第 46 卷 第 10 期 计 算 机 工 程 2020 年 10 月
Vol. 46 No. 10 Computer Engineering October 2020

·网络空间安全· 文章编号：1000-3428(2020)10-0137-06 文献标志码：A 中图分类号：TP309

电子邮件系统中指定服务器的关键字搜索加密方案

牛淑芬[a]，杨平平[a]，谢亚亚[a]，王彩芬[a]，杜小妮[b]

（西北师范大学 a. 计算机科学与工程学院；b. 数学与统计学院，兰州 730070）

摘 要：现有指定服务器的基于身份关键字搜索加密方案无法满足关键字密文的不可区分性，为满足电子邮件系统更高的安全需求，提出一种指定邮件服务器的身份认证关键字搜索加密方案。针对指定邮件存储服务器和数据接收者身份对关键字加密以抵抗离线关键字猜测攻击，在随机预言模型下，对该方案适应性选择消息攻击的关键字密文不可区分性、陷门不可区分性和离线猜测攻击的安全性进行验证。理论分析和数值实验结果表明，与dIBEKS方案相比，该方案在关键字加密和验证阶段计算效率更高。

关键词：加密电子邮件；指定服务器；身份认证；可搜索加密；关键字加密

开放科学(资源服务)标志码(OSID)：

中文引用格式：牛淑芬，杨平平，谢亚亚，等. 电子邮件系统中指定服务器的关键字搜索加密方案[J]. 计算机工程，2020，46(10)：137-142，150.

英文引用格式：NIU Shufen，YANG Pingping，XIE Yaya，et al. Keyword search encryption scheme for designated server in email system[J]. Computer Engineering，2020，46(10)：137-142，150.

Keyword Search Encryption Scheme for Designated Server in Email System

NIU Shufen[a]，YANG Pingping[a]，XIE Yaya[a]，WANG Caifen[a]，DU Xiaoni[b]

（a. College of Computer Science and Engineering；b. College of Mathematics and Statistics，Northwest Normal University，Lanzhou 730070，China）

【Abstract】The existing identity-based keyword search encryption schemes for designated server cannot satisfy the indistinguishability of keyword ciphertext. To meet the higher security requirements of email systems，this paper proposes an identity authentication-based keyword search encryption scheme for designated mail server. The scheme can resist off-line keyword guessing attacks by encrypting the identity of the designated mail storage server and data receiver. In the random oracle model，the following security features of the scheme such as the indistinguishability of keyword ciphertext in adaptively chosen message attacks，indistinguishability of trapdoor and security of offline guessing attacks are verified. Results of theoretical analysis and numerical experiments show that the proposed scheme has higher computational efficiency in keyword encryption and verification than dIBEKS scheme.

【Key words】encrypted email；designated server；identity authentication；searchable encryption；keyword encryption

DOI：10.19678/j.issn.1000-3428.0055654

0 概述

近年来，随着云计算技术[1]的迅速发展，基于网上在线存储的云存储服务得到广泛关注。将本地数据迁移到云端服务器可以节省本地数据管理开销、降低系统开发及维护成本[2]，但同时也产生了数据泄露、个人隐私信息无法得到有效保护等安全问题。此外，为了确保数据的机密性，数据拥有者在上传数据至云端服务器前会对其进行加密，导致数据使用者难以在加密文件中快速查找信息。

为解决上述问题，研究人员提出可搜索加密(Searchable Encryption，SE)技术[3-5]。可搜索加密体制分为对称可搜索加密体制和公钥可搜索加密体制[3]。文献[4]提出对称可搜索加密方案，随后文献[6]提出公钥关键字搜索加密(Public Key Encryption with Keyword Search，PEKS)概念，并结

基金项目：国家自然科学基金(61562077，61662069，61662071，61772022)；甘肃省杰出青年基金(1308RJDA007)；西北师范大学青年教师科研能力提升计划项目(NWNU-LKQN-14-7)。

作者简介：牛淑芬(1976—)，女，副教授、博士，主研方向为大数据网络隐私保护、云计算；杨平平、谢亚亚，硕士研究生；王彩芬、杜小妮，教授、博士。

收稿日期：2019-08-05 **修回日期：**2019-10-11 **E-mail：**sfniu76@nwnu.edu.cn

合公钥加密技术设计出基于双线性对的构造方案。该方案以邮件路由为应用场景以便邮件服务器对邮件进行分发,数据发送者从待发送的电子邮件中通过检索关键字与使用数据接收者公钥对关键字和电子邮件进行加密,数据接收者生成陷门并向邮件存储服务器发送相应陷门,邮件存储服务器搜索与其匹配的关键字密文,并将包含关键字的邮件密文返回给数据接收者[3]。

