基于身份的具有否认认证的关键字可搜索加密方案

曹素珍[①] 丁宾宾*[①] 丁晓晖[①] 窦凤鸽[①] 王彩芬[②]

[①](西北师范大学 兰州 730000)

[②](深圳技术大学 深圳 518118)

摘 要：云存储技术的发展实现了资源共享，为用户节省了数据管理开销。可搜索加密技术，既保护用户隐私又支持密文检索，方便了用户查找云端密文数据。现有的公钥关键字可搜索加密方案虽然支持身份认证，但未实现否认的属性。为了更好地保护发送者的身份隐私，该文将否认认证与公钥关键字可搜索加密技术相结合，提出一种基于身份的具有否认认证的关键字可搜索加密方案(IDAPKSE)。在该方案中，发送者上传密文后，能够对自己上传密文这一通信行为进行否认，与此同时，接收者可以确认密文数据的来源，但是，即使与第三方合作，接收者也不能向第三方证明其所掌握的事实。在随机预言模型下，基于Bilinear Diffie-Hellman(BDH)和Decisional Bilinear Diffie-Hellman(DBDH)数学困难问题，证明了该文方案满足不可伪造性、密文和陷门的不可区分性。

关键词：身份隐私；否认认证；可搜索加密

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2021)00-0001-07

DOI: 10.11999/JEIT210155

Identity-based Public Key Keyword Searchable Encryption Scheme with Denial Authentication

CAO Suzhen[①] DING Binbin[①] DING Xiaohui[①] DOU Fengge[①]

WANG Caifen[②]

[①](*Northwest Normal University*, *Lanzhou* 730000, *China*)

[②](*Shenzhen Technology University*, *Shenzhen* 518118, *China*)

Abstract: The development of cloud storage technology achieves resource sharing, which reduces users data management overhead. Searchable encryption technology protects users' privacy and supports ciphertext retrieval, making it easy for users to find encrypted data in the cloud. Although existing public key searchable encryption schemes support authentication, the denial property is not implemented. To better protect the sender's identity privacy, we propose an Identity-based Public Key keyword Searchable Encryption scheme with denial authentication(IDAPKSE). In the proposed scheme, the sender uploads the ciphertext and has the ability to deny that he or she uploaded the ciphertext to the cloud server. At the same time, the receiver can confirm the origin of the ciphertext, however, even with the cooperation of a third party, the receiver cannot prove the facts in his/her possession to the third party. Under the random oracle model, based on the Bilinear Diffie-Hellman(BDH) and Decisional Bilinear Diffie-Hellman(DBDH) assumptions, the proposed scheme satisfies unforgeability of the ciphertexts, and indistinguishability of ciphertexts and trapdoors.

Key words: Privacy of identity; Denial of authentication; Searchable encryption

1 引言

云存储技术[1]的发展实现了资源共享，帮助用户降低了存储成本。考虑到云端数据的敏感性，数据需要被加密后存放在云端，传统数据加密技术[2]虽有效地保护了数据的隐私，但同时又带来了对云端密文数据检索的难题。可搜索加密技术[3]在保护用户的隐私的同时又支持密文检索，在云存储中得到了广泛的应用。

2004年，Boneh等人[4]提出了第1个公钥可搜索加密方案(Public Key Encryption with Keyword Search, PEKS)，该方案既支持密文检索又实现了

收稿日期：2021-02-18

*通信作者： 丁宾宾 850216860@qq.com

基金项目：国家自然科学基金(61662071, 61662069)

Foundation Items: The National Natural Science Foundation of China (61662071,61662069)

数据共享，但搜索效率低，安全性较差。2006年，Byun等人[5]指出PEKS方案存在离线关键字猜测攻击(Keyword Guessing Attack, KGA)[6]的风险。传统的公钥可搜索加密方案需要证书颁发机构发布和管理用户的证书，基于身份密码体制[7]下的公钥可搜索加密方案解决了复杂的证书管理问题。2014年，Tseng等人[8]在身份密码体制下提出了指定测试者的可搜索加密方案，该方案具有密文和陷门不可区分性，由于该方案并未完全定义在身份密码系统架构上，不能完全满足密文不可区分性。王少辉等人[9]在Tseng等人方案基础上设计了一个具有更高效率可搜索加密方案，证明了密文不可区分性是抵御离线关键字猜测攻击的充分条件，故Tseng等人方案也存在离线关键字猜测攻击的风险。2017年，Huang等人[10]提出了具有公钥认证的可搜索加密方案，通过对关键字认证和加密，以抵御内部离线关键字猜测攻击。但该方案存在一个缺点，若云服务器被外部攻击者攻破，用户的搜索隐私将被泄露。

为了保护用户的搜索隐私，Baek等人[11]提出在拥有陷门而没有接收者私钥的情况下，一个指定测试者无法完成云端密文数据的检索，但该方案无法抵御离线关键字猜测攻击。为了提高离线关键字猜测攻击下的安全性。2019年，Li等人[12]提出了指定服务器的基于身份认证的关键字可搜索加密方案，Lu等人[13]借鉴签密思想，实现了在关键字加密过程中，敌手不能试图通过产生合法关键字密文以达到匹配陷门的目的。普遍存在的缺陷是上述方案均没有考虑到对发送者身份隐私保护的问题。

