加密邮件系统中基于身份的可搜索加密方案

牛淑芬[①] 谢亚亚[*①] 杨平平[①] 王彩芬[①] 杜小妮[②]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](西北师范大学数学与统计学院 兰州 730070)

摘 要：在加密邮件系统中，公钥可搜索加密技术可以有效地解决在不解密的情况下搜索加密邮件的问题。针对公钥可搜索加密复杂的密钥管理问题，该文在加密邮件系统中引入了基于身份的密码体制。针对可搜索加密的离线关键字猜测攻击问题，该文采用了在加密关键字和生成陷门的同时进行认证，并且指定服务器去搜索加密电子邮件的方法。同时，在随机预言机模型下，基于判定性双线性Diffie-Hellman假设，证明方案满足陷门和密文不可区分性安全。数值实验结果表明，在陷门生成和关键字密文检测阶段，该方案与现有方案相比在计算效率上较高。

关键词：加密邮件系统；可搜索加密；基于身份的密码体制

中图分类号：TN918.7 **文献标识码**：A **文章编号**：1009-5896(2020)07-1803-08

DOI: 10.11999/JEIT190578

Identity-based Searchable Encryption Scheme for Encrypted Email System

NIU Shufen[①] XIE Yaya[①] YANG Pingping[①] WANG Caifen[①] DU Xiaoni[②]

[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[②](*College of Computer Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: In encrypted email system, the public key searchable encryption technology can effectively solve the problem of searching for encrypted emails without decryption. In view of the complex key management problem of public key searchable encryption, an identity-based cryptosystem is introduced in the encrypted mail system. For the offline keyword guessing attack problem of searchable encryption, the method of encrypting keywords and generating trapdoors are adopted at the same time, and the server is designated to search for encrypted emails. At the same time, under the random oracle model, based on the decisional bilinear Diffie-Hellman assumption, the scheme is proved to satisfy the trapdoor and ciphertext indistinguishable security. The numerical experiments show that the scheme has higher computational efficiency than the existing schemes in the keyword trapdoor generation and keyword ciphertext test phase.

Key words: Encrypted emails system; Searchable encryption; Identity-based cryptosystem

1 引言

为了削减运营成本，许多公司选择将电子邮件服务外包给云服务提供商。但由于一些商务邮件的高度敏感性，邮件在发送前需要被加密。一般来说，用户拥有大量的电子邮件，在查找所需邮件时传统方法需要将所有电子邮件下载到本地并解密它们，这十分地浪费网络带宽且效率低下。在这种情况下，有效地搜索包含特定关键字的加密电子邮件是一个重要问题。

Boneh等人[1]首次提出的公钥可搜索加密方案(Public key Encryption with Keyword Search, PEKS)，允许用户通过提供与关键字对应的陷门来获取包含特定关键字的电子邮件。而没有包含特定关键字陷门的用户无法获得任何有关电子邮件的信息。PEKS解决了在共享加密数据上搜索的问题，但仍存在一些隐私问题。

Byun等人[2]指出，一些PEKS方案存在离线关键字猜测攻击的风险。因此，若云邮件服务器变得恶意，它可以通过启动离线关键字猜测攻击从用户

收稿日期：2019-07-30；改回日期：2020-03-21；网络出版：2020-04-15

*通信作者： 谢亚亚 2418606113@qq.com

基金项目：国家自然科学基金(61562077, 61662069, 61662071, 61772022)，西北师范大学青年教师科研提升计划(NWNU-LKQN-13-12)

Foundation Items: The National Natural Science Foundation of China (61562077, 61662069, 61662071, 61772022), The Young Teacher's Scientific Research Ability Promotion Program of Northwest Normal University (NWNU-LKQN-13-12)

邮件中恢复个人信息。Huang等人[3]提出了公钥认证的关键字搜索方案，然而该方案有两个缺点：一是外部攻击者一旦攻破云服务器，就能获得用户的搜索模式[4]，攻击者可能从搜索频率中得到有关明文的信息。二是其基于公钥基础设施，面临着复杂的证书管理和高昂的维护成本问题。

为了保护搜索模式不被泄露，Baek等人[5]提出指定一个测试者对加密数据进行搜索。除非拥有搜索者的私钥，否则，即使拥有陷门，也不能对加密数据进行搜索。Rhee等人[6]提出了基于匿名身份加密(Identity Based Encryption, IBE)的指定测试者公钥可搜索加密的两种通用结构。Emura等人[7]提出了另外两种基于匿名IBE的通用结构:基于标签的加密和一次性签名。但这些方案都无法抵抗内部离线关键字猜测攻击。

为了解决复杂的证书管理等问题，Boneh等人[8]提出，在加密的电子邮件系统中使用IBE。用户的身份、电子邮箱地址等[9]，都可以直接作为其公钥。

并且，焦迪[10]提出，在加密的电子邮件系统中使用IBE，用户不需要申请和交换证书，从而大大降低系统的复杂性。在基于身份的加密邮件系统中，用户无需交互证书和公钥，系统即可实现邮件在客户端与邮件服务器之间、邮件服务器之间传递保证安全、邮件在邮件服务器上存储过程安全、鉴别发件人的身份，防止冒充身份而且由于标识密码系统具有密码委托功能，可以方便地实现加密邮件的监管和归档工作[11]。

Tseng等人[12]提出了第1个支持连接关键字的具有基于身份的系统优势的指定测试者的基于身份可搜索加密方案。并在随机预言机模型下[13]，证明了所提方案同时满足密文和陷门不可区分性安全。但该方案并不是完全定义在基于身份密码体系结构下，不能完全满足密文不可区分性，故不能抵抗离线关键字猜测攻击。王少辉等人[14]针对Tseng的方案提出了基于身份密码系统下的指定测试者可搜索加密方案的的定义和安全需求，并设计了一个高效的新方案，证明了密文不可区分性是抵抗离线关键字猜测攻击的充分条件。

本文将PEKS与IBE相结合，利用公钥可搜索加密技术可以有效地解决在不解密的情况下搜索加密邮件的问题；结合IBE密钥管理的优势，实现对加密邮件系统的密钥管理，构造了加密邮件系统中基于身份的可搜索加密方案；邮件发送方和接收方在生成关键字密文和陷门的同时对身份进行认证，以解决离线关键字猜测攻击问题；指定服务器搜索加密邮件，保证了用户搜索模式不被泄露，加强了安全性；最后在随机预言机模型下证明了方案满足密文不可区分性、陷门不可区分性、指定可搜索性安全。理论分析结合数值实验结果表明本文方案在陷门生成和关键字密文检测阶段具有较高的计算效率。

