrm{pub}}=aP$,运行系统建立算法返回 $params$ 给$\mathcal{A}_1$.

阶段 1. $\mathcal{A}_1$适应性地进行以下询问:

(1)H_1询问:与引理 1 相同.

(2)H_2询问:与引理 1 相同.

(3)H_3询问:与引理 1 相同.

(4)创建用户询问:当$\mathcal{A}_1$对 id_i进行创建用户询问时,$\mathcal{B}$执行:

① 如果$(id_i,SK_i,r_i,e_i,cert_i,PK_i)$已经存在于 L_{user}中,$\mathcal{B}$返回相应的 PK_i.

② 如果 $id_i=id_s$,$\mathcal{B}$随机选择 $d_i,r_i,e_i \in \mathbb{Z}_q^*$,令 $SK_i=d_i$,$cert_i=\perp$,$PK_i=\{d_iP,r_iP\}$,分别插入$(id_i,SK_i,r_i,e_i,cert_i,PK_i)$和$(id_i,PK_i,e_i)$到 L_{user}和 L_{H_1}中,并返回 PK_i给$\mathcal{A}_1$.

③ 如果$id_i=id_r$,$\mathcal{B}$随机选择 $e_i,\alpha_i \in \mathbb{Z}_q^*$,令 $SK_i=\perp$,$cert_i=\alpha_i$,$PK_i=\{bP,\alpha_iP+e_iP_{\mathrm{pub}}\}$,分别插入$(id_i,SK_i,\perp,e_i,cert_i,PK_i)$和$(id_i,PK_i,e_i)$到 L_{user}和 L_{H_1}中,并返回 PK_i给$\mathcal{A}_1$.

④ 如果 $id_i\neq id_s \wedge id_i\neq id_r$,$\mathcal{B}$随机选择 $d_i,e_i,\alpha_i \in \mathbb{Z}_q^*$,令 $SK_i=d_i$,$cert_i=\alpha_i$,$PK_i=\{d_iP,\alpha_iP+e_iP_{\mathrm{pub}}\}$,分别插入$(id_i,SK_i,\perp,e_i,cert_i,PK_i)$和$(id_i,PK_i,e_i)$到 L_{user}和 L_{H_1}中,并返回 PK_i给$\mathcal{A}_1$.

(5)私钥提取询问:当$\mathcal{A}_1$对 id_i进行私钥提取询问时,$\mathcal{B}$检查$(id_i,SK_i,r_i,e_i,cert_i,PK_i)$是否存在于 L_{user}中.如果不存在,$\mathcal{B}$对 id_i进行创建用户询问.$\mathcal{B}$执行:

① 如果 $id_i=id_r$,$\mathcal{B}$终止模拟.

② 如果 $id_i\neq id_r$,$\mathcal{B}$返回 SK_i给$\mathcal{A}_1$.

(6)证书提取询问:当$\mathcal{A}_1$对 id_i进行证书提取询问时,$\mathcal{B}$检查$(id_i,SK_i,r_i,e_i,cert_i,PK_i)$是否存在于 L_{user}中.如果不存在,$\mathcal{B}$对 id_i进行创建用户询问.$\mathcal{B}$执行:

① 如果 $id_i=id_s$,$\mathcal{B}$终止模拟

② 如果 $id_i\neq id_s$,$\mathcal{B}$返回 $cert_i$给$\mathcal{A}_1$.

(7)陷门询问:当$\mathcal{A}_1$对(id_i,id_j,w_k)进行陷门询问时,$\mathcal{B}$检查$(id_i,SK_i,r_i,e_i,cert_i,PK_i)$和$(id_j,SK_j,r_j,e_j,cert_j,PK_j)$是否存在于 L_{user}中.如果不存在,$\mathcal{B}$对 id_i,id_j进行创建用户询问.$\mathcal{B}$执行:

① 如果 $id_j \in \{id_s,id_r\}$,$\mathcal{B}$终止模拟.

② 如果 $id_j \notin \{id_s,id_r\}$,$\mathcal{B}$计算 $K'_{ij}=d_j\cdot(R_i-e_i\cdot P_{\mathrm{pub}}+P_i)$.$\mathcal{B}$检查$(K'_{ij},id_i,id_j,w_k,\pi_{ijk})$是否存在于 L_{H_2}中.如果不存在,$\mathcal{B}$对(K'_{ij},id_i,id_j,w_k)进行哈希 H_2 询问得到 π_{ijk}.最后,$\mathcal{B}$返回陷门 $T_{w_k}=cert_j\cdot x_{K'_{ij}}+\pi_{ijk}\cdot d_j$给$\mathcal{A}_1$.