如今，个人信息和隐私趋于透明化。在电子投票、医疗信息、电子邮件、行政和司法报告等应用环境中，如何保护发送者的身份隐私，使其能够否认发送消息的行为已成为研究热点。否认认证协议由Dwork等人[14]首次提出，该协议基于零知识证明来定义，接收者可以确认消息发送者的身份，但无法向第三方证明这一事实。Li等人[15]在身份密码体制下提出了具有更高效率的否认认证加密方案，并在电子邮件系统中得到了很好的应用。Wu等人[16]在身份密码体制下提出了同时具有认证性和否认性的否认认证加密方案。

在基于身份的密码体制下，本文提出了具有否认属性的关键字可搜索加密方案，将否认认证与关键字可搜索加密技术相结合，在随机预言模型下，基于BDH和DBDH数学困难问题，证明了方案满足不可伪造性、密文和陷门不可区分性，同时具有否认性，即第三方无法确认消息的真实发送者，从而保护了发送者的身份隐私。

2 IDAPKSE方案安全模型

2.1 IDAPKSE方案系统模型

IDAPKSE方案中有密钥分发中心、发送者、接收者和云服务器4类实体，系统模型图如图1所示。

(1) 密钥分发中心(Key Generation Center, KGC)：KGC生成系统参数params和主密钥s，并为发送者、接收者和云服务器提供私钥SKi。

(2) 发送者(Data Sender, DS)：DS对明文和所选关键字加密，将密文上传到云服务器。

(3) 接收者(Data Receiver, DR)：DR运行陷门生成算法，将生成的陷门上传到云服务器。

(4) 云服务器(Cloud Server, CS)：存储发送者上传的密文数据，并通过接收者上传的陷门，进行密文检索。

2.2 IDAPKSE方案形式化定义

IDAPKSE方案包括以下算法：

(1) Setup (k)：KGC输入安全参数k，返回系统参数params和主密钥s。

(2) 密钥提取算法：(a)发送者和接收者密钥提取：KGC输入主密钥s和身份标识IDi，返回公私钥对(PKi, SKi)；(b)云服务器密钥提取：KGC输入系统参数params，返回云服务器的公私钥对$(\mathrm{PK_C}, \mathrm{SK_C})$。

(3) 关键字否认认证加密算法：发送者输入参数params、关键字w、发送者身份$\mathrm{ID_S}$和私钥$\mathrm{SK_S}$、云服务器的公钥$\mathrm{PK_C}$、接收者的身份$\mathrm{ID_R}$和公钥$\mathrm{PK_R}$，返回密文C并上传到云服务器。

(4) 陷门生成算法：接收者输入系统参数params、关键字w、发送者身份$\mathrm{ID_S}$和接收者身份$\mathrm{ID_R}$，输出陷门T_w。

(5) 测试算法：云服务器输入系统参数params、服务器私钥$\mathrm{SK_C}$和陷门T_w，输出ϕ。若接收者的上

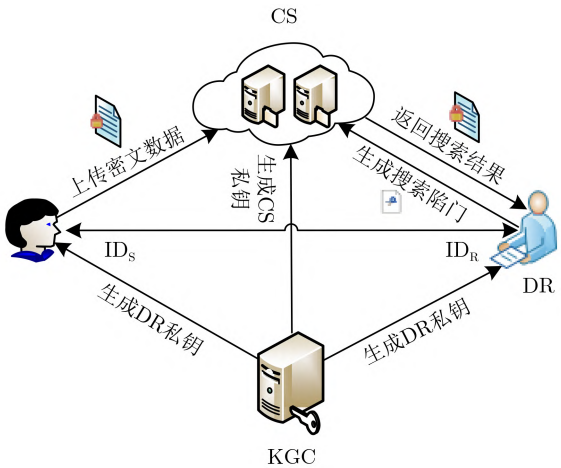

图 1 系统模型图

传的陷门与发送者上传的关键字密文中包含相同的关键字，则$\phi=1$，否则$\phi=0$。

2.3 IDAPKSE方案安全模型

IDAPKSE方案的安全性主要考虑为不可伪造性、密文和陷门的不可区分性、否认性。下面通过挑战者β和敌手$\alpha_i\ (i=1,2,3,4)$之间的游戏给出方案的安全模型。

游戏 1　不可伪造性

(1) Setup (k)：β输入安全参数k,返回系统参数params给α_1，自身保留主密钥s，运行密钥提取算法，返回云服务器公私钥对$(\mathrm{PK_C}, \mathrm{SK_C})$。

(2) 私钥询问阶段：α_1对目标身份外的用户进行私钥询问，β运行密钥提取算法返回私钥给α_1。

(3) 关键字否认认证加密询问阶段：α_1向β提交发送者身份$\mathrm{ID_S}$、接收者身份$\mathrm{ID_R}$和关键字w。β运行密钥提取算法得到发送者的私钥$\mathrm{SK_S}$，运行关键字否认认证加密算法，返回密文C给α_1。