2 基础知识及困难问题假设

2.1 基础知识

定义1 双线性映射[15]：G_1和G_{T}分别是阶为素数p的循环群，P是G_1的生成元。定义一个双线性映射$e:G_1\times G_1\to G_{\mathrm{T}}$，满足如下性质：

双线性：对于任意的$P,Q\in G_1$和满足$e(aP,bQ)=e(P,Q)^{ab}$。

非退化性：$e(P,P)\neq 1$，其中，1是群G_{T}的单位元。

可计算性：对任意$P,Q\in G_1$，存在有效的算法计算$e(P,Q)$。

2.2 困难问题假设

定义2 判定性双线性Diffie - Hellman (Decisional Bilinear Diffie - Hellman, DBDH)问题[16]：给定两个阶为素数p的循环加法群G_1和循环乘法群G_{T}。一个双线性映射$e:G_1\times G_1\to G_{\mathrm{T}}$, P是G_1的生成元，DBDH问题是给定$(P,aP,bP,cP)\in G_1$和$T\in G_{\mathrm{T}}$，判断$T=e(P,P)^{abc}$。

3 形式化定义与安全模型

本节首先介绍方案的系统模型，其次对算法进行形式化定义并给出算法的安全模型。方案的安全性包括密文不可区分性，陷门不可区分性，指定可搜索性。

本文方案的系统模型如图1所示，主要包括云邮件服务器，邮件发送方A，邮件接收方B，密钥生成中心(Private Key Generator, PKG)。其中，A和B的身份的哈希值H(ID)被用作公钥，PKG根据H(ID)为其生成各自的私钥。云邮件服务器存储

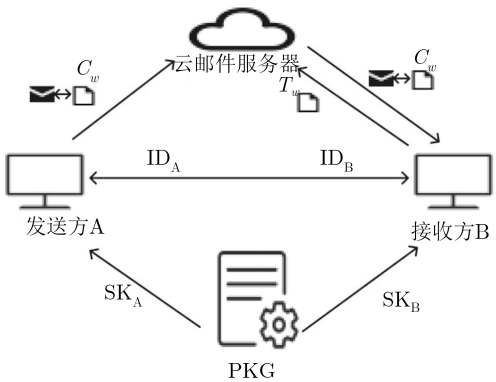

图 1 系统模型

加密邮件和所提取关键字的密文。B向云邮件服务器提交一个包含自己感兴趣关键字w的搜索陷门。然后指定的云邮件服务器去搜索邮件，若B提交的陷门中包含的关键字与A上传的关键字密文中所含关键字相同，则云邮件服务器将加密邮件发送给B, B到本地解密即可。

图1中C_w表示对关键字w进行加密后产生的关键字密文，T_w表示邮件接收方B产生的陷门信息，$\mathrm{ID_A}$和$\mathrm{ID_B}$分别表示邮件发送方A和接收方B的身份，$\mathrm{SK_A}$和$\mathrm{SK_B}$分别表示PKG为邮件发送方A和接收方B分发的密钥。

3.1 算法形式化定义

方案包括6个阶段：系统建立，服务器密钥生成，用户密钥生成，关键字密文生成，陷门生成，关键字密文检测。

系统建立：输入系统参数λ，返回系统公开参数Params和系统主密钥msk。

服务器密钥生成：输入系统公开参数Params，输出服务器的公私钥对$(\mathrm{PK_S}, \mathrm{SK_S})$。

用户密钥生成：输入Params和用户i的身份标识ID_i，输出用户i的私钥$\mathrm{SK}_{\mathrm{ID}_i}$。

关键字密文生成：输入Params，关键字w，服务器的公钥$\mathrm{PK_S}$，发送方的私钥$\mathrm{SK}_{\mathrm{ID_A}}$，发送方的身份$\mathrm{ID_A}$，接收方的身份$\mathrm{ID_B}$，输出关键字密文$C_{w,A,B}$。

陷门生成：输入Params，关键字w，服务器的公钥$\mathrm{PK_S}$，接收方的私钥$\mathrm{SK}_{\mathrm{ID_B}}$，发送方的身份$\mathrm{ID_A}$，接收方的身份$\mathrm{ID_B}$，输出陷门$T_{w,A,B}$。

关键字密文检测：输入Params，服务器的私钥$\mathrm{SK_S}$，发送方的身份$\mathrm{ID_A}$，接收方的身份$\mathrm{ID_B}$，关键字密文$C_{w,A,B}$和陷门$T_{w,A,B}$，输出β，当陷门和关键字密文中包含相同的关键字时$\beta=1$，否则$\beta=0$。

3.2 安全模型

下面，通过攻击者$\mathcal{A}$和挑战者$\mathcal{B}$之间的游戏来定义方案在内部离线关键字猜测攻击下的密文不可区分性，陷门不可区分性，指定可搜索性。

游戏 I (密文不可区分性)：在这个游戏中，半可信的云服务器作为攻击者$\mathcal{A}$。它按照要求完成自己的任务，也尽量获取用户数据的信息。密文的不可区分性是指如果攻击者不知道发送方A和接收方B的密钥，则不能对自己选定的两个挑战搜索关键字生成的密文进行区分。即密文的不可区分性保证了服务器不能在未经用户授权的情况下搜索密文。

初始阶段：挑战者$\mathcal{B}$运行系统建立算法，生成系统参数Params, PKG的密钥对(Params, msk)和服务器的公私钥对$(\mathrm{PK_S}, \mathrm{SK_S})$。并将Params和$(\mathrm{PK_S}, \mathrm{SK_S})$发送给攻击者$\mathcal{A}$。

阶段1：在此阶段攻击者$\mathcal{A}$适应性地进行多项式有界次以下询问：

Extract Oracle：选择用户i的身份ID_i, $\mathcal{B}$运行密钥提取算法将用户(接收方)的私钥$\mathrm{SK}_{\mathrm{ID}_i}$发送给攻击者$\mathcal{A}$。

Trapdoor Oracle：给定一个关键字w，发送方的身份$\mathrm{ID_A}$和接收方的身份$\mathrm{ID_B}$，计算相应的陷门$T_{w,A,B}$并将它返回给攻击者$\mathcal{A}$。