挑战阶段.当阶段 1 结束后,$\mathcal{A}_1$选择两个关键词 w_0^*,w_1^*,以及发送者的身份 id_i^* 和接收者的身份 id_j^* 发送给$\mathcal{B}$.$\mathcal{B}$检查$(id_i^*,SK_i^*,r_i^*,e_i^*,cert_i^*,PK_i^*)$和$(id_j^*,SK_j^*,r_j^*,e_j^*,cert_j^*,PK_j^*)$是否存在于 L_{user}中.如果不存在,$\mathcal{B}$对 id_i^*,id_j^* 进行创建用户询问.$\mathcal{B}$执行:

(1)如果 $id_i^*\neq id_s \vee id_j^*\neq id_r$,$\mathcal{B}$终止模拟.

(2) 如果 $id_i^* = id_s \wedge id_j^* = id_r$，$\mathcal{B}$ 随机选择 $\xi \in \{0,1\}$，$T_{w_\xi^*}^* \in \mathbb{Z}_q^*$. 最后，$\mathcal{B}$ 返回挑战陷门 $T_{w_b^*}^*$ 给 $\mathcal{A}_{\mathrm{I}}$.

阶段 2. $\mathcal{A}_{\mathrm{I}}$ 继续进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^* \in \{id_s^*, id_r^*\}$，$\mathcal{A}_{\mathrm{I}}$ 不能进行私钥提取询问和证书提取询问.

(2) $\mathcal{A}_{\mathrm{I}}$ 不能对 $\{id_i^*, id_j^*, w_0^*\}$ 和 $\{id_i^*, id_j^*, w_1^*\}$ 进行陷门询问.

猜测阶段. 最后，$\mathcal{A}_{\mathrm{I}}$ 输出 $\xi' \in \{0,1\}$. $\mathcal{B}$ 忽略 $\mathcal{A}_{\mathrm{I}}$ 的输出，从 L_{H_2} 中选择 $(K_{sr}, id_s, id_r, w_\xi^*, \pi_{sr\xi}^*)$，计算 $T = e_s^{-1}((r_s + d_s) \cdot bP - K_{sr})$ 作为 CDH 问题的解.

由于 $P_{\mathrm{pub}} = aP$，$P_r = d_r P = bP$，则

$$K_{sr} = d_r(R_s - e_s P_{\mathrm{pub}} + P_s) = b(r_s P - e_s \cdot aP + d_s P)$$
$$= (r_s + d_s) \cdot bP - e_s \cdot abP,$$
$$T = e_s^{-1}((r_s + d_s) \cdot bP - K_{sr})$$
$$= abP.$$

类似于引理 1 的分析方法，$\mathcal{B}$ 解 CDH 问题的优势为 $\epsilon' \geq (2\epsilon/q_2) \cdot (1/q_u(q_u - 1)) \cdot (1 - 1/q_u)^{q_s + q_c} \cdot (1 - 2/q_u)^{q_t}$.

证毕.

引理 4. 如果类型 II 攻击者 $\mathcal{A}_{\mathrm{II}}$ 能够以不可忽略的优势 ϵ 攻破本文所提方案的 IND-KGA，则可以构造算法 $\mathcal{B}$ 以优势 $\epsilon' \geq (2\epsilon/q_2) \cdot (1 - 2/q_u)^{q_s + q_t} \cdot (1/q_u(q_u - 1))$ 解 CDH 问题，其中 q_2, q_u, q_s, q_t 分别表示 $\mathcal{A}_{\mathrm{II}}$ 进行 H_2 询问，创建用户询问，私钥提取询问和陷门询问的最大次数.

证明. 给定 CDH 问题的一个实例 (P, aP, bP)，算法 $\mathcal{B}$ 可以通过将 $\mathcal{A}_{\mathrm{II}}$ 作为子程序调用来计算 abP.

初始化阶段. $\mathcal{B}$ 随机选择 $\{id_s, id_r\}$ $(1 \leq s \leq r \leq q_u)$ 作为挑战身份，随机选择 $s \in \mathbb{Z}_q^*$，计算 $P_{\mathrm{pub}} = sP$，运行系统建立算法返回 $\{params, s\}$ 给 $\mathcal{A}_{\mathrm{II}}$.

阶段 1. $\mathcal{A}_{\mathrm{II}}$ 适应性地进行以下询问：

(1) H_1 询问：与引理 1 相同.