在加密的电子邮件系统中,带关键字搜索的公钥加密方案是在不解密情况下搜索加密邮件的有效手段,但是其存在安全问题。文献[7]指出 PEKS 方案和结合域关键字搜索的公钥加密(Public Key Encryption with Conjunctive Field Keyword Search,PECKS)方案[8]中存在离线关键字猜测攻击(Keyword Guessing Attack,KGA)风险。恶意敌手能在离线状态下采用穷举法搜索候选关键字[9],并分别对其进行验证。研究人员通过实验发现,该攻击具有可行性。如果邮件服务器变得恶意,其可以通过离线启动 KGA 从用户邮件中恢复信息[10]。文献[11]研究了基于身份的关键字搜索加密(Identity Based Encryption with Keyword Search,IBEKS)方案,并对 IBEKS 方案进行定义。该文献指出,数据发送者使用基于身份的加密(Identity-Based Encryption,IBE)方法对电子邮件进行加密,并使用 IBEKS 方案加密关键字,然后将加密的电子邮件和关键字上传到邮件存储服务器[12-13],数据接收者为检索包含某个关键字的电子邮件,委托邮件服务器提供陷门搜索加密的关键字,邮件服务器将与加密关键字关联的电子邮件返回给数据接收者作为搜索结果。但是由于 IBEKS 方案无法抵抗内部离线关键字猜测攻击[14],同时还隐藏了外部敌手搜索模式,因此文献[15]提出一种指定服务器的基于身份关键字搜索加密(designated Server Identity-Based Encryption with Keyword Search,dIBEKS)方案,然而文献[16]指出该方案不能满足关键字密文的不可区分性。

为提高 dIBEKS 方案的安全性,本文提出一种指定邮件服务器的基于身份认证关键字搜索加密(designated Server Identity-Based Authenticated Encryption with Keyword Search,dIBAEKS)方案。在未知数据发送者私钥的情况下,攻击者难以伪造数据发送者加密的关键字,从而无法进行离线关键字猜测攻击,对该方案适应性选择消息攻击的关键字密文不可区分性、陷门不可区分性和离线猜测攻击的安全性进行验证。

1 基础知识

1.1 双线性对

令(G_1, +)和(G_2, ×)为 2 个阶均为大素数 q 的循环群,p 是群 G_1 的生成元。

定义 1(双线性对[17])循环群上线性映射 e: $G_1 \times G_1 \rightarrow G_2$ 具有以下性质:

1)双线性。对任意 $P, Q \in G_1$ 和 $a, b \in \mathbb{Z}_q^*$, $e(aP, bP) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab}$。

2)非退化性。存在 $P, Q \in G_1$,满足 $e(P, Q) \neq 1$。

3)可计算性。对于任意 $P, Q \in G_1$,存在 1 个有效算法计算 $e(P, Q)$。

1.2 困难性问题假设

本文方案采用双线性 Diffie-Hellman 计算(Computational Bilinear Diffie-Hellman,CBDH)假设[18]。

定义 2(CBDH 假设)给定三元组$(P, aP, bP) \in G_1$,其中 $a, b \in \mathbb{Z}_q^*$ 未知,任意的多项式时间攻击者 R 根据(P, aP, bP)计算出 $e(P, P)^{ab}$的概率优势如下:

$$\mathrm{Adv}_{\mathrm{CBDH}}(\mathrm{R}) = \Pr[\mathrm{R}(P, aP, bP) = e(P, P)^{ab}] \tag{1}$$

其中,$e(P, P)^{ab}$的概率优势可以忽略。

2 系统模型和安全模型

2.1 系统模型

图 1 为 dIBAEKS 方案的电子邮件系统模型。该模型主要包括数据发送者 A、数据接收者 B、指定邮件服务器 S[19]以及可信任的密钥生成中心(Private Key Generator,PKG)4 个实体。其中:数据发送者 A 对数据文件进行加密,使用其私钥 $\mathrm{sk_A}$ 为加密的数据文件生成关键字索引 C_w,并将数据密文与关键字索引 C_w 共同上传到指定邮件服务器 S;数据接收者 B 用其私钥 $\mathrm{sk_B}$ 生成陷门 T_w,并将陷门 T_w 发送给指定邮件服务器 S 进行搜索服务请求;指定邮件服务器 S 为加密的电子邮件提供存储服务并利用其私钥 $\mathrm{sk_S}$ 完成数据接收者 B 的搜索请求;可信任的密钥生成中心 PKG 主要负责生成主密钥 s 和系统公共参数 Params,并根据用户身份信息生成用户密钥。

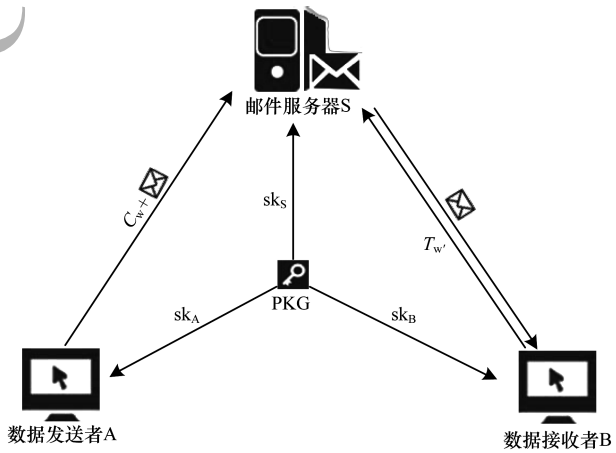

图 1 dIBAEKS 方案的电子邮件系统模型

Fig. 1 Email system model of dIBAEKS scheme

dIBAEKS 方案由以下 5 个概率多项式时间算法组成:

1)系统建立算法 Setup(λ):给定 1 个安全参数 λ,产生 PKG 的主密钥 s 和系统公共参数 Params。

2)密钥生成算法 KeyGen(Params,s,ID_A,ID_B,ID_S):输入系统公共参数 Params、主密钥 s 和身份信息(ID_A、ID_B、ID_S),PKG 生成各身份对应的密钥(pk_A,sk_A)、(pk_B,sk_B)和(pk_S,sk_S)。