C_wOracle：给定一个关键字w，发送方的身份$\mathrm{ID_A}$和接收方的身份$\mathrm{ID_B}$，计算相应的关键字密文$C_{w,A,B}$ 并将它返回给攻击者$\mathcal{A}$。

挑战：攻击者$\mathcal{A}$将发送方的身份$\mathrm{ID_A^*}$，接收方的身份$\mathrm{ID_B^*}$和两个挑战关键字(w_0^*, w_1^*)发送给挑战者$\mathcal{B}$。$\mathcal{B}$随机地选取一个比特$\beta\in\{0,1\}$，并运行关键字密文生成算法计算出对应的关键字密文$C_{w_\beta^*,A^*,B^*}$，将$C_{w_\beta^*,A^*,B^*}$返回给攻击者$\mathcal{A}$。要求对$(w_0^*, \mathrm{ID_A^*}, \mathrm{ID_B^*})$和$(w_1^*, \mathrm{ID_A^*}, \mathrm{ID_B^*})$没有进行陷门询问和密文询问。

阶段2：$\mathcal{A}$像阶段1一样继续发起一系列询问，要求$\mathrm{ID_A}\neq\mathrm{ID_A^*}$，$\mathrm{ID_B}\neq\mathrm{ID_B^*}$和$w\neq(w_0^*, w_1^*)$。

猜测：最后$\mathcal{A}$输出$\beta'\in\{0,1\}$，若$\beta'=\beta$则$\mathcal{A}$赢得游戏 I 。

定义3　$\mathcal{A}$成功地区分关键字密文的优势被定义为$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{C}}(\lambda)=|\mathrm{pr}[\beta'=\beta]-1/2|$。

若对于任意的概率多项式时间攻击者$\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{C}}(\lambda)$可忽略，则称方案满足密文不可区分性。

游戏 II (陷门不可区分性)：与游戏 I 相似，在这个游戏中半可信的云服务器作为攻击者$\mathcal{A}$。不同在于，若攻击者$\mathcal{A}$不知道接收方和发送方的密钥，陷门的不可区分性是为了阻止攻击者从被给定的陷门中了解关键字的信息。这说明，即使服务器也不能产生关于发送方和接收方的有效密文，也就是无法对选择的挑战关键字生成的搜索陷门进行区分。

初始阶段：与游戏 I 相似。

阶段1：与游戏 I 相似。

挑战：攻击者$\mathcal{A}$将发送方的身份$\mathrm{ID_A^*}$，接收方的身份$\mathrm{ID_B^*}$和两个挑战关键字(w_0^*, w_1^*)发送给挑战者$\mathcal{B}$。$\mathcal{B}$随机地选取一个比特$\beta\in\{0,1\}$，并运行陷门生成算法计算对应的陷门$T_{w_\beta^*,A^*,B^*}$，将$T_{w_\beta^*,A^*,B^*}$返回给$\mathcal{A}$。

阶段2：与游戏 I 相似。

猜测：最后$\mathcal{A}$输出$\beta'\in\{0,1\}$，若$\beta'=\beta$则$\mathcal{A}$赢得游戏 II 。

定义4　$\mathcal{A}$成功地区分陷门的优势被定义为：$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{T}}(\lambda)=|\mathrm{pr}[\beta'=\beta]-1/2|$。

若对于任意的概率多项式时间攻击者$\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{T}}(\lambda)$是可忽略的，则称方案满足陷门不可区分性。

游戏III (指定可搜索性)：在这个游戏中外部攻击者作为攻击者$\mathcal{A}$，能够攻破云得到用户的密文，也可以通过监听用户和云服务器之间的通信信道来获得陷门信息。若$\mathcal{A}$不知道服务器的密钥，则无法进行搜索。指定可搜索性确保只有指定的服务器能够搜索密文。

初始阶段：挑战者$\mathcal{B}$运行系统建立算法，生成系统参数Params, PKG的密钥msk和服务器的密钥对$(\mathrm{PK_S}, \mathrm{SK_S})$，并将Params和$\mathrm{PK_S}$发送给攻击者$\mathcal{A}$。

阶段1：在此阶段攻击者$\mathcal{A}$适应性地进行多项式有界次以下询问：

Extract Oracle：选择用户i的身份ID_i，$\mathcal{B}$运行密钥提取算法将用户的私钥$\mathrm{SK}_{\mathrm{ID}_i}$发送给攻击者$\mathcal{A}$。

挑战：攻击者$\mathcal{A}$将发送方的身份$\mathrm{ID}_{\mathrm{A}}^*$，接收者的身份$\mathrm{ID}_{\mathrm{B}}^*$和两个挑战关键字$(w_0^*, w_1^*)$发送给挑战者$\mathcal{B}$。$\mathcal{B}$随机地选取一个比特$\beta \in \{0,1\}$，并运行关键字密文生成算法计算对应的关键字密文$C_{w_\beta^*, A^*, B^*}$。将$C_{w_\beta^*, A^*, B^*}$返回给$\mathcal{A}$。

阶段2：$\mathcal{A}$像阶段1一样继续发起一系列询问。

猜测：最后$\mathcal{A}$输出$\beta' \in \{0,1\}$，若$\beta' = \beta$则$\mathcal{A}$赢得游戏III。

定义5 $\mathcal{A}$成功地攻破指定可搜索性的优势被定义为$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{D}}(\lambda) = |\mathrm{pr}[\beta' = \beta] - 1/2|$。

若对于任意的概率多项式时间攻击者$\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{D}}(\lambda)$是可忽略的，则称方案满足指定可搜索性。

4 具体方案

本文提出一个基于身份密码体制且能够抵抗离线关键字猜测攻击的方案，方案具体算法由系统建立算法、服务器密钥生成算法、用户密钥生成算法、关键字密文生成算法、陷门生成算法和关键字密文检测算法6部分构成。

系统建立算法(SetUp)：输入安全参数λ。

(1) PKG首先生成双线性映射$e: G_1 \times G_1 \to G_{\mathrm{T}}$，其中$G_1, G_{\mathrm{T}}$是阶为素数$p$的循环群，$g$和$h$是$G_1$的生成元。

(2) PKG随机选择$\alpha \in Z_p$, $\mathrm{msk} = \alpha$作为主密钥，计算$\mathrm{mpk} = g^\alpha$作为系统公钥。PKG选择两个哈希函数$H: G_{\mathrm{T}} \times \{0,1\}^* \to G_1$, $H_1: \{0,1\}^* \to G_1$。