(2) H_2 询问：与引理 1 相同.

(3) H_3 询问：与引理 1 相同.

(4) 创建用户询问：当 $\mathcal{A}_{\mathrm{II}}$ 对 id_i 进行创建用户询问时，$\mathcal{B}$ 执行：

① 如果 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 已经存在于 L_{user} 中，$\mathcal{B}$ 返回相应的 PK_i.

② 如果 $id_i = id_s$，$\mathcal{B}$ 随机选择 $r_i, e_i \in \mathbb{Z}_q^*$，令 $SK_i = \perp$，$cert_i = r_i - e_i \cdot s$，$PK_i = \{aP, r_i P\}$，分别插入 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 和 (id_i, PK_i, e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_{\mathrm{II}}$.

③ 如果 $id_i = id_r$，$\mathcal{B}$ 随机选择 $r_i, e_i \in \mathbb{Z}_q^*$，令 $SK_i = \perp$，$cert_i = r_i - e_i \cdot s$，$PK_i = \{bP, r_i P\}$，分别插入 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 和 (id_i, PK_i, e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_{\mathrm{II}}$.

④ 如果 $id_i \neq id_s \wedge id_i \neq id_r$，$\mathcal{B}$ 随机选择 $d_i, r_i, e_i \in \mathbb{Z}_q^*$，令 $SK_i = d_i$，$cert_i = r_i - e_i \cdot s$，$PK_i = \{d_i P, r_i P\}$，分别插入 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 和 (id_i, PK_i, e_i) 到 L_{user} 和 L_{H_1} 中，并返回 PK_i 给 $\mathcal{A}_{\mathrm{II}}$.

(5) 私钥提取询问：当 $\mathcal{A}_{\mathrm{II}}$ 对 id_i 进行私钥提取询问时，$\mathcal{B}$ 检查 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i 进行创建用户询问. $\mathcal{B}$ 执行：

① 如果 $id_i \in \{id_s, id_r\}$，$\mathcal{B}$ 终止模拟.

② 如果 $id_i \notin \{id_s, id_r\}$，$\mathcal{B}$ 返回 SK_i 给 $\mathcal{A}_{\mathrm{II}}$.

(6) 陷门询问：当 $\mathcal{A}_{\mathrm{II}}$ 对 (id_i, id_j, w_k) 进行陷门询问时，$\mathcal{B}$ 检查 $(id_i, SK_i, r_i, e_i, cert_i, PK_i)$ 和 $(id_j, SK_j, r_j, e_j, cert_j, PK_j)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i, id_j 进行创建用户询问. $\mathcal{B}$ 执行：

① 如果 $id_j \in \{id_s, id_r\}$，$\mathcal{B}$ 终止模拟.

② 如果 $id_j \notin \{id_s, id_r\}$，$\mathcal{B}$ 计算 $K'_{ij} = d_j \cdot (R_i - e_i \cdot P_{\mathrm{pub}} + P_i)$. $\mathcal{B}$ 检查 $(K'_{ij}, id_i, id_j, w_k, \pi_{ijk})$ 是否存在于 L_{H_2} 中. 如果不存在，$\mathcal{B}$ 对 $(K'_{ij}, id_i, id_j, w_k)$ 进行哈希 H_2 询问得到 π_{ijk}. 最后，$\mathcal{B}$ 返回陷门 $T_{w_k} = cert_j \cdot x_{K'_{ij}} + \pi_{ijk} \cdot d_j$ 给 $\mathcal{A}_{\mathrm{II}}$.

挑战阶段. 当阶段 1 结束后，$\mathcal{A}_{\mathrm{II}}$ 选择两个关键词 w_0^*, w_1^*，以及发送者的身份 id_i^* 和接收者的身份 id_j^* 发送给 $\mathcal{B}$. $\mathcal{B}$ 检查 $(id_i^*, SK_i^*, r_i^*, e_i^*, cert_i^*, PK_i^*)$ 和 $(id_j^*, SK_j^*, r_j^*, e_j^*, cert_j^*, PK_j^*)$ 是否存在于 L_{user} 中. 如果不存在，$\mathcal{B}$ 对 id_i^*, id_j^* 进行创建用户询问. $\mathcal{B}$ 执行：

(1) 如果 $id_i^* \neq id_s \vee id_j^* \neq id_r$，$\mathcal{B}$ 终止模拟.