(4) 陷门询问阶段：α_1可以对挑战关键字外的任意关键字进行陷门询问。β通过α_1选取的关键字w，运行陷门生成算法生成陷门T_w，返回给α_1。

(5) 伪造阶段：α_1输入$(w^*, \mathrm{PK_{C^*}}, \mathrm{PK_{S^*}}, \mathrm{PK_{R^*}}, \mathrm{ID_{S^*}}, \mathrm{ID_{R^*}})$，生成$\mathrm{ID_{S^*}}$和$\mathrm{ID_{R^*}}$下的合法密文$C^*$。若$\alpha_1$未对$\mathrm{ID_{S^*}}$和$\mathrm{ID_{R^*}}$进行私钥询问，则在游戏1中获胜。

游戏 2　密文不可区分性

(1) Setup (k)、私钥询问阶段、关键字否认认证加密询问阶段和陷门询问阶段同游戏1。

(2) 挑战阶段：α_2向β提交发送者的身份$\mathrm{ID_S}$和接收者的身份$\mathrm{ID_R}$、挑战关键字(w_0^*, w_1^*)。β随机选择$b\in\{0,1\}$，生成w_b密文C^*返回给α_2。

(3) α_2继续执行以上的询问。

(4) 猜测阶段：α_2输出$b'\in\{0,1\}$，若$b'=b$，α_2未对$\mathrm{ID_{S^*}}$和$\mathrm{ID_{R^*}}$进行私钥询问且未对(w_0^*, w_1^*)进行关键字否认认证加密询问，则在游戏2中获胜。

α_2赢得游戏2优势为

$$\mathrm{Adv}_{\alpha_2}(k)=\left|\Pr\left[b'=b\right]-1/2\right| \tag{1}$$

游戏 3　陷门不可区分性

(1) Setup (k)、私钥询问阶段、关键字否认认证加密询问阶段和陷门询问阶段同游戏1。

(2) 挑战阶段：α_3向β提交发送者的身份$\mathrm{ID_S}$和接收者的身份$\mathrm{ID_R}$、挑战关键字(w_{0^*}, w_{1^*})。β随机选择$b\in\{0,1\}$，生成w_b的陷门T_{w^*}返回给α_3。

(3) α_3继续执行以上的询问。

(4) 猜测阶段：α_3输出$b'\in\{0,1\}$，若$b'=b$，α_3未对$\mathrm{ID_{S^*}}$和$\mathrm{ID_{R^*}}$进行私钥询问且未对关键字(w_{0^*}, w_{1^*})进行关键字否认认证加密和陷门询问，则在游戏3中获胜。

α_3赢得游戏3优势为

$$\mathrm{Adv}_{\alpha_3}(k)=\left|\Pr\left[b'=b\right]-1/2\right| \tag{2}$$

游戏 4　否认性

(1) Setup (k)：假设β能够为系统中的任何诚实用户生成IDAPKSE方案下的合法密文，选择两个诚实的用户D_0和D_1。

(2) 挑战阶段：α_4向β提交明文消息M，β随机选择$b\in\{0,1\}$，并与D_b交互，使D_b能够将M生成IDAPKSE方案下的合法密文C^*返回给α_4。

(3) 区分阶段：α_4输出$b'\in\{0,1\}$，若$b'=b$，则α_4在游戏4中获胜。

因游戏中D_0和D_1生成的密文的概率分布是相同的，所以对于区分者是不可区分的。

α_4赢得游戏4优势为

$$\mathrm{Adv}_{\alpha_4}(k)=\left|\Pr\left[b'=b\right]-1/2\right| \tag{3}$$

3 IDAPKSE方案

3.1 具体方案

(1) Setup (k)：输入安全参数k，KGC执行以下操作：(a)选择q阶循环群G_1和G_2，g为G_1的生成元，再选择双线性映射$e: G_1\times G_1\to G_2$；(b)在G_1群中选择生成元U和h，KGC随机选择$s\in Z_{q^*}$作为主密钥，并计算公钥$P_{\mathrm{pub}}=sU$；(c)定义3个抗碰撞的哈希函数：$H_1:\{0,1\}^*\to G_1$；$H_2: G_2\times\{0,1\}^*\to G_1$；$H_3:\{0,1\}^*\to Z_{q^*}$。KGC保留主密钥$s$，公开系统参数$\mathrm{params}=\{k, q, G_1, G_2, U, h, g, P_{\mathrm{pub}}, H_1, H_2, H_3\}$。

(2) 密钥提取算法：(a)发送者和接收者密钥提取：发送者和接收者将身份IDi发送给KGC，KGC计算对应公钥$Q_i=H_1(\mathrm{ID}i)$和私钥$\mathrm{SK}_i=sQ_i$，并通过安全信道将私钥返回给发送者和接收者；(b)云服务器密钥提取：KGC随机选择$t\in Z_{q^*}$作为云服务器私钥；输入t和系统参数params，计算云服务器公钥$\mathrm{PK_C}=tg$。

(3) 关键字否认认证加密算法：发送者输入系统参数params、关键字w、发送者身份$\mathrm{ID_S}$和公私钥对$(\mathrm{PK_S}, \mathrm{SK_S})$、接收者身份$\mathrm{ID_R}$和公钥$\mathrm{PK_R}$、云服务器公钥$\mathrm{PK_C}$，按以下步骤加密关键字：

(a)计算：$Q_\mathrm{S}=H_1(\mathrm{IDs})$, $Q_\mathrm{R}=H_1(\mathrm{ID_R})$, $T=rQ_\mathrm{S}$其中$r\in Z_{q^*}$；