(3) 系统的公开参数为$\mathrm{Params} = \{G_1, G_{\mathrm{T}}, e, p, g, h, H, H_1, \mathrm{mpk}\}$且系统主密钥msk。

服务器密钥生成算法($\mathrm{KGen_s}$)：云服务器S随机选择$t \in Z_p$，服务器私钥$\mathrm{SK_S} = t$，计算并返回服务器的公钥$(\mathrm{PK_{S1}}, \mathrm{PK_{S2}}) = (g^t, h^t)$。

用户密钥生成算法($\mathrm{KGen_U}$)：给定邮件发送方A的身份$\mathrm{ID_A} \in \{0,1\}^*$和邮件接收方B的身份$\mathrm{ID_B} \in \{0,1\}^*$。

(1) 首先计算邮件发送方A的公钥$\mathrm{PK_A} = H_1(\mathrm{ID_A})$，生成并返回其私钥$\mathrm{SK_A} = H_1(\mathrm{ID_A})^\alpha$。

(2) 计算邮件接收方B的公钥$\mathrm{PK_B} = H_1(\mathrm{ID_B})$，生成并返回其私钥$\mathrm{SK_B} = H_1(\mathrm{ID_B})^\alpha$。

关键字密文生成算法(C_w)：给定云邮件服务器S的部分公钥$\mathrm{PK_{S1}}$，邮件接收方B的身份$\mathrm{ID_B}$以及关键字w。

(1) 利用邮件发送方A的私钥$\mathrm{SK_A}$且随机选择$s \in Z_p$，计算得到关键字密文$C_{w,\mathrm{A,B}} = (C_1, C_2, C_3)$。其中，$C_1 = e(H(k,w), (\mathrm{PK_{S1}})^s), C_2 = g^s, C_3 = h^s, k = e(\mathrm{SK_A}, H_1(\mathrm{ID_B}))$；

(2) 邮件发送方A将关键字密文$C_{w,\mathrm{A,B}} = (C_1, C_2, C_3)$发送给云邮件服务器S。

陷门生成算法(Trapdoor)：给定云邮件服务器S的公钥$(\mathrm{PK_{S1}}, \mathrm{PK_{S2}})$，邮件发送方A的身份$\mathrm{ID_A}$，所要搜索邮件包含的关键字$w$。

(1) 利用邮件接收方B的私钥$\mathrm{SK_B}$且随机选择$r \in Z_p$，计算陷门$T_{w,\mathrm{A,B}} = (T_1, T_2)$。$T_1 = H(k,w) \cdot h^r \cdot (\mathrm{PK_{S2}})^r$, $T_2 = g^r \cdot (\mathrm{PK_{S1}})^r$, $k = e(H_1(\mathrm{ID_A}), \mathrm{SK_B})$;

(2) 邮件接收方B将陷门$T_{w,\mathrm{A,B}} = (T_1, T_2)$发送给云邮件服务器。

关键字密文检测(Test)：给定关键字密文$C_{w,\mathrm{A,B}}$和用户陷门$T_{w,\mathrm{A,B}}$。

(1) 首先将关键字密文$C_{w,\mathrm{A,B}}$解析为(C_1, C_2, C_3)，给定的陷门$T_{w,\mathrm{A,B}}$解析为(T_1, T_2);

(2) 云邮件服务器S再利用自身的私钥$\mathrm{SK_S}$，计算判断$C_1 \cdot (T_2^{\mathrm{SK_S}}, C_3) = e(T_1^{\mathrm{SK_S}}, C_2)$是否成立，若成立说明关键字密文和陷门相匹配，则返回1，否则返回0;

(3) 若关键字密文和陷门相匹配，则云邮件服务器S将关键字密文$C_{w,\mathrm{A,B}}$对应的加密云邮件发送给邮件接收方B，邮件接收方B在本地执行解密邮件操作即可。

正确性证明：

$$\begin{aligned} C_1 \cdot (T_2^{\mathrm{SK_S}}, C_3) &= e(H(k,w), g^{t \cdot s}) \cdot e((g^r \cdot g^{t \cdot r})^t, h^s) \\ &= e(H(k,w), g^{t \cdot s}) \cdot e((g^{r+t \cdot r})^t, h^s) \\ &= e(H^t(k,w), g^s) \cdot e(g^s, h^{(r+tr)t}) \\ &= e(g^s, H^t(k,w) \cdot h^{(r+tr)t}) \end{aligned}$$

$$\begin{aligned} e(T_1^{\mathrm{SK_S}}, C_2) &= e((H(k,w) \cdot h^r \cdot (\mathrm{PK_{S2}})^r)^t, g^s) \\ &= e(H^t(k,w) \cdot (h^r \cdot h^{t \cdot r})^t, g^s) \\ &= e(H^t(k,w) \cdot (h^{r+tr})^t, g^s) \end{aligned}$$

从而，$C_1 \cdot (T_2^{\mathrm{SK_S}}, C_3) = e(T_1^{\mathrm{SK_S}}, C_2)$。 证毕

5 安全性分析

下面从密文和陷门不可区分性以及指定可搜索性3个方面具体分析所提方案的安全性。

5.1 方案的密文不可区分性

定理1　若DBDH假设成立，本文所提方案在随机预言机模型下满足密文不可区分性。

证明　假设$\mathcal{A}$是一个试图攻破密文不可区分性的多项式时间攻击者。挑战者$\mathcal{B}$通过建立算法解决DBDH问题，$\mathcal{B}$获得实例$F=(G_1,G_{\mathrm{T}},e,p,g,g^x,g^y,g^z,Z)$。

初始阶段：$\mathcal{B}$从G_1中随机选择$h,t\in Z_p$, $\mathrm{Params}=(G_1,G_{\mathrm{T}},e,p,g,h,\mathrm{mpk}=g^z)$, $(\mathrm{PK_S},\mathrm{SK_S})=((g^t,h^t),t)$, 并返回Params和$(\mathrm{PK_S},\mathrm{SK_S})$。

阶段1：在此阶段$\mathcal{A}$适应性地向由挑战者$\mathcal{B}$模拟的预言机进行如下询问。假设$\mathcal{A}$不会对预言机重复询问，在发起Oracle O_{H_1}之前，在任何的计算中攻击者$\mathcal{A}$都不使用身份ID。否则，返回给$\mathcal{A}$的$H_1(\mathrm{ID})$的值随机的，而$\mathcal{A}$猜对$H_1(\mathrm{ID})$值的概率是可忽略的。