(2) 如果 $id_i^* = id_s \wedge id_j^* = id_r$，$\mathcal{B}$ 随机选择 $\xi \in \{0,1\}$，$T_{w_\xi^*}^* \in \mathbb{Z}_q^*$，最后，$\mathcal{B}$ 返回挑战陷门 $T_{w_b^*}^*$ 给 $\mathcal{A}_{\mathrm{II}}$.

阶段 2. $\mathcal{A}_{\mathrm{II}}$ 继续进行阶段 1 中的询问，但是存在以下限制：

(1) 对于 $id^* \in \{id_s^*, id_r^*\}$，$\mathcal{A}_{\mathrm{II}}$ 不能进行私钥提取询问.

(2) $\mathcal{A}_{\mathrm{II}}$ 不能对 $\{id_i^*, id_j^*, w_0^*\}$ 和 $\{id_i^*, id_j^*, w_1^*\}$ 进行陷门询问.

猜测阶段. 最后，$\mathcal{A}_{\mathrm{II}}$ 输出 $\xi' \in \{0,1\}$. $\mathcal{B}$ 忽略 $\mathcal{A}_{\mathrm{II}}$ 的输出，从 L_{H_2} 中选择 $(K_{sr}, id_s, id_r, w_\xi^*, \pi_{sr\xi}^*)$，计算 $T = K_{sr} - (r_s - e_s \cdot s) \cdot bP$ 作为 CDH 问题的解.

由于 $P_s = d_s P = aP$，$P_r = d_r P = bP$，则

$$\begin{aligned}K_{sr}&=d_r(R_s-e_sP_{\text{pub}}+P_s)\\&=b(r_sP-e_ssP+aP)\\&=(r_s-e_s\cdot s)\cdot bP+abP,\\T&=K_{sr}-(r_s-e_s\cdot s)\cdot bP\\&=abP.\end{aligned}$$

类似于引理 1 的分析方法，$\mathcal{B}$解 CDH 问题的优势为 $\epsilon'\geq(2\epsilon/q_2)\cdot(1-2/q_u)^{q_s+q_t}\cdot(1/q_u(q_u-1))$.

证毕.

5 性能分析

本节分别从理论和实验方面对相关方案[9-10]和本文所提方案进行分析.

5.1 理论分析

双线性映射定义为 $e:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_T$，其中 $\mathbb{G}_1$，$\mathbb{G}_T$ 分别为素数 q 阶加法循环群和乘法循环群. $\mathbb{G}$ 定义为非奇异椭圆曲线 E 上所有的有理点构成的素数 q 阶加法循环群. 方案[9-10]和本文所提方案的比较结果见表 2，其中 T_{BP}，T_{SM_1}，T_{SM_T}，T_{MTP}，T_{SM} 和 T_h 分别表示双线性映射操作，$\mathbb{G}_1$ 中的标量乘操作，$\mathbb{G}_T$ 中的指数操作，Map-to-Point 哈希函数操作，$\mathbb{G}$ 中的标量乘操作和通用安全哈希函数操作所需要的时间. $|\mathbb{G}_1|$，$|\mathbb{G}_T|$，$|\mathbb{G}|$ 和 $|\mathbb{Z}_q^*|$ 分别表示 $\mathbb{G}_1$，$\mathbb{G}_T$，$\mathbb{G}$ 和 $\mathbb{Z}_q^*$ 中元素的长度.

表 2 理论分析比较

方案	计算代价			通信代价		特点					
	关键词加密算法	搜索陷门生成算法	密文匹配算法	密文长度	搜索陷门长度	F1	F2	F3	F4	F5	F6
方案[9]	$n(2T_{BP}+T_{SM_1}+T_{SM_T}+T_{MTP}+4T_h)$	$T_{BP}+3T_{SM_1}+2T_{MTP}+2T_h$	T_{BP}	$n(\lvert\mathbb{G}_1\rvert+l)$	$\lvert\mathbb{G}_1\rvert$	✓	✓	✓	×	✓	×
方案[10]	$5nT_{SM}+4nT_h$	$2T_{SM}+2T_h$	$2T_{SM}+2T_h$	$n(\lvert\mathbb{G}\rvert+2\lvert\mathbb{Z}_q^*\rvert+l)$	$\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_q^*\rvert$	✓	✓	✓	✓	×	×
本文所提方案	$(4n+1)T_{SM}+3nT_h$	$2T_{SM}+2T_h$	$T_{SM}+T_h$	$\lvert\mathbb{G}\rvert+n\lvert\mathbb{Z}_q^*\rvert$	$\lvert\mathbb{Z}_q^*\rvert$	✓	✓	✓	✓	✓	✓

注：F1：IND-CKA，F2：IND-KGA，F3：无安全信道，F4：无双线性映射，F5：发送者匿名，F6：多接收者.

n 表示接收者的数量，l 表示通用安全哈希函数输出长度，✓表示满足，×表示不满足.