3)关键字加密算法 dIBAEKS(Params,w,sk_A,ID_B,ID_S):对于关键字 w,数据发送者结合数据接收者的身份信息 ID_B 和指定邮件服务器的身份信息 ID_S,计算生成密文 C_w。

4)陷门生成函数 dTrapdoor(Params,w',ID_A,ID_S,sk_B):对于给定搜索的关键字 w',数据接收者使用自身私钥sk_B、数据发送者身份信息 ID_A 以及指定邮件存储服务器身份信息 ID_S,生成相对应的搜索陷门 $T_{w'}$,然后数据接收者将 $T_{w'}$ 发送给指定邮件服务器进行搜索请求。

5)验证算法 dTest(Params,sk_S,C_w,$T_{w'}$):指定邮件服务器利用自身私钥sk_S,与接收的 C_w 和 $T_{w'}$ 进行验证,如果验证通过,则输出“True”并返回给数据接收者 C_w 所对应的加密邮件;否则,输出“False”。

2.2　安全模型

dIBAEKS 方案的安全性由关键字密文不可区分性、陷门不可区分性以及抗离线关键字猜测攻击构成。

2.2.1　关键字密文不可区分性

以敌手 A_1 和挑战者 F 的交互游戏 1 来定义 dIBAEKS 方案的关键字密文不可区分性。假设敌手 A_1 是外部攻击者。

1)系统初始化。挑战者 F 执行 Setup 算法产生系统参数并发送给敌手 A_1。

2)询问 1。外部攻击者 A_1 向挑战者 F 进行以下询问:

(1)密钥询问。当敌手 A_1 向挑战者 F 进行密钥询问时,挑战者 F 调用 KeyGen 算法并返回数据接收者私钥sk_B 和指定邮件服务器私钥sk_S 给敌手 A_1。

(2)陷门询问。敌手 A_1 将数据发送者身份信息ID_A、数据接收者身份信息ID_B 和关键字 w 发送给挑战者 F,挑战者 F 调用 dTrapdoor 算法返回给敌手 A_1 搜索陷门 T_w。

(3)测试询问。敌手 A_1 将生成的密文 C^*、指定邮件存储服务器的身份信息ID_S^*、数据接收者身份信息ID_B^* 以及搜索陷门 T_w^* 发送给挑战者 F。挑战者 F 调用 dTest 算法,返回“True”或“False”给敌手 A_1。

3)挑战。当询问阶段 1 结束,敌手 A_1 选择 2 个搜索关键字(w_0、w_1)和数据接收者身份信息ID_B^* 发送给挑战者 F。挑战者 F 随机选择猜测值 $b\in\{0,1\}$ 并调用 dIBAEKS 算法计算密文 C^* = dIBAEKS(w_b,ID_S^*,ID_B^*,sk_A^*),然后将密文 C^* 发送给敌手 A_1。

4)询问 2。敌手 A_1 向挑战者 F 进行密钥询问,除不能对指定邮件服务器身份信息ID_S 进行公钥询问和测试询问以外,其他与询问阶段 1 一致。

5)猜测。敌手 A_1 输出猜测值 $b'\in\{0,1\}$,如果 $b'=b$,则挑战成功,敌手 A_1 赢得游戏 1 的胜利。

定义游戏1中敌手A_1赢得游戏的优势$Adv_{A_1}(\lambda)=\left|\Pr(b=b')-\frac{1}{2}\right|$。

2.2.2　陷门不可区分性

以敌手 A_2 和挑战者 F 的交互游戏 2 来定义 dIBAEKS 方案的陷门不可区分性。假设敌手 A_2 是外部攻击者。

1)系统初始化。挑战者 F 执行 Setup 算法产生系统参数并发送给敌手 A_2。

2)询问 1。外部攻击者 A_2 向挑战者 F 进行以下询问:

(1)密钥询问。当敌手 A_2 向挑战者 F 进行密钥询问时,挑战者 F 调用 KeyGen 算法并返回数据接收者的私钥sk_B 和指定邮件存储服务器私钥sk_S 给敌手 A_2。

(2)陷门询问。敌手 A_2 将数据发送者身份信息ID_A、数据接收者身份信息ID_B 和关键字 w 发送给挑战者 F,并对其进行陷门询问。挑战者 F 调用 dTrapdoor 算法返回给敌手 A_2 搜索陷门 T_w。

(3)测试询问。敌手 A_2 将生成的密文 C^*、指定邮件存储服务器的身份信息ID_S^*、数据接收者的身份信息ID_B^* 以及陷门 T_w^* 发送给挑战者 F。挑战者 F 调用 dTest 算法,返回“True”或“False”给敌手 A_2。

3)挑战。当询问阶段 1 结束,敌手 A_2 选择 2 个搜索关键字(w_0、w_1)、数据发送者身份信息ID_A^* 和数据接收者身份信息ID_B^* 发送给挑战者 F。挑战者 F 随机选择猜测值 $b\in\{0,1\}$ 并调用 dTrapdoor 算法计算 T_w^* = dTrapdoor(w_b,ID_A^*,ID_S^*,sk_B^*),然后将密文 T_w^* 发送给敌手 A_2。

4)询问 2。敌手 A_2 向挑战者 F 进行密钥询问,除不能对指定邮件服务器身份信息ID_S、接收者的身份信息ID_B 进行公钥询问和测试询问以外,其他与询问阶段 1 一致。