(b)计算：$C_1=e\left(H_2\left(Z, w\right), \mathrm{PK_C}\right)^r$，其中$Z=e\left(\mathrm{SK_S}, Q_\mathrm{R)}\right)$；

(c)计算：$C_2=rg$, $C_3=rh$；

(d)计算：$Y=H_3\left(w||\mathrm{ID_R}||\mathrm{ID_S}, T\right)$；

(e)计算：$V=e\left((r+Y)\,\mathrm{SK_S}, Q_\mathrm{R}\right)$；

(f)$C=(T, C_1, C_2, C_3, V)$，将C上传到云服务器。

(4) 陷门生成算法：接收者输入系统参数params、关键字w、发送者公钥$\mathrm{PK_S}$和接收者私钥$\mathrm{SK_R}$, 按下步骤生成关键字陷门：

(a)计算：$Z'=e\left(H_1\left(\mathrm{ID_S}\right), \mathrm{SK_R}\right)$;

(b)计算：$T_1=ag$，$T_2=H_2\left(Z', w\right)+ah$，其中$a\in Z_q^*$，将陷门$T_w=(T_1, T_2)$上传到云服务器。

(5) 测试算法：云服务器运行该算法，验证等式$C_1\cdot e\left(\mathrm{SK_C}T_1, C_3\right)=e\left(\mathrm{SK_C}T_2, C_2\right)$是否成立，若成立，说明关键字密文与陷门相匹配，返回1，否则返回0。

(6) 解密算法：若关键字密文与陷门相匹配，云服务器将关键字密文C发送给接收者，接收者利用自身私钥$\mathrm{SK_R}$在本地执行解密操作。

3.2 IDAPKSE方案正确性分析

IDAPKSE方案的正确性当且仅当验证等式$C_1\cdot e\left(\mathrm{SK_C}T_1, C_3\right)=e\left(\mathrm{SK_C}T_2, C_2\right)$是否成立

$$\begin{aligned}e\left(\mathrm{SK_C}T_2, C_2\right)&=e\left(t\left(H_2\left(Z', w\right)+ah\right), rg\right)\\&=e\left(tH_2\left(Z', w\right), rg\right)\cdot e\left(tah, rg\right)\\&=e\left(H_2\left(Z', w\right), tg\right)^r\cdot e\left(tag, rh\right)\\&=e\left(H_2\left(Z, w\right), tg\right)^r\cdot e\left(tag, rh\right)\\&=e\left(H_2\left(Z, w\right), \mathrm{PK_C}\right)^r\cdot e\left(tag, rh\right)\\&=C_1\cdot e\left(\mathrm{SK_C}T_1, C_3\right)\end{aligned}\tag{4}$$

因为

$$\begin{aligned}Z'&=e\left(H_1\left(\mathrm{ID_S}\right), \mathrm{SK_R}\right)\\&=e\left(H_1\left(\mathrm{ID_S}\right), sH_1\left(\mathrm{ID_R}\right)\right)\\&=e\left(sH_1\left(\mathrm{ID_S}\right), H_1\left(\mathrm{ID_R}\right)\right)\\&=e\left(\mathrm{SK_S}, Q\mathrm{R}\right)\\&=Z\end{aligned}\tag{5}$$

所以$C_1\cdot e\left(\mathrm{SK_C}T_1, C_3\right)=e\left(\mathrm{SK_C}T_2, C_2\right)$成立。

4 安全性分析

4.1 不可伪造性

引理1 在随机预言模型下，若敌手α_1在时间t内赢得游戏1，则存在算法$\mathbb{C}$可以解决BDH问题。

证明 挑战者β输入1个随机的BDH问题实例(P, aP, bP, cP)，目标计算$e\left(P, P\right)^{abc}$。

(1) Setup (k)：β输入安全参数k,返回系统参数params给α_1。设置公钥$P_{\mathrm{pub}}=cP$，c为主密钥。

(2) 攻击阶段：β维护L_1, L_2, L_3列表，将其初始化为空，分别作为α_1对随机预言机H_1, H_2, H_3的查询追踪，α_1执行多项式有界次查询：

(a)公钥询问：α_1向β提交任意用户身份IDi，β检查L_1。

若未对IDi进行任何询问，IDi为$\perp$，β得到(IDi, ni)，随机选择$xi\in Z_q^*$作为私钥SKi，计算公钥PK$i=xiP$，返回PKi给α_1并向列表L_1中添加一个新的元组(IDi, PKi, SKi, ni)。

若IDi不为$\perp$，L_1列表中存在相应的元组，则返回存在的结果。

(b)私钥询问：α_1提交用户身份IDi，获取相应的用户私钥，若ID$i=\mathrm{ID_S}$或ID$i=\mathrm{ID_R}$，结束模拟。否则，β检查列表L_1。

若未对IDi进行任何询问，IDi为$\perp$，β得到(IDi, ni)，随机选择$xi\in Zq^*$作为私钥SKi，计算公钥PK$i=xiP$，返回SKi给α_1，并向列表L_1中添加一个新的元组(IDi, PKi, SKi, ni)。