根据表 2 可知，相比于方案[9-10]，本文所提方案的关键词加密算法和密文匹配算法的计算代价均为最小. 方案[10]和本文所提方案的搜索陷门生成算法的运算量相同. 相比于方案[9-10]，本文所提方案取得了通信代价的优势. 此外，虽然方案[9-10]和本文所提方案的安全性均满足 IND-CKA 和 IND-KGA 且无需安全信道，但本文所提方案中相同数据仅需加密一次即可实现多接收者检索，同时实现了发送者匿名性.

非对称可搜索加密中搜索模式主要包括精确关键词搜索[6]、连接关键词搜索[32]和模糊搜索[17]. 本文所提方案的设计能够实现精确关键词搜索，下面分析本文所提方案在连接关键词搜索模式和模糊搜索模式下性能指标.

连接关键词搜索模式. 本文所提方案能够通过两种方式实现连接关键词搜索模式. 基于文献[38]，接收者分别对每个关键词生成陷门，然后服务器返回每个关键词搜索结果的交集. 采用该方法实现连接关键词搜索，方案的生成关键词密文和搜索陷门阶段所需的计算代价和通信代价会随着关键词的数量线性增加. 基于文献[7]的构造思路，关键词密文和搜索陷门均对应一个关键词集合，只有当两个关键词集合相等时，该密文和陷门才能够匹配成功. 使用该方法，方案不会产生额外的计算代价和通信代价.

模糊搜索模式. 基于文献[17]思想，本文所提方案中发送者通过使用一个模糊函数提取模糊关键词，然后对该模糊关键词进行加密. 接收者生成模糊关键词对应的搜索陷门进行搜索. 本文所提方案以额外增加一个模糊函数的代价实现了模糊搜索模式，不会产生额外的通信代价，仅在生成关键词密文和搜索陷门阶段产生可忽略的计算代价.

5.2 仿真实验

使用 Python 语言基于 Charm-Crypto 库[39]在 PC 端实现了方案[9-10]和本文所提方案，实验环境为 Intel(R) Core(TM) i7-7700HQ@2.80GHz 的 8 核处理器、4GB 内存和 50GB 磁盘存储的 Linux 操作系统. 在 80 比特的安全性下，方案[9]使用非奇异曲线 $E/F_p:y^2=x^3+x$ 上嵌入度为 2 的 Type A 映射，方案[10]和本文所提方案采用 SECG 推荐的曲线参数 secp160k1[40]. 通用安全哈希函数使用 SHA-256 算法. $\mathbb{G}_1$，$\mathbb{G}_T$，$\mathbb{G}$ 和 $\mathbb{Z}_q^*$ 中元素的长度分别为 1024，1024，320 和 160 比特. 图 2 给出方案[9-10]和本文所提方案中关键词加密算法、搜索陷门生成算法和密文匹配算法的计算代价以及通信代价比较.