Hash Oracle O_H：给定$k\in G_{\mathrm{T}}$，关键字w，从G_{T}中随机选择一个元素，并返回它作为$H(k,w)$的输出。

Oracle O_{H_1}：维护一个初始为空的列表$L_{H_1}=\{\langle\cdot,\cdot,\cdot\rangle\}$。假设$\mathcal{A}$对$O_{H_1}$最多发起$q_{\mathrm{H}}$次询问。随机选择$i,j\in\{1,2,\cdots,q\}$，猜测$\mathcal{A}$对$O_{H_1}$发起的第$i$次询问和第$j$次询问分别是挑战发送方和接收方的身份$\mathrm{ID}_{\mathrm{A}}^*$, $\mathrm{ID}_{\mathrm{B}}^*$。给定一个身份ID，它根据以下情况返回给$\mathcal{A}$。

若这是第i次询问，若$\mathrm{ID}=\mathrm{ID}_{\mathrm{A}}^*$，返回$H_1(\mathrm{ID})=g^x$，并且向$L_{H_1}$添加$\langle\mathrm{ID},g^x,\perp\rangle$。

若这是第j次询问，若$\mathrm{ID}=\mathrm{ID}_{\mathrm{B}}^*$，返回$H_1(\mathrm{ID})=g^y$，并且向$L_{H_1}$添加$<\mathrm{ID},g^y,\perp>$。

否则，随机选取$v\in Z_p$，返回$H_1(\mathrm{ID})=g^v$，并且向L_{H_1}添加$<\mathrm{ID},g^v,v>$。

Extract Oracle O_E：以ID作为输入，若$\mathrm{ID}=\mathrm{ID}_{\mathrm{A}}^*$或$\mathrm{ID}=\mathrm{ID}_{\mathrm{B}}^*$，输出一个随机比特$\beta'$并且中止。否则，从$L_{H_1}$中查找$<\mathrm{ID},H_1(\mathrm{ID}),v>$。并将密钥$\mathrm{SK_{ID}}=(g^z)^v$返回给$\mathcal{A}$。

Ciphertext Oracle O_C：给定$(w,\mathrm{ID_A},\mathrm{ID_B})$，随机选择$s\in Z_p$，根据以下情况计算密文$C_{w,\mathrm{A,B}}=(C_1,C_2,C_3)$。

若$(\mathrm{ID_A},\mathrm{ID_B})=(\mathrm{ID}_{\mathrm{A}}^*,\mathrm{ID}_{\mathrm{B}}^*)$或$(\mathrm{ID_A},\mathrm{ID_B})=(\mathrm{ID}_{\mathrm{B}}^*,\mathrm{ID}_{\mathrm{A}}^*)$，计算$C_1=e(H(Z,w),(\mathrm{PK_{S1}})^s)$, $C_2=g^s$, $C_3=h^s$。

否则，假设$\mathrm{ID_A}\notin\{\mathrm{ID}_{\mathrm{A}}^*,\mathrm{ID}_{\mathrm{B}}^*\}$，从$L_{H_1}$中查找$<\mathrm{ID_A},H_1(\mathrm{ID_A}),v_{\mathrm{A}}>$，计算$k=e((g^z)^{v_A},H_1(\mathrm{ID}_B))$并且返回$C_1=\mathrm{e}(H(k,w),(\mathrm{PK_{S1}})^s)$, $C_2=g^s$, $C_3=h^s$。

Trapdoor Oracle O_T：给定$(w,\mathrm{ID_A},\mathrm{ID_B})$，随机选择$r\in Z_p$，并根据以下情况计算陷门$T_{w,\mathrm{A,B}}=(T_1,T_2)$。

若$(\mathrm{ID_A},\mathrm{ID_B})=(\mathrm{ID}_{\mathrm{A}}^*,\mathrm{ID}_{\mathrm{B}}^*)$或$(\mathrm{ID_A},\mathrm{ID_B})=(\mathrm{ID}_{\mathrm{B}}^*,\mathrm{ID}_{\mathrm{A}}^*)$，计算$T_1=H(Z,w)\cdot h^r\cdot(\mathrm{PK_{S2}})^r$, $T_2=g^r\cdot(\mathrm{PK_{S1}})^r$。

否则，假设$\mathrm{ID_A}\notin\{\mathrm{ID}_{\mathrm{A}}^*,\mathrm{ID}_{\mathrm{B}}^*\}$，从$L_{H_1}$中查找$<\mathrm{ID_B},H_1(\mathrm{ID_B}),v_{\mathrm{B}}>$，计算$k'=e((g^z)^{v_A},H_1(\mathrm{ID_B}))$并且返回$T_1=\mathrm{H}(k',w)\cdot h^r\cdot(\mathrm{PK_{S2}})^r$, $T_2=g^r\cdot(\mathrm{PK_{S1}})^r$。

挑战：$\mathcal{A}$向$\mathcal{B}$提交两个挑战关键字(w_0^*,w_1^*)，发送方的$\mathrm{ID}_{\mathrm{A}}^*$和接收方的$\mathrm{ID}_{\mathrm{B}}^*$。$\mathcal{B}$随机地选择一个比特$\beta\in\{0,1\}$, $s\in Z_p$，并且返回密文$C_{w_\beta^*,\mathrm{A}^*,\mathrm{B}^*}=(C_1^*,C_2^*,C_3^*)$, $C_1^*=e(H(Z,w),(\mathrm{PK_{S1}})^s)$, $C_2^*=g^s$, $C_3^*=h^s$。

阶段2：与阶段1一样。

猜测：$\mathcal{A}$输出一个比特β'。若$\beta'=\beta$, $\mathcal{B}$输出$\beta'=0$。

若对挑战身份的猜测错误，$\mathcal{B}$中止，用ϖ表示这个事件。若$\mathcal{B}$中止，$\mathcal{B}$输出的随机比特等于β的概率是1/2。$\mathcal{B}$猜对挑战身份的概率是$1/q_{\mathrm{H}}(q_{\mathrm{H}}-1)$，用$\omega$表示这个事件。