若IDi不为$\perp$，L_1列表中存在相应的元组，则返回存在的结果。

(c)关键字否认认证加密询问：α_1向β提交选定的发送者身份$\mathrm{ID_S}$和接收者身份$\mathrm{ID_R}$和关键字w,β执行以下操作：

若α_1提交的IDi与β选择的两个身份不同，即ID$i\neq\mathrm{ID_S}$和ID$i\neq\mathrm{ID_R}$。β运行密钥提取算法得到发送者私钥$\mathrm{SK_S}$，运行关键字否认认证加密算法生成密文C返回给α_1。

若α_1提交发送者身份IDi是β选择的两个身份之一，即ID$i=\mathrm{ID_S}$或ID$i=\mathrm{ID_R}$，但接收者身份ID$j\neq\mathrm{ID_S}$且ID$j\neq\mathrm{ID_R}$。β不能计算发送者的私钥，但能计算接收者的私钥$\mathrm{SK}j=njP_{\mathrm{pub}}$。$\beta$随机选择$r\in Z_q^*$，进行以下计算：

(a)计算：$T=rQ_i, C_1=e\left(H_2\left(e\left(T, \mathrm{SK}j\right), w\right), \mathrm{PK_C}\right)^r$;

(b)计算：$C_2=rg$,$C_3=rh$;

(c)计算：$Y=H_3\left(w||\mathrm{ID}i||\mathrm{ID}j, T\right)$;

(d)计算：$V=e\left(T+YQi\right), \mathrm{SK}j)$;

(e)$C=(T, C_1, C_2, C_3, V)$，返回密文C给α_1。

若α_1提交发送者身份与β选中身份相同，即ID$i=\mathrm{ID_S}$且ID$j=\mathrm{ID_R}$或ID$j=\mathrm{ID_S}$且ID$i=\mathrm{ID_R}$。这时，β不能够计算发送者和接收者的私钥，β随机选择$r, h\in Z_q^*$，进行以下计算：

(a)计算：$T=rP-hQi, Y=H_3\left(w||\mathrm{ID_R}||\mathrm{ID_S}, T\right)$，向列表$L_3$中添加元组$(w||\mathrm{ID_R}||\mathrm{ID_S}, T, h)$;

(b)计算：$C_1=e\left(H_2\left(e\left(\mathrm{SK_S}, Q\mathrm{R}\right), w\right), \mathrm{PK}_C\right)^r$，向列表$L_2$中添加元组$(\mathrm{PK_S}, \mathrm{PK_R}, C_1, V)$，其中$V=e\left(r+Y\right)\mathrm{SK_S}, Q_{\mathrm{R}})$;

(c)$C=(T, C_1, C_2, C_3, V)$，返回密文C给α_1。

(d)伪造阶段：α_1输出发送者身份$\mathrm{ID_R}$、接收者身份$\mathrm{ID_S}$和密文$C^*=(T^*, C_1^*, C_2^*, C_3^*, V^*)$。其中，$\alpha_1$未对$\mathrm{ID_S}$和$\mathrm{ID_R}$进行私钥询问，不确定$C^*$是否为有效密文。由分叉引理[17]知，如果$\alpha_1$为上述

游戏中的一个成功的伪造者，那么可以构造α_{1^*}，α_{1^*}能够生成具有相同部分密文T^*的元组($\mathrm{ID_R}$，$\mathrm{ID_S}$，C^*，C_1^*,C_2^*，C_3^*，Y^*，V^*)和($\mathrm{ID_R}$，$\mathrm{ID_S}$，C^*，C_1^*,C_2^*，C_3^*，Y_1^*，V_1^*)，其中$Y1^* \neq Y^*$。

目前没有公认的解决BDH困难问题的有效算法，因此α_1不存在，方案满足密文的不可伪造性。

4.2 密文不可区分性

引理2 在随机预言模型下，若敌手α_2在时间t内赢得游戏2，则有算法$\mathbb{C}$可以解决DBDH问题。

证明 挑战者β输入一个随机的DBDH问题实例(G_1，G_2，e，q，g，xg，yg，zg，Z)，目标是解决DBDH问题。

(1) Setup(k)：β输入安全参数k,，返回$\mathrm{params}=\{k,q,G_1,G_2,e,P,h,g,P_{\mathrm{pub}}\}$，其中$P_{\mathrm{pub}}=ZP$，$Z$为主密钥。计算云服务器公私钥对$\mathrm{PK_C}=tg$和$\mathrm{SK_C}=t$，将params和云服务器公私钥对($\mathrm{PK_C}$，$\mathrm{SK_C}$)返回给$\alpha_2$。

(2) 攻击阶段：β维护L_1，L_2，L_3列表，将其初始化为空，分别作为α_2对随机预言机H_1，H_2，H_3的查询追踪，α_2执行多项式有界次查询：

(a)公钥询问，私钥询问和关键字否认认证加密询问同上文不可伪造性证明。

(b)陷门询问阶段：α_2向β提交选择的发送者身份$\mathrm{ID_S}$、接收者身份$\mathrm{ID_R}$和关键字w，β执行以下操作：

若α_2提交的发送者的身份与β选取的身份相同，即$\mathrm{ID}i=\mathrm{ID_S}$且$\mathrm{ID}j=\mathrm{ID_R}$或$\mathrm{ID}i=\mathrm{ID_R}$且$\mathrm{ID}j=\mathrm{ID_S}$，计算$T_1=ag$，$T_2=H_2(Z,w)+ah$，返回陷门$T_w=(T_1,T_2)$给$\alpha_2$。

