计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170431
54(10):2369-2377, 2017

适合移动云存储的基于属性的关键词搜索加密方案

苏 航 朱智强 孙 磊
(解放军信息工程大学 郑州 450000)
(Suhang_039@163.com)

Attribute-Based Encryption with Keyword Search in Mobile Cloud Storage

Su Hang, Zhu Zhiqiang, and Sun Lei
(*PLA Information Engineering University*, *Zhengzhou* 450000)

Abstract In recent years, with the further improvement of mobile devices' performance and the rapid development of mobile Internet, more and more mobile terminals participate in cloud data storage and data sharing. In order to support mobile devices with constrained resource effectively in terms of sharing data safely and efficiently in the cloud, a secure and efficient attribute-based encryption scheme with keyword search (ABKS) is proposed in this paper. The proposed scheme is based on the AND gate access structure with wildcards, which is proven to be IND-CKA (indistinguishable against chosen keyword attack) secure and achieves keyword security under the standard model. The scheme adopts the Viète's formulas to make each attribute only be represented by one element, and the length of index is constant, the length of trapdoor and secret key and the computation complexity of trapdoor algorithm and search algorithm grow linearly with the maximum number of wildcards that can be used in the access structure, in addition, the scheme removes the secure channel, which reduces the communication overhead further during the transmission process of index and trapdoor. Efficiency analysis shows that compared with other schemes, the proposed scheme has less computation overhead and communication overhead, which is more suitable for mobile cloud storage environment.

Key words mobile cloud storage; searchable encryption; attribute-based encryption (ABE); secure-channel free; Viète's formulas

摘 要 近年来,随着移动设备性能的不断提升和移动互联网的迅猛发展,越来越多的移动终端参与云端数据存储与共享.为了更好地解决资源受限的移动设备参与云端数据共享的安全和效率问题,基于支持通配符的与门访问结构,提出了一种高效的基于属性的关键词搜索加密方案,并证明了其在标准模型下满足选择关键词明文攻击的不可区分安全性和关键词安全性.该方案采用韦达定理使得每个属性仅需用一个元素表示,方案中索引长度固定,陷门和密钥的长度及陷门算法和搜索算法的计算复杂度与访问结构中可使用的通配符数量上限成正比,同时,移除了索引和陷门传输过程中的安全信道,进一步降低了开销.效率分析表明:与其他方案相比,该方案的计算开销和通信开销较小,更加适用于移动云存储环境.

关键词 移动云存储;可搜索加密;属性基加密;移除安全信道;韦达定理

中图法分类号 TP390

收稿日期:2017-06-12;**修回日期**:2017-07-27

基金项目:国家重点研发计划项目(2016YFB0501900)

This work was supported by the National Key Research and Development Program of China (2016YFB0501900).

便捷的移动终端已成为人们生活中不可或缺的一部分,移动用户可通过移动游戏、移动支付等移动应用获取多种服务.由于移动终端在存储空间、通信带宽及电池容量等多方面存在限制,移动应用提供的服务质量难以获得显著提升.为更好地支持日益复杂的移动应用并提升用户体验,云计算被引入到移动环境中[1].移动云计算作为一种将移动终端上复杂的数据存储和处理操作置于云端的应用模式,可较好地解决移动终端资源受限的问题.

移动云存储作为一种移动云计算的核心应用,具有容量可扩展、成本费用低、便于统一管理等诸多优势,受到越来越多用户的青睐.通过移动云存储,用户可高效便捷地在云端存储和共享数据,包含个人隐私等信息的敏感数据往往也会存储到云端,但数据上传云端后,其实际物理控制权交由第三方云服务提供商.为防止云中存储的敏感数据被云服务提供商或其他恶意用户窃取,数据拥有者通常会在上传敏感数据前对其进行加密处理.传统的加密方式可保护数据的安全性,但是无法对数据实施灵活的访问控制.Sahai 和 Waters[2] 提出的属性基加密(attribute-based encryption, ABE)方案可较好地同时解决数据安全性和数据访问控制问题.在 ABE 方案中,密文和密钥分别与一组属性相关联,加密者基于接收者的属性特征制定相应的访问策略,当且仅当解密者的属性集合满足访问策略时可完成解密,ABE 方案可有效实现一对多应用场景下细粒度的非交互访问控制.