5)猜测。敌手 A_2 输出猜测值 $b'\in\{0,1\}$,如果 $b'=b$,则挑战成功,敌手 A_2 赢得游戏 2 的胜利。

定义游戏2中敌手A_2,赢得游戏的优势$Adv_{A_2}(\lambda)=\left|\Pr(b=b')-\frac{1}{2}\right|$。

2.2.3　离线猜测关键字攻击

由于本文提出的 dIBAEKS 方案在满足适应性选择消息下的陷门不可区分性时,可抵御离线关键字猜测攻击[15],因此 dIBAEKS 方案能够抵御离线关键字猜测攻击。

3　具体方案

dIBAEKS 方案具体算法如下:

1)Setup 算法。设 G_1 和 G_2 分别是 2 个阶为素数 q 的循环群,p 是 G_1 的 1 个生成元,$e:G_1\times G_1\rightarrow G_2$ 是 1 个双线性映射。密钥生成中心 PKG 随机选取主密钥 $s\in\mathbb{Z}_q^*$,计算出 $P_{pub}=sp$,然后选择 2 个哈希

函数 $H_1:\{0,1\}^*\rightarrow G_1$ 和 $H_2:G_2\times\{0,1\}^*\rightarrow\mathbb{Z}_q^*$，最后 PKG 公布系统参数 Params = $\{G_1,G_2,e,q,p,P_{\text{pub}},H_1,H_2\}$。

2）KeyGen 算法。以主密钥 s 和指定邮件服务器 S 的身份信息 $\text{ID}_S\in\{0,1\}^*$ 为输入，PKG 生成指定邮件服务器 S 的私钥 $\text{sk}_S=sH_1(\text{ID}_S)$，其中 $H_1(\text{ID}_S)$ 为指定邮件服务器 S 的公钥。类似地，PKG 根据数据发送者 A 身份信息 $\text{ID}_A\in\{0,1\}^*$ 和数据接收者 B 身份信息 $\text{ID}_B\in\{0,1\}^*$，生成数据发送者 A 的私钥 $\text{sk}_A=sH_1(\text{ID}_A)$ 和数据接收者 B 的私钥 $\text{sk}_B=sH_1(\text{ID}_B)$，其中，$H_1(\text{ID}_A)$ 和 $H_1(\text{ID}_B)$ 分别为数据发送者 A 和数据接收者 B 的公钥。

3）dIBAEKS 算法。数据发送者 A 随机选取 $r\in\mathbb{Z}_q^*$，计算 $\alpha_1=e(\text{sk}_A,H_1(\text{ID}_B))$，将关键字 w 与 α_1 进行哈希运算，得到 $q_1=H_2(w,\alpha_1)$，并计算 $C_1=r\cdot q_1$、$C_2=e(rH_1(\text{ID}_S),q_1\cdot P_{\text{pub}})$。数据发送者 A 将生成的邮件密文与关键字密文 C_1、C_2 一起上传到指定邮件存储服务器 S。

4）dTrapdoor 算法。对于要检索的关键字 w'，数据接收者 B 随机选取 $t\in\mathbb{Z}_q^*$，计算陷门 $T_1=tp$，$\alpha_2=e(\text{sk}_B,H_1(\text{ID}_A))$，$q_2=H_2(w',\alpha_2)$，陷门 $T_2=q_2p$，陷门 $T_3=e((t+q_2)P_{\text{pub}},H_1(\text{ID}_S))$。数据接收者 B 将 T_1、T_2 和 T_3 发送给指定邮件服务器 S 完成搜索请求。

5）dTest 算法。指定邮件服务器 S 利用自身私钥 sk_S，与接收的 C_1、C_2、T_1、T_2、T_3 进行验证，判断 $C_2\cdot T_3$ 是否与 $e(C_1+T_1+T_2,\text{sk}_S)$ 相等。若两者相等则输出“True”，并将 C_w 所对应的加密邮件发送给数据接收者 B，否则输出“False”。

4 正确性、安全性证明与效率分析

4.1 正确性证明

本文方案的正确性证明如下：

$$\begin{aligned}C_2T_3&=e(rH_1(\text{ID}_S),q_1\cdot P_{\text{pub}})e((t+q_2)P_{\text{pub}},H_1(\text{ID}_S))=\\&e(rH_1(\text{ID}_S),q_1\cdot sp)e((t+q_2)sp,H_1(\text{ID}_S))=\\&e(rpq_1,sH_1(\text{ID}_S))e((t+q_2)p,sH_1(\text{ID}_S))=\\&e(rpq_1+(t+q_2)p,sH_1(\text{ID}_S))=\\&e(rpq_1+tp+q_2p,sH_1(\text{ID}_S))=\\&e(C_1+T_1+T_2,\text{sk}_S)\end{aligned}\tag{2}$$

由于 $C_2T_3=e(C_1+T_1+T_2,\text{sk}_S)$ 等式成立，符合关键字 w' 等于 w 以及对数据接收者身份的验证，因此证明了本文提出方案的正确性。

4.2 安全性证明

本节证明 dIBAEKS 方案能满足在随机预言模型适应性选择消息攻击下的关键字密文不可区分性和陷门不可区分性，进而证明该方案可抵御离线关键字猜测攻击[11,16]。