若α_2提交的发送者的身份$\mathrm{ID}i$最多与β选择的两个身份中的一个相同，则计算$T_1=ag$，$T_2=H_2(Zg,w)+ah$，返回陷门$Tw=(T_1,T_2)$给α_2。

(3) 挑战阶段：α_2输出两个挑战关键词(w_0^*,w_1^*)、发送者身份$\mathrm{ID_S}$和接收者身份$\mathrm{ID_R}$。β随机选取$b\in\{0,1\}$，随机选择$r\in Z_q^*$，返回密文$C^*=(T^*,C_1^*,C_2^*,C_3^*,V^*)$给$\alpha_2$。

(4) α_2继续执行上询问。

(5) 猜测阶段：α_2输出$b'\in\{0,1\}$，若$b'=b$，输出1，否则输出0。

$\overline{F}$表示对挑战身份的猜测是不正确的，挑战者β将中止。

若β中止，则β随机输出b的概率为1/2。当β随机猜测时，$\overline{F}$不发生的概率是$1/(q_H(q_H-1))$，即$\Pr(F)=1/(q_H(q_H-1))$，q_H为α_2最多询问次数。

若β不被中止，$\alpha 2$最多赢得游戏2的概率1/2，故β解决DBDH困难问题的优势为：

$$\begin{aligned}\mathrm{Adv}_{\beta}^{\mathrm{DBDH}}(k)=&|\Pr[b=b'|F]\cdot\Pr[F]\\&+|\Pr[b=b'|\overline{F}]\cdot\Pr[\overline{F}]-1/2|\\=&1/2\Pr[\overline{F}]\cdot\mathrm{Adv}_{\alpha 2}^{\beta}(k)\\=&\frac{1}{2q_H(q_H-1)}\mathrm{Adv}_{\alpha 2}^{\beta}(k))\end{aligned}$$

如果$\mathrm{Adv}_{\alpha 2}^{\beta}(k)$是不可忽略的，则$\mathrm{Adv}_{\beta}^{\mathrm{DBDH}}(k)$不可忽略。因此，该方案具有密文不可区分性。

4.3 陷门不可区分性

引理3 若DBDH假设为真，则本文方案满足陷门不可区分性。

证明 证明过程与引理2相似，不同之处在于，在引理3的证明中，挑战者β随机选择$a\in Z_q^*$，计算$T_1^*=ag$，$T_2^*=H_2(Z',w^*)+ah$，生成挑战陷门$T_w^*=(T_1^*,T_2^*)$。因篇幅限制，这里省略了详细的证明。

4.4 否认性

在本文方案中，接收者在收到密文$C=(T,C_1,C_2,C_3,V)$后，用私钥对密文解密得到明文M，运行模拟算法构造M的合法密文$C^*=(T^*,C_1^*,C_2^*,C_3^*,V^*)$。由于密文$C$和$C^*$是无法区分的，第三方无法判断$C^*$是发送者或接收者加密后得到，模拟算法如下：

(a)计算：$T^*=xQ_{\mathrm{S}}$，其中$C_3^*=xh$；

(b)计算：$C_1^*=e(H_2(Z,w),\mathrm{PK_C})^x$，其中$Z=e(\mathrm{SK_S},Q\mathrm{R})$；

(c)计算：$C_2^*=xg$，$C_3^*=xh$；

(d)计算：$Y^*=H_3(w||\mathrm{ID_R}||\mathrm{ID_S},T^*)$；

(e)计算：$V^*=e(x+Y^*)\mathrm{SK_S},Q_{\mathrm{R}})$；

$C^*=(T^*,C_1^*,C_2^*,C_3^*,V^*)$是接收者运行模拟算法生成的$M$的合法密文，由于密文$C$和$C^*$具有相同的概率分布，第三方无法区分哪个密文由发送者发送，发送者可以否认他已经生成了密文的行为。

5 分析和比较

5.1 安全功能分析

公开发表的文献显示，目前还没有基于身份的具有否认认证的关键字可搜索的加密方案。因此，本文的方案不能与同类方案进行比较。本文方案将在关键字加密、陷门生成和关键字密文检索3个方面与文献[8,10,12]的方案进行比较，表1为各方案功能对比。

从表1可以看出本文方案和文献[8,12]的方案都是在基于身份密码体制下构建且指定测试者，文献[10,12]的方案和本文方案能够抵御内部和外部关键字猜测攻击，文献[8]的方案能够抵御外部关键字猜测攻击，但不能抵御内部关键字猜测攻击。

表 1 各方案功能对比

方案	基于身份	指定测试	防止外部关键字猜测攻击	防止内部关键字猜测攻击
文献[8]	√	√	√	×
文献[10]	×	×	√	√
文献[12]	√	√	√	√
IDAPKSE	√	√	√	√