当数据以密文形式存储在云端后,云服务提供商不能有效地为用户提供数据检索服务[3],极大降低了云端数据的取用效率.Dan 等人[4] 提出了公钥关键词搜索加密(public key encryption with keyword search, PEKS)方案可实现密文数据检索,但该方案仅支持一对一应用场景,不适用于云存储环境.为了对云端数据实施细粒度的访问控制并提供高效的密文检索服务,Sun 等人[5]、Zheng 等人[6]、Qiu 等人[7] 结合 ABE 方案和 PEKS 方案,提出了多种基于属性的关键词搜索(attribute-based encryption with keyword search, ABKS)方案.

现有的 ABKS 方案效率较低,对计算能力和通信带宽有限的移动设备的影响尤为明显,不能较好地适用于移动云存储环境.主要表现在 2 个方面:1)在 ABE 方案中,随着属性数量增多,加解密算法计算复杂度和密文长度随之线性增长,这就造成 ABKS 方案中索引和陷门算法计算复杂度以及索引和陷门长度随属性数量线性增长;2)在 ABKS 方案中,为保证方案的安全性,搜索服务器和用户之间需要通过安全信道传输索引、陷门和搜索结果,而使用安全信道也将加重移动用户端的计算和通信开销.

针对 ABE 方案效率受属性数量增加影响的问题,2007 年 Cheung 等人[8] 基于支持通配符的与门访问结构,提出首个在标准模型下可证明安全的 ABE 方案,该方案具有较低的计算复杂度.Emura 等人[9]、Zhang 等人[10] 和肖思煜等人[11] 提出基于与门访问结构的 ABE 方案,上述方案中的密文长度与解密算法中双线性对运算量恒定,但不支持通配符,导致访问策略的数量呈指数增长,且要求解密者属性与访问策略完全匹配,方案灵活性较差.Nishide 等人[12] 和 Lai 等人[13] 的方案支持通配符,但方案中单个属性需要用若干个元素表示,效率较低.Phuong 等人[14] 的方案支持通配符,该方案采用韦达定理使得各属性只需用单个元素表示,此外方案还具有密文定长,解密算法中双线性对运算量固定的优势.Phuong 等人[14] 方案是选择安全的,为提高方案安全性,Jin 等人[15] 对文献[14]中的方案进行改进,基于合数群提出一种完全安全的 ABE 方案.

Baek 等人[16] 首次指出安全信道问题,他们指出在 PEKS 方案中,陷门和搜索结果易遭受恶意攻击,为保证其安全,需要在搜索服务器和用户之间建立安全信道.为移除安全信道,他们提出一种指定测试者的 PEKS 方案(PEKS with a designated tester, dPEKS),通过使用指定搜索服务器的公钥加密陷门和索引从而移除了安全信道.Rhee 等人[17] 考虑到来自恶意服务器和恶意接收者的攻击,增强了 Baek 等人[16] 方案的安全模型,并提出一种在随机预言机模型下可证明安全的 dPEKS 方案.Fang 等人[18] 给出选择密文攻击安全、选择关键词攻击安全并且可抵抗关键词攻击的安全模型,基于上述模型提出在标准模型下可证明安全的 dPEKS 方案.林鹏等人[19] 提出一种通过指定搜索服务器从而移除安全信道的 ABKS 方案.

本文构造了一种适用于移动云环境的 ABKS 方案,其主要优势体现在 4 个方面:

1) 方案采用支持通配符的与门访问结构,受到 Phuong 等人[14] 方案的启发,使用不同属性出现的“位置”匹配访问策略与用户属性,并基于韦达定理实现解密过程中通配符的移除.传统方案为支持通配符需要用多个元素表示一个属性,而本方案一个属性只需要用一个元素表示,效率更高.