4.2.1 关键字密文不可区分性的具体证明

定理 1 在计算双线性 Diffie-Hellman 是困难问题的情况下，对于游戏 1 的攻击者，dIBAEKS 方案在随机预言模型下满足适应性选择关键字密文攻击时的不可区分性安全。

证明 假设存在敌手 A_1 能够以不可忽略的概率优势对关键字密文进行区分，此时挑战者 F 获得 CBDH 实例 (P,aP,bP)，其中 $a,b\in\mathbb{Z}_q^*$。挑战者 F 通过与敌手 A_1 按照游戏 1 的定义进行交互，最后输出 $e(p,p)^{ab}$。

1）系统初始化。挑战者 F 通过运行 Setup 算法产生系统参数 Params = $\{G_1,G_2,e,q,p,P_{\text{pub}},H_1,H_2\}$ 并发送给敌手 A_1，设 $P_{\text{pub}}=ap$。

2）询问 1。敌手 A_1 向挑战者 F 进行以下询问：

（1）H_1 询问。为应答敌手 A_1 针对邮件服务器 S、数据发送者 A、数据接收者 B 这 3 个实体的 H_1 询问，挑战者 F 需建立 3 个列表 $L_{H_1}^{\text{S}}$、$L_{H_1}^{\text{A}}$、$L_{H_1}^{\text{B}}$，且上述列表初始状态为空。

当敌手 A_1 对邮件服务器 ID_{S_i} 进行 H_1 询问时，挑战者 F 查询 ID_{S_i} 是否在列表 $L_{H_1}^{\text{S}}$ 中，若存在，则返回 $H_1(\text{ID}_{S_i})=\text{pk}_{S_i}$；若不存在，则挑战者 F 随机产生 $\text{coin}\in\{0,1\}$，且 coin 以概率 $\Pr(\text{coin}=0)=\delta$ 分布产生。如果 coin = 0，则挑战者 F 随机选择 $v_i\in\mathbb{Z}_q^*$ 并计算 $\text{pk}_{S_i}=v_ip$；否则 $\text{pk}_{S_i}=bp$。挑战者 F 在列表 $L_{H_1}^{\text{S}}$ 中保存四元组 $(\text{ID}_{S_i},\text{pk}_{S_i},v_i,\text{coin})$ 并将 pk_{S_i} 返回给敌手 A_1。

当敌手 A_1 对数据发送者身份信息 ID_{A_i} 进行 H_1 询问时，挑战者 F 需查看 ID_{A_i} 是否存在于列表 $L_{H_1}^{\text{A}}$ 中，如果存在，则返回 $H_1(\text{ID}_{A_i})=\text{pk}_{A_i}$，否则挑战者 F 随机选择 $x_i\in\mathbb{Z}_q^*$ 并计算 $\text{pk}_{A_i}=x_ip$。挑战者 F 在列表 $L_{H_1}^{\text{A}}$ 中保存三元组 $(\text{ID}_{A_i},\text{pk}_{A_i},x_i)$，同时将 pk_{A_i} 返回给敌手 A_1。与此类似，挑战者 F 在列表 $L_{H_1}^{\text{B}}$ 中保存三元组 $(\text{ID}_{B_i},\text{pk}_{B_i},u_i)$，并将 pk_{B_i} 返回给敌手 A_1。

（2）H_2 询问。为应答敌手 A_1 针对的 H_2 询问，挑战者 F 需要建立列表 L_{H_2}，且列表初始状态为空。当敌手 A_1 对 (w_i,α_i) 进行 H_2 询问时，挑战者 F 查看 (w_i,α_i) 是否存在于列表 L_{H_2} 中，如果存在，则返回 $H_2(w_i,\alpha_i)=Y_i$，否则挑战者 F 随机选择 $Y_i\in\mathbb{Z}_q^*$，且 $Y_i=H_2(w_i,\alpha_i)$。挑战者 F 在列表 L_{H_2} 中保存三元组 (w_i,α_i,Y_i)，并将 Y_i 返回给敌手 A_1。

（3）密钥询问。敌手 A_1 向挑战者 F 进行 3 个实体的密钥询问。当敌手 A_1 对邮件服务器身份 ID_{S_i} 进行询问时，挑战者 F 查询列表 $L_{H_1}^{\text{S}}$ 中四元 $(\text{ID}_{S_i},\text{pk}_{S_i},v_i,\text{coin})$，如果 coin = 1，则挑战者 F 输出 $\perp$，游戏 1 结束，否则挑战者 F 返回邮件服务器 S 的私钥 $\text{sk}_{S_i}=v_iP_{\text{pub}}$。当敌手 A_1 对数据发送者身份 ID_{A_i} 进行询问时，挑战者 F 查看列表 $L_{H_1}^{\text{A}}$ 中三元组 $(\text{ID}_{A_i},\text{pk}_{A_i},x_i)$，并返回数据发送者 A 的私钥 $\text{sk}_{A_i}=x_iP_{\text{pub}}$。与此类似，挑战者 F 返回数据接收者 B 的私钥 $\text{sk}_{B_i}=u_iP_{\text{pub}}$。

(4)陷门询问。敌手 A_1 向挑战者 F 询问 w_i 的陷门。挑战者 F 随机选择 $t \in \mathbb{Z}_q^*$,计算 $T_1 = tp$ 并调用 H_2 询问得到三元组(w_i,α_i,Y_i),进而计算出 $T_2 = Y_i p$,同时调用公钥询问得到 $H_1(\mathrm{ID_S})$ 的值pk_{S_i}和$T_3 = e((t+Y_i)P_{\mathrm{pub}},\mathrm{pk}_{S_i})$,最后挑战者 F 将 T_1、T_2、T_3 发送给敌手 A_1。