5.2 计算量分析

表2为各方案计算量对比，E为双线性对运算，E为指数运算，M为点乘运算，H为哈希运算。表3为基本运算所消耗的时间，在关键字加密阶段，本文方案有3个双线性对运算，文献[8,12]分别存在1、2个双线性对运算，文献[10]没有对运算，计算量由大到小依次为：文献[12]、本文方案、文献[10]、文献[8]；在陷门生成阶段，本文方案与文献[10,12]都存在1个对运算，文献[8]没有对运算，计算量由大到小依次为：文献[12]、文献[10]、本文方案、文献[8]；在关键字密文检索阶段，各个方案都存在2个对运算，文献[8]多出1个哈希运算，文献[12]多出2个指数运算，计算量由大到小依次为：文献[12]、文献[8]、本文方案、文献[10]。综合以上分析，本文方案在关键字加密和生成陷门阶段，计算效率偏低，计算性能上并未占据优势。在关键字密文检索阶段，本文方案与文献[10]的计算效率相似，与文献[8,12]相比，具有更佳的计算性能表现。

5.3 时间性能分析

本节通过仿真实验将本文方案与文献[8,10,12]的方案在关键字加密、陷门生成和关键字密文检索3个方面进行了对比，加密函数由PBC[18]提供，实验环境为Lenovo笔记本(AMD Ryzen 5 4600U with Radeon Graphics @2.10 Hz，16GB内存和Linux实验选取关键字分别为：1，50，100，300，500，700，900，1000，实验结果如图2所示。从图2可以看出在关键字加密阶段，随着关键字数量的增加，关键字加密的时间也在增加，在关键字数量相同的情况下，本文方案在加密阶段加密时间小于文献 [12]，相较于文献[8]，本文方案比文献[8]多出2个对运算，加密时间比文献[8]要长。在陷门生成阶段，本文方案与文献[10，12]均有1个对运算，但文献[12]中存在2个指数运算，文献[10]中存在1个指数运算，本文方案相较于文献[10，12]，优势在于在该阶段没有指数运算，生成陷门的时间相对较短，与文献[8]相比较，文献[8]在该阶段不存在对运算和指数运算，生成陷门时间比本文方案要短。在关键字密文检索阶段，各方案均有2个对运算，文献[12]中多出了两个指数运算，运算时间相对于其他方案较长，本文方案在关键字密文检索阶段比文献[8，10]多出了2个点乘运算时间，文献[8]比本文方案和文献[10]多出1个哈希运算。由表3可以看出，点乘耗费时间最短，检索关键字密文所耗费的时间本文方案接近于文献[10]。本文方案在各个阶段的计算所消耗的时间相较于其他3种方案有长有

表 2 计算量对比

方案	关键字加密	陷门生成	关键字密文检索
文献[8]	P+3M+2H	2M+H	2P+M+H
文献[10]	3E+M+H	P+E+H	2P+M
文献[12]	2P+3E+2H	P+2E+M+2H	2P+2E+M
IDAPKSE	3P+E+4M+2H	P+2M+H	2P+3M

表 3 基本运算耗费时间

操作	T_{H}	T_{E}	T_{M}	T_{p}
时间(ms)	3.301	2.864	0.135	3.658

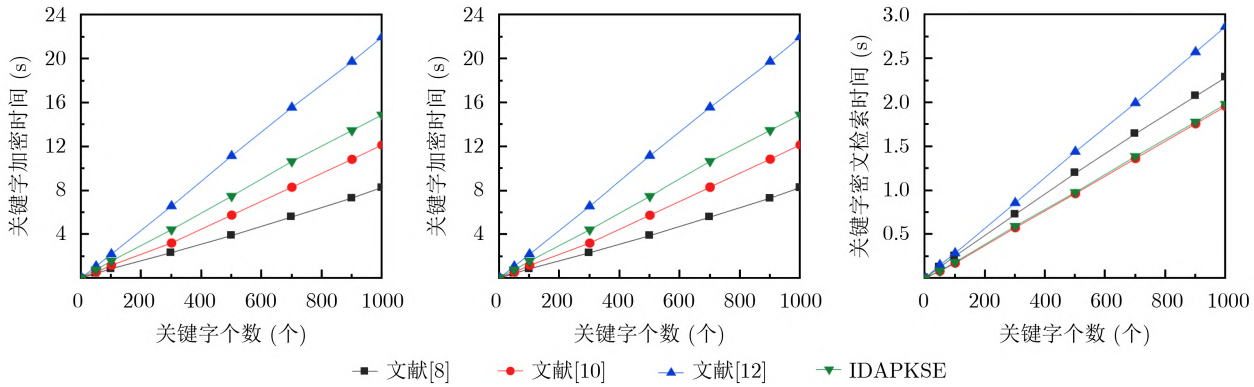

图 2 算法运行时间比较

短，但本文最大的优势在于实现了否认属性，对发送者的隐私有了很好的保护，在电子邮件、医疗信息等方面有着较好的应用前景。

6　结束语

本文方案将关键字可搜索加密与否认认证加密相结合，基于BDH和DBDH困难问题证明了方案满足不可伪造性、密文和陷门的不可区分性。本文方案中的否认属性，在保护发送者身份隐私上具有较高的实用性。不足的是本文方案基于身份密码体制构建，基于身份的密码体制虽解决了PKI中的证书管理问题，但也存在密钥托管和密钥撤销的缺陷，未来我们将否认认证加密迁移到无证书密码体制下，利用无证书优势解决密钥托管问题。

参 考 文 献

[1] 白利芳, 祝跃飞, 芦斌. 云数据存储安全审计研究及进展[J]. 计算机科学, 2020, 47(10): 290–300. doi: 10.11896/jsjkx.191000111.
BAI Lifang, ZHU Yuefei, and LU Bin. Research and development of data storage security audit in cloud[J]. *Computer Science*, 2020, 47(10): 290–300. doi: 10.11896/jsjkx.191000111.