假设$\mathcal{B}$不中止，若$Z=e(g,g)^{xyz}$，比如$\beta=0$，$\mathcal{A}$赢得游戏 I 的概率是$\mathrm{Adv}_{\mathcal{A}}^{C}(\lambda)+1/2$。若$Z$是从$G_{\mathrm{T}}$中随机选取，则$k=H(Z,w_\beta)$从$G_1$中随机选取。$\mathcal{A}$和$\mathcal{B}$使用相同的方式产生$C_{w_\beta^*,\mathrm{A}^*,\mathrm{B}^*}$和$T_{w_\beta^*,\mathrm{A}^*,\mathrm{B}^*}$，若有相同的关键字，关键字密文检测算法输出1。故可知$\mathcal{B}$解决DBDH问题的优势是：

$$\begin{aligned}&\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DBDH}}(\lambda)=|\Pr[\beta'=\beta|\omega]\cdot\Pr[\omega]\\&+\Pr[\beta'=\beta|\overline{\omega}]\cdot\Pr[\overline{\omega}]-1/2|\\&=|1/2\cdot(1-\Pr[\overline{\omega}])+(\Pr[\beta'=0|\overline{\omega}\cap\beta=0]\\&\cdot\Pr[\beta=0]+\Pr[\beta'=1|\overline{\omega}\cap\beta=1]\cdot\Pr[\beta=1])\\&\cdot\Pr[\overline{\omega}]-1/2|\geq|1/2\cdot(1-\Pr[\overline{\omega}])\\&+\Pr[\overline{\omega}]\cdot((\mathrm{Adv}_{\mathcal{A}}^{\mathrm{C}}(\lambda)+1/2)1/2+1/2\cdot1/2)-1/2|\\&=1/2\cdot Pr[\overline{\omega}]\cdot\mathrm{Adv}_{\mathcal{A}}^{\mathrm{C}}(\lambda)=1/2\cdot q_{\mathrm{H}}(q_{\mathrm{H}}-1)\cdot\mathrm{Adv}_{\mathcal{A}}^{\mathrm{C}}(\lambda)\end{aligned}$$

若$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{C}}(\lambda)$不可忽略，则$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DBDH}}(\lambda)$也不可忽略，这与DBDH问题的困难性假设矛盾。　　证毕

5.2 方案的陷门不可区分性

定理2　若DBDH假设成立，所提方案在随机预言机模型下满足陷门不可区分性。

证明　此处证明与密文不可区分性的证明相似。但证明陷门不可区分性的时候，$\mathcal{B}$产生挑战陷门。具体的证明省略。

5.3 方案的指定可搜索性

定理3　若DBDH假设成立，所提方案在随机预言机模型下满足指定可搜索性。

证明　假设$\mathcal{A}$是一个试图攻破指定可搜索性的多项式时间攻击者。挑战者$\mathcal{B}$通过建立算法解决DBDH问题，$\mathcal{B}$获得实例$F=(G_1,G_{\mathrm{T}},e,p,g,g^x,g^y,g^z,Z)$。

初始阶段：$\mathcal{B}$随机选择$\alpha,\gamma\in Z_p$，设置$\mathrm{Params}=(G_1,G_{\mathrm{T}},e,p,g,h=g^\gamma,\mathrm{mpk}=g^\alpha)$, $\mathrm{PK_{S1}}=g^x$并返回Params和$\mathrm{PK_{S1}}$。

阶段1：假设$\mathcal{A}$不重复地进行询问，$\mathcal{B}$如下对$\mathcal{A}$的询问进行回答。

哈希询问H：$\mathcal{B}$维护一个初始为空的列表$L_H=\{<\cdot,\cdot,\cdot>\}$。给定$k\in G_{\mathrm{T}}$和一个关键字$w$, $\mathcal{B}$随机选择$v_{k,w}\in Z_p$，返回$H(k,w)=g^{y}\cdot g^{v_{k,w}}$，并将$<(k,w),H(k,w),v_{k,w}>$添加到$L_H$中。

哈希询问H_1：给定ID，$\mathcal{B}$随机从G_1中选择一个元素作为$H_1(\mathrm{ID})$的输出，将其返回给A。

Extract Oracle O_E：给定ID, $\mathcal{B}$返回$\mathrm{SK_{ID}}=H_1(\mathrm{ID})^{\alpha}$。

挑战：$\mathcal{A}$向$\mathcal{B}$提交两个挑战关键字(w_0^*,w_1^*)，发送方的$\mathrm{ID_A^*}$和接收方的$\mathrm{ID_B^*}$。$\mathcal{B}$随机地选择一个比特$\beta\in\{0,1\}$，并从L_H中查找$<(k^*,w_\beta^*),H(k^*,w_\beta^*),v_{k^*,w_\beta^*}>$，其中$k^*=e(H_1(\mathrm{ID_A^*}),H_1(\mathrm{ID_B^*}))^{\alpha}$。若不存在这样的元组，$\mathcal{B}$像回答$\mathcal{A}$的哈希询问$H$一样生成该元组。然后返回挑战密文$C_{w_\beta^*,\mathrm{A}^*,\mathrm{B}^*}=(C_1^*,C_2^*,C_3^*)$，且$C_1^*=Z\cdot e(g^z,g^x)^{v_{k,w_\beta^*}}$, $C_2^*=g^z$, $C_3^*=(\mathrm{g}^z)^r=h^z$。

阶段2：与阶段1一样。

猜测：$\mathcal{A}$输出一个比特β'。若$\beta'=\beta$, $\mathcal{B}$输出$\beta'=0$。

若$Z=e(g,g)^{xyz}$，计算可得$C_1^*=e(H(k,w_\beta^*),\mathrm{PK_{S1}})^z$，$\mathcal{A}$赢得游戏III的概率是$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{D}}(\lambda)$。

若Z是随机选取的，则C_1^*也是随机的。故可知挑战者$\mathcal{B}$解决DBDH问题的优势是：

$$\begin{aligned}\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DBDH}}(\lambda)=&|\Pr[\beta'=1|\beta=1]\cdot\Pr[\beta=1]\\&+\Pr[\beta'=0|\beta=0]\cdot\Pr[\beta=0]-1/2|\\=&|1/2\cdot1/2+1/2\cdot\mathrm{Adv}_{\mathcal{A}}^{\mathrm{D}}(\lambda)-1/2|\\=&|1/2\cdot\mathrm{Adv}_{\mathcal{A}}^{\mathrm{D}}(\lambda)|\end{aligned}$$