3)挑战。当询问 1 结束后,敌手 A_1 选择 2 个搜索关键字(w_0,w_1) 和数据接收者身份信息ID_B^* 发送给挑战者 F,挑战者 F 随机选择$\mu \in \{0,1\}$和 $r^* \in \mathbb{Z}_q^*$,并进行 H_2 询问得到 $Y^* = H_2(w_\mu,\alpha)$,计算$C_1^* = r^* Y^* p$ 和 $C_2^* = e(r^* bp, Y^* ap)$,最终将关键字密文 C_1^* 和 C_2^* 发送给敌手 A_1。

4)询问 2。敌手 A_1 进行询问,除了不能对ID_S^*、ID_B^* 进行公钥询问以及对四元组$(C_w^*,\mathrm{ID}_S^*,\mathrm{ID}_B^*,T_{w'}^*)$测试询问以外$(w' = \{w_0,w_1\})$,其他同询问与询问 1 一致。

5)猜测。敌手 A_1 输出猜测值 $\mu' \in \{0,1\}$,如果 $\mu' = \mu$,则挑战成功,敌手 A_1 赢得游戏 1 的胜利。

4.2.2　陷门不可区分性的具体证明

定理 2　在计算双线性 Diffie-Hellman 是困难问题的情况下,对于游戏 2 的攻击者,dIBAEKS 方案在随机预言模型下满足适应性选择消息攻击时的陷门不可区分性。

证明　假设存在敌手 A_2 能够以不可忽略的概率优势搜索陷门并进行区分,这时挑战者 F 获得 CDH 实例(P,aP,bP),其中 $a,b \in \mathbb{Z}_q^*$。挑战者 F 通过与敌手 A_2 按照游戏 2 的定义进行交互,最后输出$e(p,p)^{ab}$。

1)系统初始化。挑战者 F 通过运行 Setup 算法产生系统参数 $\mathrm{Params} = \{G_1,G_2,e,q,p,P_{\mathrm{pub}},H_1,H_2\}$并发送给敌手 A_2,设 $P_{\mathrm{pub}} = ap$。

2)询问 1。敌手 A_2 向挑战者 F 进行以下询问:

(1)H_1 询问。为应答敌手 A_2 针对 3 个实体的 H_1 询问,挑战者 F 需建立 3 个列表 $L_{H_1}^{\mathrm{S}}$、$L_{H_1}^{\mathrm{A}}$、$L_{H_1}^{\mathrm{B}}$,上述列表初始状态为空。当敌手 A_2 对邮件服务器ID_{S_i}进行 H_1 询问时,挑战者 F 需要查询ID_{S_i}是否在列表 $L_{H_1}^{\mathrm{S}}$中,若存在,则返回 $H_1(\mathrm{ID}_{S_i}) = \mathrm{pk}_{S_i}$;若不存在,则挑战者 F 随机选择 $v_i \in \mathbb{Z}_q^*$ 并计算$\mathrm{pk}_{S_i} = v_i p$。然后在列表 $L_{H_1}^{\mathrm{S}}$中保存三元组$(\mathrm{ID}_{S_i},\mathrm{pk}_{S_i},v_i)$,并将$\mathrm{pk}_{S_i}$返回给敌手 A_2。与此类似,挑战者 F 在列表 $L_{H_1}^{\mathrm{A}}$中保存三元组$(\mathrm{ID}_{A_i},\mathrm{pk}_{A_i},x_i)$,并将$\mathrm{pk}_{A_i}$返回给敌手 A_2,在列表 $L_{H_1}^{\mathrm{B}}$中保存三元组$(\mathrm{ID}_{B_i},\mathrm{pk}_{B_i},u_i)$,并将$\mathrm{pk}_{B_i}$返回给敌手 A_2。

(2)H_2 询问。具体过程与定理 1 一致。

(3)密钥询问。敌手 A_2 向挑战者 F 进行 3 个实体的密钥询问。当敌手 A_2 对邮件服务器身份ID_{S_i}进行询问时,挑战者 F 查看列表 $L_{H_1}^{\mathrm{S}}$中三元组$(\mathrm{ID}_{S_i},\mathrm{pk}_{S_i},v_i)$,并返回邮件服务器 S 的私钥$\mathrm{sk}_{S_i} = v_i P_{\mathrm{pub}}$。与此类似,挑战者 F 查看列表 $L_{H_1}^{\mathrm{A}}$和 $L_{H_1}^{\mathrm{B}}$并返回数据发送者 A 的私钥$\mathrm{sk}_{A_i} = x_i P_{\mathrm{pub}}$和数据接收者 B 的私钥$\mathrm{sk}_{B_i} = u_i P_{\mathrm{pub}}$。

(4)陷门询问。具体过程与定理 1 一致。

3)挑战。当询问 1 结束后,敌手 A_2 选择 2 个搜索关键字(w_0,w_1) 和数据发送者身份信息ID_A^* 发送给挑战者 F,挑战者 F 随机选择$\mu \in \{0,1\}$和 $t^* \in \mathbb{Z}_q^*$,计算 $T_1 = t^* p$ 并调用 H_2 询问得到 $Y^* = H_2(w_\mu,\alpha)$,从而计算出 $T_2 = Y^* p$ 和 $T_3 = e((t^* + Y^*)ap, bp)$。