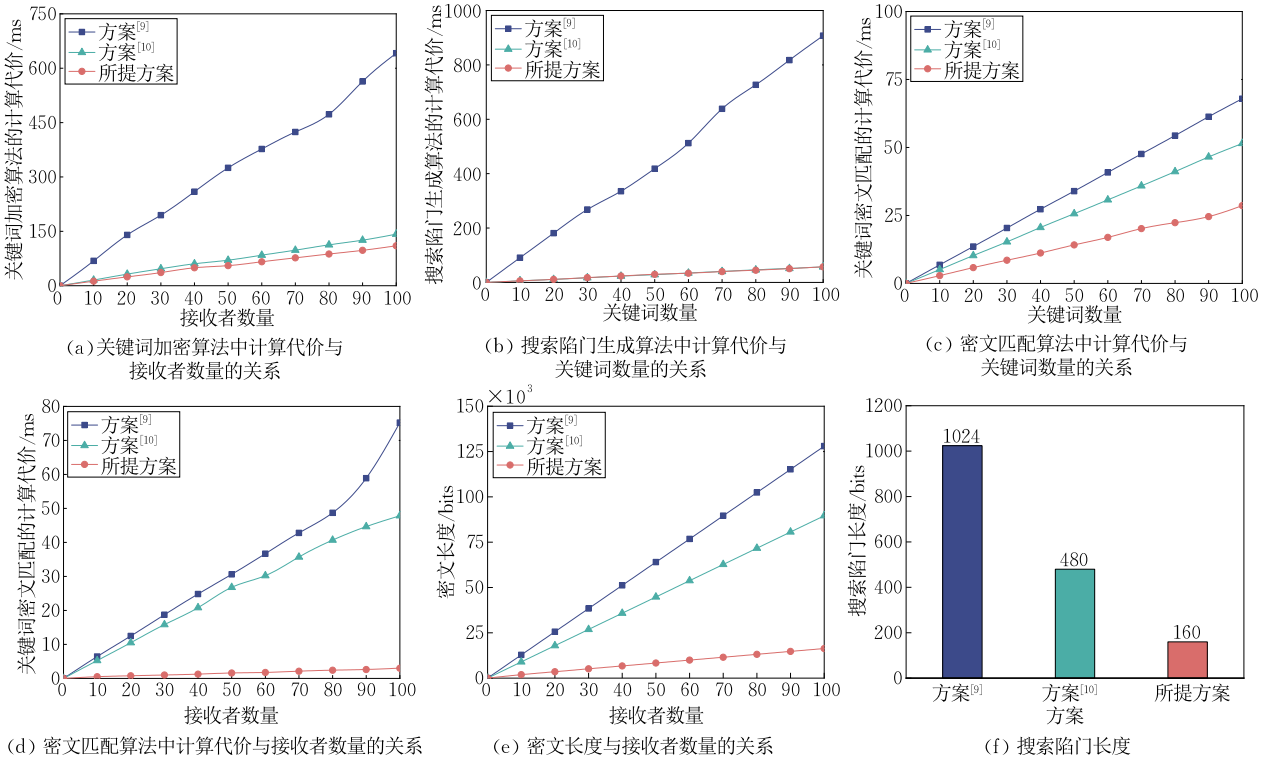

图 2　仿真实验分析比较

图 2(a)给出了关键词加密算法中计算代价与接收者数量之间的关系. 当接收者数量为 100 时，本文所提方案生成关键词密文需要 110.06 ms，相比于方案[9]降低了 82.84%，比方案[10]降低了 22.63%. 本文所提方案的关键词加密算法的计算代价最小. 图 2(b)给出了搜索陷门生成算法中计算代价与关键词数量之间的关系. 当关键词数量为 100 时，本文所提方案生成搜索陷门需要 57.20 ms，相比于方案[9]降低了 93.70%，方案[10]和本文所提方案计算代价相当. 图 2(c)给出了密文匹配算法中计算代价与关键词数量之间的关系. 当关键词数量为 100 时，本文所提方案密文匹配需要 28.60 ms，相比于方案[9]降低了 57.89%，比方案[10]降低了 44.45%. 图 2(d)给出了密文匹配算法中计算代价与接收者数量之间的关系. 当接收者数量为 100 时，本文所提方案密文匹配需要 2.99 ms，相比于方案[9]降低了 96.03%，比方案[10]降低了 93.75%. 本文所提方案显著地降低了云服务器的计算代价，在云计算环境下更具有实用性.

图 2(e)给出了密文长度与接收者数量之间的关系. 当接收者数量为 100 时，本文所提方案的关键词密文长度为 16320 比特，相比方案[9]降低了 87.25%，比方案[10]降低了 81.79%. 图 2(f)给出了方案搜索陷门长度的比较. 本文所提方案的搜索陷门长度为 160 比特，相比于方案[9]降低了 84.38%，比方案[10]降低了 66.67%. 因此，本文所提方案的密文长度和搜索陷门长度均为最小，取得了低的通信代价.

6　总　结

证书基可搜索加密在实现云存储中密文检索的同时，解决了证书管理、密钥托管以及安全信道问题. 然而，已有技术仅支持单个接收者的关键词搜索，导致在多个接收者的场景中搜索效率低下. 此外，已知方案要么使用耗时的双线性映射操作，要么无法满足发送者匿名特性. 基于此，本文提出了多接收者证书基可搜索加密方案. 本文所提方案在实现多个接收者高效搜索的同时，保护了发送者的隐私信息. 在随机预言机模型中，基于计算性 Diffie-Hellman 假设，证明本文所提方案满足适应性选择关键词攻击的不可区分性和适应性关键词猜测攻击的不可区分性. 理论和实验分析表明，与已知方案相比，本文所提方案取得低的计算代价和通信代价，更加符合云存储环境的实际情况，具有更强的实用性和应用前景.