若$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{D}}(\lambda)$不可忽略，则$\mathrm{Adv}_{\mathcal{B}}^{\mathrm{DBDH}}(\lambda)$也不可忽略，这与DBDH问题的困难性假设矛盾。 证毕

6 效率分析

6.1 理论分析与比较

(1) 计算量比较：在表1中，T_{p}表示配对运算的时间，T_{e}表示指数运算的时间，T_{m}表示乘法运算的时间，T_{h}表示哈希运算的时间。由表1可以看出，常用密码操作配对时间的排序为$T_{\mathrm{p}}>T_{\mathrm{e}}>T_{\mathrm{m}}>T_{\mathrm{h}}$，且配对运算的时间$T_{\mathrm{p}}$远大于其他密码操作的时间。

在表2中，C_w表示关键字密文生成算法，Trapdoor表示陷门生成算法，Test表示关键字密文检测算法，主要比较的运算包括双线性对运算，哈希运算，乘法运算，指数运算。

由表2可以看出，在关键字密文生成阶段，各方案计算量由大到小依次为文献[14]、本文方案、文献[3]；在陷门生成阶段，各方案计算量由大到小依次为文献[3]、文献[14]、本文方案；在关键字密文检测阶段，各方案计算量由大到小依次为文献[14]、文献[3]、本文方案，且本文方案与文献[3]方案计算量几乎一样。

(2) 通信量比较：在表3中，$\mathrm{SK_{ID}}$表示系统中不同身份的私钥，C_w表示关键字密文生成算法，Trapdoor表示陷门生成算法，分别用$|G_1|$, $|G_2|$, $|G_{\mathrm{T}}|$和$|Z_{\mathrm{p}}|$表示G_1, G_2, G_{T}和Z_{p}中元素的长度。用$|h|$统一表示不同方案中抗碰撞哈希函数的长度。

由表3可以看出，在密钥生成阶段，各方案通信量几乎相同；在关键字密文生成阶段，各方案通信量由大到小依次为文献[14]、本文方案、文献[3]，且本文方案与文献[3]的通信量几乎相同；在陷门生成阶段，各方案通信量由大到小依次为文献[14]、本文方案、文献[3]，且本文方案与文献[3]的通信量几乎一样。

6.2 数值分析与比较

笔者在Linux操作系统下利用双线性对包(pairing - based cryptography library)[17]，用C语言编程，在2.9 GHz CPU, 4 GB RAM PC机上运行[15]。表4说明双线性对包参数Type - A的性质。实验结果如图2(a)、图2(b)和图2(c)所示。

图2(a)表示各方案关键字密文生成算法的运行时间与关键字数量的关系。横轴表示加密关键字的数量，纵轴表示加密关键字所需的时间。由表2可知，文献[14]的方案中有3个对运算，文献[3]的方案中没有对运算，本文方案中有2个对运算。由表1

表 1 常用密码操作的计算时间[17]

操作	T_{p}	T_{e}	T_{m}	T_{h}
时间(ms)	16.064	1.882	0.013	0.006

表 2 计算量比较

方案	C_w	Trapdoor	Test
文献[14]方案	$3T_{\mathrm{p}}+2T_{\mathrm{h}}+6T_{\mathrm{m}}$	$T_{\mathrm{p}}+T_{\mathrm{h}}+4T_{\mathrm{m}}$	$3T_{\mathrm{p}}+2T_{\mathrm{h}}+2T_{\mathrm{m}}+T_{\mathrm{e}}$
文献[3]方案	$T_{\mathrm{h}}+T_{\mathrm{m}}+3T_{\mathrm{e}}$	$T_{\mathrm{p}}+T_{\mathrm{h}}+T_{\mathrm{e}}$	$2T_{\mathrm{p}}+T_{\mathrm{m}}+2T_{\mathrm{e}}$
本文方案	$2T_{\mathrm{p}}+T_{\mathrm{h}}+3T_{\mathrm{e}}$	$T_{\mathrm{h}}+3T_{\mathrm{m}}+4T_{\mathrm{e}}$	$2T_{\mathrm{p}}+T_{\mathrm{m}}+2T_{\mathrm{e}}$

表 3 通信量比较

方案	$\mathrm{SK_{ID}}$	C_w	Trapdoor
文献[14]方案	$\|G_1\|$	$3\|G_1\|+\|Z_{\mathrm{P}}\|$	$2\|G_1\|+\|Z_{\mathrm{P}}\|$
文献[3]方案	$\|Z_{\mathrm{P}}\|$	$2\|G_1\|+\|h\|$	$\|G_{\mathrm{T}}\|+\|h\|$
本文方案	$\|G_1\|$	$2\|G_1\|+\|G_{\mathrm{T}}\|$	$2\|G_1\|$

表 4 对参数的主要性质

参数类型	基域(bit)	Dlog安全(bit)	椭圆曲线次数
Type - A	512	1024	2

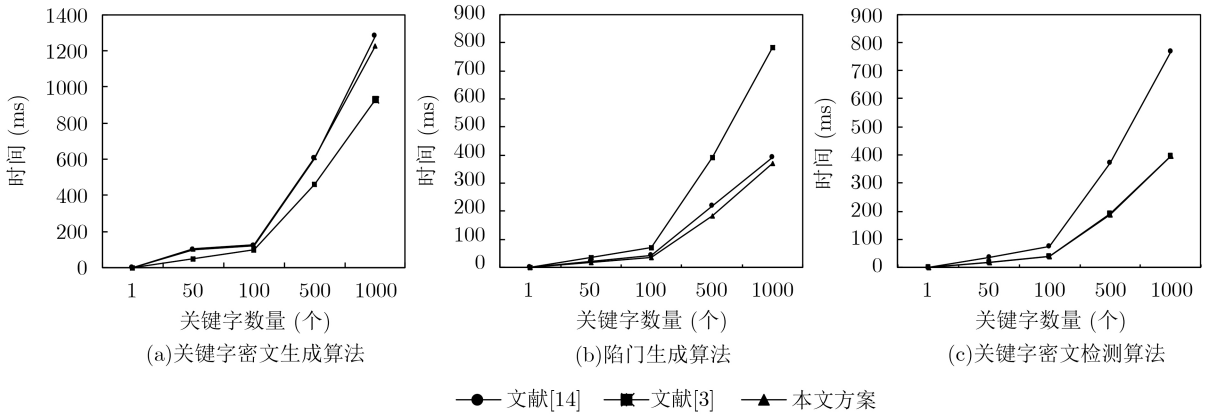

图 2 算法运行时间比较

可知，对运算的计算量远远大于其他运算的计算量，故本文方案的计算量小于文献[14]的方案且大于文献[3]方案。同样由图2(a)可以看出，本文方案在关键字密文生成阶段，计算效率高于文献[14]但低于文献[3]，但本文的方案完全满足密文不可区分性，陷门不可区分性和指定的可搜索安全性，具有较高的安全性。