[2] 韩培义, 刘川意, 王佳慧, 等. 面向云存储的数据加密系统与技术研究[J]. 通信学报, 2020, 41(8): 55–65. doi: 10.11959/j.issn.1000-436x.2020140.
HAN Peiyi, LIU Chuanyi, WANG Jiahui, *et al*. Research on data encryption system and technology for cloud storage[J]. *Journal on Communications*, 2020, 41(8): 55–65. doi: 10.11959/j.issn.1000-436x.2020140.

[3] YANG Ningbin, XU Shumei, and QUAN Zhou. An efficient public key searchable encryption scheme for mobile smart terminal[J]. *IEEE Access*, 2020, 8: 77940–77950. doi: 10.1109/ACCESS.2020.2989628.

[4] BONEH D, DI CRESCENZO G, OSTROVSKY R, *et al*. Public key encryption with keyword search[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, 2004: 506–522. doi: 10.1007/978-3-540-24676-3_30.

[5] BYUN J W, RHEE H S, PARK H A, *et al*. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[C]. The 3rd VLDB Workshop on Secure Data Management, Seoul, 2006: 75–83. doi: 10.1007/11844662_6.

[6] LU Yang and LI Jiguo. Efficient searchable public key encryption against keyword guessing attacks for cloud-based EMR systems[J]. *Cluster Computing*, 2019, 22(1): 285–299. doi: 10.1007/s10586-018-2855-y.

[7] LIN Qun, YAN Hongyang, HUANG Zhengan, *et al*. An ID-based linearly homomorphic signature scheme and its application in blockchain[J]. *IEEE Access*, 2018, 6: 20632–20640. doi: 10.1109/ACCESS.2018.2809426.

[8] WU T Y, TSAI T T, and TSENG Y M. Efficient searchable ID-based encryption with a designated server[J]. *Annals of Telecommunications-Annales Des Télécommunications*, 2014, 69(7/8): 391–402. doi: 10.1007/s12243-013-0398-z.

[9] 王少辉, 韩志杰, 肖甫, 等. 指定测试者的基于身份可搜索加密方案[J]. 通信学报, 2014, 35(7): 22–32. doi: 10.3969/j.issn.1000-436x.2014.07.003.
WANG Shaohui, HAN Zhijie, XIAO Fu, *et al*. Identity-based searchable encryption scheme with a designated tester[J]. *Journal on Communications*, 2014, 35(7): 22–32. doi: 10.3969/j.issn.1000-436x.2014.07.003.

[10] HUANG Qiong and LI Hongbo. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks[J]. *Information Sciences*, 2017, 403/404: 1–14. doi: 10.1016/j.ins.2017.03.038.

[11] BAEK J, SAFAVI-NAINI R, and SUSILO W. Public key encryption with keyword search revisited[C]. 2008 International Conference on Computational Science and its Applications, Perugia, 2008: 1249–1259. doi: 10.1007/978-3-540-69839-5_96.

[12] LI Hongbo, HUANG Qiong, SHEN Jian, *et al*. Designated-server identity-based authenticated encryption with keyword search for encrypted emails[J]. *Information Sciences*, 2019, 481: 330–343. doi: 10.1016/j.ins.2019.01.004.

[13] LU Yang and LI Jiguo. Constructing designated server public key encryption with keyword search schemes withstanding keyword guessing attacks[J]. *International Journal of Communication Systems*, 2019, 32(3): e3862. doi: 10.1002/dac.3862.

[14] DWORK C, NAOR M, and SAHAI A. Concurrent Zero-knowledge[J]. *Journal of the ACM*, 2004, 51(6): 851–898. doi: 10.1145/1039488.1039489.

[15] LI Fagen, ZHENG Zhaohui, and JIN Chunhua. Identity-based deniable authenticated encryption and its application to e-mail system[J]. *Telecommunication Systems*, 2016, 62(4): 625–639. doi: 10.1007/s11235-015-0099-1.

[16] WU Weifeng and LI Fagen. An efficient identity-based deniable authenticated encryption scheme[J]. *KSII Transactions on Internet and Information Systems*, 2015, 9(5): 1904–1919. doi: 10.3837/tiis.2015.05.020.

[17] POINTCHEVAL D and STERN J. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396. doi: 10.1007/s001450010003.

[18] PBC Library. The pairing-based cryptography library[EB/OL]. http://crypto.stanford.edu/pbc/, 2015.

曹素珍：女，1976年生，副教授，研究方向为公钥密码学和软件安全.

丁宾宾：男，1994年生，硕士生，研究方向为密码学与信息安全.

丁晓晖：男，1997年生，硕士生，研究方向为密码学与信息安全.

窦凤鸽：女，1996年生，硕士生，研究方向为密码学与信息安全.

王彩芬：女，1963年生，教授，研究方向为密码学与信息安全.

责任编辑：余　蓉