参　考　文　献

[1] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing. Communications of the ACM, 2010, 53(4):

50-58

[2] Kamara S, Lauter K. Cryptographic cloud storage//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Germany, 2010: 136-149

[3] Feng Deng-Guo, Zhang Min, Zhang Yan, et al. Study on cloud computing security. Journal of Software, 2011, 22(1): 71-83(in Chinese)
(冯登国, 张敏, 张妍等. 云计算安全研究. 软件学报, 2011, 22(1): 71-83)

[4] Feng Chao-Sheng, Qin Zhi-Guang, Yuan Ding. Techniques of secure storage for cloud data. Chinese Journal of Computers, 2015, 38(1): 150-163(in Chinese)
(冯朝胜, 秦志光, 袁丁. 云数据安全存储技术. 计算机学报, 2015, 38(1): 150-163)

[5] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA, 2000: 44-55

[6] Boneh D, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search//Proceedings of the Advances in Cryptology—EUROCRYPT'04. Berlin, Germany, 2004: 506-522

[7] Park D J, Kim K, Lee P J. Public key encryption with conjunctive field keyword search//Proceedings of the Information Security Applications. Berlin, Germany, 2005: 73-86

[8] Gentry C. Certificate-based encryption and the certificate revocation problem//Proceedings of the Advances in Cryptology—EUROCRYPT'03. Berlin, Germany, 2003: 272-293

[9] Lu Y, Li J, Zhang Y. Secure channel free certificate-based searchable encryption withstanding outside and inside keyword guessing attacks. IEEE Transactions on Services Computing, 2019, 14(6): 2041-2054

[10] Lu Y, Li J, Wang F. Pairing-free certificate-based searchable encryption supporting privacy-preserving keyword search function for IIoTs. IEEE Transactions on Industrial Informatics, 2020, 17(4): 2696-2706

[11] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[12] Schnorr C P. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4(3): 161-174

[13] Boneh D, Franklin M. Identity-based encryption from the Weil pairing//Proceedings of the Advances in Cryptology—CRYPTO'01. Berlin, Germany, 2001: 213-229

[14] Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited//Proceedings of the International Conference on Computational Science and Its Applications. Berlin, Germany, 2008: 1249-1259

[15] Rhee H S, Park J H, Susilo W, et al. Improved searchable public key encryption with designated tester//Proceedings of the International Symposium on Information. Sydney, Australia, 2009: 376-379

[16] Byun J W, Rhee H S, Park H A, et al. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data//Proceedings of the International Workshop on Secure Data Management. Berlin, Germany, 2006: 75-83

[17] Xu P, Jin H, Wu Q, et al. Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack. IEEE Transactions on Computers, 2012, 62(11): 2266-2277

[18] Huang Q, Li H. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. Information Sciences, 2017, 403: 1-14

[19] Noroozi M, Eslami Z. Public key authenticated encryption with keyword search: Revisited. IET Information Security, 2019, 13(4): 336-342

[20] Chen R, Mu Y, Yang G, et al. Server-aided public key encryption with keyword search. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2833-2842

[21] Zhao Y, Ning J, Liang K, et al. Privacy preserving search services against online attack. Computers & Security, 2020, 95: 101836

[22] Peikert C, Waters B. Lossy trapdoor functions and their applications//Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York, USA, 2008: 187-196

[23] Abdalla M, Bellare M, Catalano D, et al. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions//Proceedings of the Advances in Cryptology—CRYPTO'05. Berlin, Germany, 2005: 205-222

[24] Peng Y, Cui J, Peng C, et al. Certificateless public key encryption with keyword search. China Communications, 2014, 11(11): 100-113

[25] Ma M, He D, Kumar N, et al. Certificateless searchable public key encryption scheme for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2017, 14(2): 759-767

[26] He D, Ma M, Zeadally S, et al. Certificateless public key authenticated encryption with keyword search for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2017, 14(8): 3618-3627

[27] Uwizeye E, Wang J, Cheng Z, et al. Certificateless public key encryption with conjunctive keyword search and its application to cloud-based reliable smart grid system. Annals of Telecommunications, 2019, 74(7): 435-449

[28] Pakniat N. Designated tester certificateless encryption with keyword search. Journal of Information Security and Applications, 2019, 49: 102394

[29] Ma M, He D, Fan S, et al. Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare. Journal of Information Security and Applications, 2020, 50: 102429