图2(b)表示各方案陷门生成算法运行时间与关键字数量的关系。由表2可知，文献[14]和文献[3]的方案中，都有1个对运算，本文方案中并未出现对运算。虽然本文出现了指数运算，但由表1可知，对运算的计算量远远大于其他运算的计算量，故本文方案的计算量小于文献[14]和文献[3]方案的计算量。同样由图2(b)可以看出，本文方案的计算效率高于文献[14]和文献[3]。即可以得出结论，本文方案在陷门生成阶段具有较高的计算效率。

图2(c)表示各方案关键字密文检测算法运行时间与关键字数量的关系。由表2可知，文献[14]的方案中有3个对运算，本文方案和文献[3]的方案均有2个对运算、2个指数运算和1个乘法运算。由表1可知，对运算的计算量远远大于其他运算的计算量，故本文方案的计算量小于文献[14]且与文献[3]方案的计算量几乎一样。在图2(c)可以看出，本文方案在关键字密文检测阶段计算效率高于文献[14]，并且与文献[3]几乎一样。即可得出结论，本文方案在关键字密文检测阶段具有较高的计算效率。

7　结束语

本文将PEKS与IBE相结合，利用公钥可搜索加密技术可以有效地解决在不解密的情况下搜索加密邮件的问题，结合IBE密钥管理的优势，实现对加密邮件系统的密钥管理，构造了加密邮件系统中基于身份的可搜索加密方案。基于DBDH假设，在随机预言机模型下证明所提方案满足密文、陷门不可区分性和指定可搜索性安全，故可以加强用户的邮件信息安全性。理论分析结合数值实验结果表明本文方案在陷门生成阶段和关键字密文检测阶段具有较高的计算效率。在本文方案中，由于密文和陷门都与发送方和接收方的身份绑定在一起，这在实际的电子邮件系统应用场景中缺少灵活性。在未来的工作中，考虑去构造一个更为灵活的方案。

参 考 文 献

[1] 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, Switzerland, 2004: 506–522. doi: 10.1007/978-3-540-24676-3_30.

[2] 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 Secure Data Management, Seoul, Korea, 2006: 75–83. doi: 10.1007/11844662_6.

[3] 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.

[4] 陆海宁. 可隐藏搜索模式的对称可搜索加密方案[J]. 信息网络安全, 2017(1): 38–42. doi: 10.3969/j.issn.1671-1122.2017.01.006.
LU Haining. Searchable symmetric encryption with hidden search pattern[J]. *Netinfo Security*, 2017(1): 38–42. doi: 10.3969/j.issn.1671-1122.2017.01.006.

[5] 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, Italy, 2008: 1249–1259. doi: 10.1007/978-3-540-69839-5_96.

[6] RHEE H S, PARK J H, and LEE D H. Generic construction of designated tester public-key encryption with keyword search[J]. *Information Sciences*, 2012, 205: 93–109.

doi: 10.1016/j.ins.2012.03.020.

[7] SUZUKI T, EMURA K, and OHIGASHI T. A generic construction of integrated secure-channel free PEKS and PKE and its application to EMRs in cloud storage[J]. *Journal of Medical Systems*, 2019, 43(5): 128. doi: 10.1007/s10916-019-1244-2.

[8] BONEH D and FRANKLIN M. Identity-based encryption from the Weil pairing[C]. The 21st Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2001: 213–229. doi: 10.1007/3-540-44647-8_13.

[9] 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(4): 118–121. doi: 10.3969/j.issn.1006-2475.2017.04.024.

WANG Gang, LI Feifei, and WANG Yao. Designated server identity-based encryption with conjunctive keyword search scheme[J]. *Computer and Modernization*, 2017(4): 118–121. doi: 10.3969/j.issn.1006-2475.2017.04.024.

[10] 焦迪. 关于安全电子邮箱的标识密码技术研究与应用[J]. 网络安全技术与应用, 2019(2): 19–21. doi: 10.3969/j.issn.1009-6833.2019.02.014.

JIAO Di. Research and application of identification password technology for secure E-mail[J]. *Network Security Technology and Application*, 2019(2): 19–21. doi: 10.3969/j.issn.1009-6833.2019.02.014.

[11] 龙毅宏, 黄强, 王维. 电子邮件IBE加密研究[J]. 软件, 2018, 39(2): 1–6. doi: 10.3969/j.issn.1003-6970.2018.02.001.

LONG Yihong, HUANG Qiang, and WANG Wei. Study on IBE for email[J]. *Computer Engineering & Software*, 2018, 39(2): 1–6. doi: 10.3969/j.issn.1003-6970.2018.02.001.

[12] 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): 391–402. doi: 10.1007/s12243-013-0398-z.

[13] CANETTI R, GOLDREICH O, and HALEVI S. The random oracle methodology, revisited[J]. *Journal of the ACM*, 2004, 51(4): 557–594. doi: 10.1145/1008731.1008734.

[14] 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.

[15] 牛淑芬, 牛灵, 王彩芬, 等. 一种可证安全的异构聚合签密方案[J]. 电子与信息学报, 2017, 39(5): 1213–1218. doi: 10.11999/JEIT160829.

NIU Shufen, NIU Ling, WANG Caifen, *et al*. A provable aggregate signcryption for heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1213–1218. doi: 10.11999/JEIT160829.

[16] BOYEN X. The uber-assumption family: A unified complexity framework for bilinear groups[C]. The 2nd International Conference on Pairing-Based Cryptography, London, UK, 2008: 258–263. doi: 10.1007/978-3-540-85538-5_3.

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

牛淑芬：女，1976年生，博士，副教授，研究方向为云计算和大数据网络的隐私保护.

谢亚亚：女，1996 年生，硕士，研究方向为网络与信息安全.

杨平平：女，1995 年生，硕士，研究方向为网络与信息安全.

王彩芬：女，1963 年生，博士，教授，研究方向为网络安全.

杜小妮：女，1972 年生，博士，教授，研究方向为流密码.

责任编辑：马秀强