4)询问 2。敌手 A_2 进行询问,除了不能对ID_S^*、ID_B^* 进行密钥钥询问以及对四元组$(C_{w'}^*,\mathrm{ID}_S^*,\mathrm{ID}_B^*,T_{w'}^*)$测试询问以外$(w' = \{w_0,w_1\})$,其他与询问 1 一致。

5)猜测。敌手 A_2 输出猜测值 $\mu' \in \{0,1\}$,如果 $\mu' = \mu$,则挑战成功,敌手 A_2 赢得游戏 2 的胜利。

4.3　效率分析

本节通过理论对比和数值实验对 dIBAEKS 方案进行效率分析。

4.3.1　理论对比

将采用 dIBAEKS 方案与 dIBEKS 方案的关键字加密算法、陷门生成算法以及验证算法的计算效率进行对比,并以点乘运算($\mathrm{P_M}$)、双线性运算($\mathrm{P_B}$)和哈希运算($\mathrm{P_H}$)的数量作为评估指标,结果如表 1 所示。可以看出:在关键字加密算法中,dIBAEKS 方案比 dIBEKS 方案少 1 个点乘运算和2 个哈希运算;在陷门生成算法中,dIBAEKS 方案比 dIBEKS 方案多 1 个双线性运算和 1 个哈希运算;在验证算法中,dIBAEKS 方案比 dIBEKS 方案少3 个双线性运算和 2 个哈希运算。由上述可知,在关键字加密算法和验证算法中,dIBAEKS 方案的计算效率均优于 dIBEKS 方案,因此从总体来看,dIBAEKS 方案的计算效率更高。

表 1　不同算法下 2 种方案的计算效率对比

Table 1　Comparison of calculation efficiency of two schemes under different algorithms

算法	dIBEKS 方案	dIBAEKS 方案
关键字加密算法	$5\mathrm{P_M} + 2\mathrm{P_B} + 5\mathrm{P_H}$	$4\mathrm{P_M} + 2\mathrm{P_B} + 3\mathrm{P_H}$
陷门生成算法	$3\mathrm{P_M} + \mathrm{P_B} + 2\mathrm{P_H}$	$3\mathrm{P_M} + 2\mathrm{P_B} + 3\mathrm{P_H}$
验证算法	$\mathrm{P_M} + 4\mathrm{P_B} + 2\mathrm{P_H}$	$\mathrm{P_M} + \mathrm{P_B}$

4.3.2　数值实验分析

本文采用数值实验对 dIBAEKS 方案与 dIBEKS 方案在关键字加密和验证阶段的计算效率进行对比分析。实验环境如下:ASUS A455L 型计算机,Inter® Core™ i5-4210U 处理器,4 GB 内存,Win10 操作系统,Linux 虚拟机。使用 C 语言基于配对的密码学(Pairing-Based Cryptography,PBC)库[20],群 G_1、G_2 的长度为 1 024 bit,利用 A 型椭圆曲线 $y^2 = x^3 + x \bmod q$ 进行计算,且用户身份和关键字随机产生,实验参数设置如表 2 所示。

表 2 数值实验参数设置

Table 2 Parameter setting of numerical experiment

参数	参数设置
基域大小/bit	512
离散对数安全/bit	1 024
A 型椭圆曲线次数	2

关键字数量决定 dIBAEKS 方案的执行时间。在数值实验中,关键字数量分别取 100、200、300、400、500、600、700、800、900 和 1 000,取 50 次运算结果的平均值作为最终实验结果。图 2 和图 3 分别为 2 种方案在关键字加密和验证阶段的执行时间随关键字数量的变化情况。由图 2 和图 3 可以看出,随着当关键字数量的增加,dIBAEKS 方案与 dIBEKS 方案的执行时间均延长;在关键字加密阶段,dIBAEKS 方案的执行时间增幅略低于 dIBEKS 方案,其计算效率略高;在验证阶段,dIBAEKS 方案和 dIBEKS方案执行时间的增幅分别为 0.9% 和 1.3% ,dIBAEKS 方案的计算效率明显高于 dIBEKS 方案。

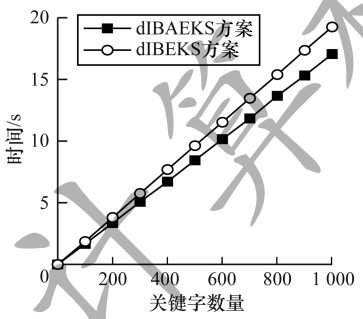

图 2 2 种方案在关键字加密阶段执行时间随关键字数量的变化

Fig. 2 The change of execution time with the number of keywords in the keyword encryption phase of two schemes

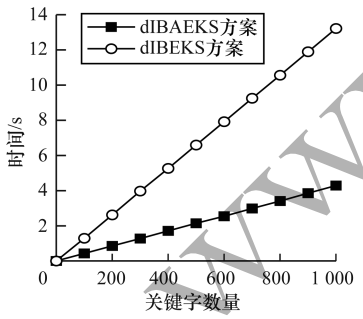

图 3 2 种方案在验证阶段执行时间随关键字数量的变化

Fig. 3 The change of execution time with the number of keywords in the verification phase of two schemes

5 结束语

本文提出一种指定服务器的身份认证邮件关键字加密方案,通过在指定服务器上进行陷门搜索,并由指定数据发送者发出关键字密文,可避免离线关键字猜测攻击。理论分析和数值实验结果表明,该方案具有较高的计算效率和安全性。下一步将在本文工作的基础上,增加数据接收者对返回加密电子邮件的验证,以更准确地分辨服务器返回结果的真实性。

参考文献

[1] CHEN Kang, ZHENG Weimin. Cloud computing: system instances and current research[J]. Journal of Software, 2009, 20(5): 1337-1348. (in Chinese)
陈康,郑纬民. 云计算:系统实例与研究现状[J]. 软件学报, 2009, 20(5): 1337-1348.