[30] Yang Xiao-Dong, Tian Tian, Wang Jia-Qi, et al. Certificateless ciphertext retrieval scheme with multi-user and multi-keyword based on cloud-edge collaboration. Journal on Communications, 2022, 43(5): 144-154(in Chinese)
(杨小东, 田甜, 王嘉琪等. 基于云边协同的无证书多用户多关键字密文检索方案. 通信学报, 2022, 43(5): 144-154)

[31] Senouci M R, Benkhaddra I, Senouci A, et al. An efficient

and secure certificateless searchable encryption scheme against keyword guessing attacks. Journal of Systems Architecture, 2021, 119: 102271

[32] Hwang Y H, Lee P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system// Proceedings of the Pairing-Based Cryptography. Tokyo, Japan, 2007: 2-22

[33] Lu Y, Li J, Zhang Y. Privacy-preserving and pairing-free multi-recipient certificateless encryption with keyword search for cloud-assisted IIoT. IEEE Internet of Things Journal, 2019, 7(4): 2553-2562

[34] Ma M, Fan S, Feng D. Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine. Journal of Information Security and Applications, 2020, 55: 102652

[35] Yang N, Zhou Q, Huang Q, et al. Multi-recipient encryption with keyword search without pairing for cloud storage. Journal of Cloud Computing, 2022, 11(1): 1-12

[36] Chenam V B, Ali S T. A designated cloud server-based multi-user certificateless public key authenticated encryption with conjunctive keyword search against IKGA. Computer Standards & Interfaces, 2022, 81: 103603

[37] Miller V S. Use of elliptic curves in cryptography//Proceedings of the Advances in Cryptology — CRYPTO'85. Berlin, Germany, 1985: 417-426

[38] Bösch C, Hartel P, Jonker W, et al. A survey of provably secure searchable encryption. ACM Computing Surveys, 2014, 47(2): 1-51

[39] Akinyele J A, Garman C, Miers I, et al. Charm: A framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 2013, 3(2): 111-128

[40] Standards for Efficient Cryptography Group. SEC 2: Recommended elliptic curve domain parameters, Version 1.0. Available: https://www.secg.org/SEC2-Ver-1.0.pdf

LIU Hang, Ph. D. candidate. His research interests include public key cryptography and blockchain technology.

MING Yang, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

WANG Chen-Hao, Ph. D. candidate. His research interests include public key cryptography and digital twin security.

ZHAO Yi, Ph. D., lecturer. His research interests include cryptography and network security.

Background

In 2004, Boneh et al. utilized the identity-based cryptosystem to present the public-key encryption with keyword search (PEKS) scheme, which solved the problem of ciphertext retrieval in the public key scenario. Subsequently, some related schemes, such as identity-based encryption with keyword search (IBEKS), certificateless PEKS (CLPEKS), have been proposed by scholars. However, these schemes have some inherent drawbacks, i.e., certificate management problem, key escrow problem, or the use of secure channel. To eliminate these problems, Lu et al. put forward the conception of certificated-based searchable encryption (CBSE). Whereas, existing CBSE schemes don't consider the search pattern for multiple recipients, which considerably reduces efficiency. In addition, they either use time-consuming bilinear pairing operations or cannot achieve sender anonymity.

This paper makes up the gaps by presenting the multi-recipient certificated-based searchable encryption scheme. The proposed scheme achieves the property of sender anonymity and supports multi-recipient for keyword search without using bilinear pairing. The security proof indicates that the proposed scheme satisfies the indistinguishability under adaptive chosen keyword attack and the indistinguishability under adaptive keyword guessing attack. By performing performance analysis, compared with the related schemes, when the number of receivers is 100, the computation cost of the algorithm KwEnc of the proposed scheme reduces about 82.84% and 22.63%, and the computation cost of the algorithm Test of the proposed scheme reduces about 96.03% and 93.75%, respectively; when the number of keywords is 100, the computation cost of the algorithm Test of the proposed scheme reduces about 57.89% and 44.45%, respectively. At the same time, the proposed scheme has the lowest communication cost compared to related schemes. This undoubtedly reveals the practicability of the proposed scheme in a real cloud storage scenario.

This work was supported in part by the National Natural Science Foundation of China under Grant No. 62072054, the Key Research and Development Program of Shaanxi Province under Grant Nos. 2021GY-047 and 2022GY-032, the Xi'an Science and Technology Planning Program under Grant No. 23ZDCYJSGG0009-2022 and the Fundamental Research Funds for the Central Universities, CHD, under Grant No. 300102242201.