[2] SHEN Zhirong, XUE Wei, SHU Jiwu. Survey on the research and development of searchable encryption schemes[J]. Journal of Software, 2014, 25(4): 880-895. (in Chinese)
沈志荣,薛巍,舒继武. 可搜索加密机制研究与进展[J]. 软件学报, 2014, 25(4): 880-895.

[3] QIN Zhiguang, XU Jun, NIE Xuyun, et al. A survey of public-key encryption with keyword search[J]. Journal of Cyber Security, 2017, 2(3): 1-12. (in Chinese)
秦志光,徐骏,聂旭云,等. 公钥可搜索加密体制综述[J]. 信息安全学报, 2017, 2(3): 1-12.

[4] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//Proceedings of 2000 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2000: 212-220.

[5] LI Ying, MA Chunguang. Overview of searchable encryption research[J]. Chinese Journal of Network and Information Security, 2018, 4(7): 13-21. (in Chinese)
李颖,马春光. 可搜索加密研究进展综述[J]. 网络与信息安全学报, 2018, 4(7): 13-21.

[6] BONEH D, CRESCENZO D G, OSTROVSKY R, et al. Public key encryption with keyword search[C]// Proceedings of EUROCRYPT'04. Berlin, Germany: Springer, 2004: 506-522.

[7] BYUN J W, RHEE H S, PARK H A, et al. Off-line keyword guessing attacks on recent keyword search schemes over encry[C]//Proceedings of the 3nd Workshop on Secure Data Management. Berlin, Germany: Springer, 2006: 75-83.

[8] PARK D J, KIM K, LEE P J. Public key encryption with conjunctive field keyword search[C]//Proceedings of International Conference on Information Security Applications. Berlin, Germany: Springer, 2005: 73-86.

[9] WANG Gang, LI Feifei, WANG Yao. Designated server identity-based encryption with conjunctive keyword search scheme[J]. Computer and Modernization, 2017, 33(4): 118-121. (in Chinese)
王刚,李非非,王瑶. 指定服务器的基于身份加密连接关键字搜索方案[J]. 计算机与现代化, 2017, 33(4): 118-121.

[10] WANG Bo. Research on index based searchable encryption technology in cloud environment[D]. Chengdu: University of Electronic Science and Technology of China, 2018. (in Chinese)
王勃. 云环境下基于索引的可搜索加密技术研究[D]. 成都:电子科技大学, 2018.

(下转第 150 页)

(上接第 142 页)

[11] ABDALLA M, BELLARE M, CATALANO D, et al. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions [C]// Proceedings of CRYPTO'05. Berlin, Germany: Springer, 2005:205-222.

[12] ZHU Minhui. Research on identity based proxy searchable encryption scheme [D]. Nanjing: Nanjing University of Posts and Telecommunications,2018. (in Chinese)
朱敏惠. 基于身份的代理可搜索加密方案的研究[D]. 南京:南京邮电大学,2018.

[13] NIU Shufen, CHEN Lixia, LIU Wenke, et al. Proxy reencryption scheme supporting keyword search in email system[J]. Computer Engineering, 2020, 46(6):136-143. (in Chinese)
牛淑芬,陈俐霞,刘文科,等. 电子邮件系统中支持关键字搜索的代理重加密方案[J]. 计算机工程,2020,46(6):136-143.

[14] LI Hongbo, HUANG Qing, SHEN Jian, et al. Designated server identity-based authenticated encryption with keyword search for encrypted emails [J]. Information Sciences, 2019, 481:330-343.

[15] WU T Y, TSAI T T, TSENG Y M. Efficient searchable ID-based encryption with a designated server[J]. Annals of Telecommunications, 2014, 69(7):391-402.

[16] 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. (in Chinese)
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.

[17] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]//Proceedings of CRYPTO'09. Berlin, Germany: Springer, 2009:619-636.

[18] ZHANG Fangguo. From bilinear pairings to multilinear maps[J]. Journal of Cryptologic Research, 2016, 3(3): 211-228. (in Chinese)
张方国. 从双线性对到多线性映射[J]. 密码学报,2016,3(3):211-228.

[19] ZIIU Minhui, CHEN Yanli, HU Yuanyuan. Identity-based searchable encryption scheme supporting proxy re-encryption [J]. Computer Engineering, 2019, 45(1): 129-135, 140. (in Chinese)
朱敏惠,陈燕俐,胡媛媛. 支持代理重加密的基于身份可搜索加密方案[J]. 计算机工程,2019,45(1):129-135,140.

[20] The pairing-based cryptography library [EB/OL]. [2019-06-20]. http://crypto.stanford.edu/pbc/.

编辑 宋 圆