2) 无需建立用户列表. 在 Sun[5] 与 Qiu[7] 的方案中,数据拥有者需要建立一个合法数据使用者列表,当系统中加入新用户时数据拥有者需要更新该列表,即要求数据拥有实时在线. 本文采用不同的索引生成方式,无需建立用户列表.

3) 移除安全信道. 授权机构为用户选择相对可信的搜索服务器,搜索过程中使用该搜索服务器的公钥加密索引或陷门,即使恶意用户截获索引或陷门也无法从中获取关键词信息,移除了索引和陷门传输过程中的所需的安全信道,减轻了用户的通信开销.

4) 计算与通信开销低. 方案中索引和陷门算法的计算复杂度较小,索引长度固定,陷门长度较短,降低了用户在搜索过程中的计算开销和通信开销.

1　预备知识

1.1　双线性映射及复杂性假设

定义 1. 非对称双线性映射. 令 G_1,G_2,G_T 表示阶为素数 p 的乘法循环群,若 $e:G_1\times G_2\rightarrow G_T$ 为有效的双线性映射,则其满足性质:

1) 双线性. $\forall g\in G_1,h\in G_2,a,b\in\mathbb{Z}_p,e(g^a,h^b)=e(g^b,h^a)=e(g,h)^{ab}$.

2) 非退化性. $\forall g\in G_1,h\in G_2,e(g,h)\neq 1$.

3) 可计算性. $\forall g\in G_1,h\in G_2$,存在多项式时间算法计算 $e(g,h)$.

若 $G_1\neq G_2$,该映射为非对称双线性映射.

定义 2. DLIN(decisional linear)假设. 令 G_1, G_2 表示阶为素数 p 的乘法循环群,$e:G_1\times G_2\rightarrow G_T$ 为有效的双线性映射,g_1,g_2 分别为群 G_1,G_2 的生成元,给定元组 $y_{\mathrm{DLIN}}=(g_1,g_1^a,g_1^b,g_1^{ac},g_1^d,g_2,g_2^a,g_2^b,g_2^{ac},g_2^d,Z)$,其中 $a,b,c,d\in\mathbb{Z}_p,Z\in G_2$. 在多项式时间内判定 $Z=g_2^{b(c+d)}$ 是否成立是困难的.

定义 3. DDDH(divisible decision Diffie-Hellman)假设. 令 G 表示阶为素数 p 的乘法循环群,g 为群 G 的生成元,给定元组 $y_{\mathrm{DDDH}}=(g,g^a,g^b,Z)$,其中 a, $b\in\mathbb{Z}_p,Z\in G$. 在多项式时间内判定 $Z=g^{\frac{a}{b}}$ 是否成立是困难的.

1.2　访问结构

定义 4. 支持通配符的与门访问结构. 系统属性集合为 $U=\{Att_1,Att_2,\cdots,Att_L\}$,其中属性 Att_i 的属性值为 A_i. 系统中用户的属性集合为 $S=\{S_1,S_2,\cdots,S_L\}$,S_i 的取值有 2 种,即"+"和"−". 访问结构为 $W=\{W_1,W_2,\cdots,W_L\}$,W_i 的取值有"+","−"和"*"3 种,其中"*"表示通配符,当属性取值为"*"时表示访问结构对此属性不做要求. $S\models W$ 表示属性集合 S 满足访问结构 W.

1.3　韦达定理[15]

向量 $\boldsymbol{A}=(v_1,v_2,\cdots,v_L)$,$\boldsymbol{B}=(z_1,z_2,\cdots,z_L)$,$\boldsymbol{A}$ 中包含字符和通配符,$\boldsymbol{B}$ 中仅包含字符. 向量 $\boldsymbol{A}$ 中通配符的数量为 n,集合 $J=\{j_1,j_2,\cdots,j_n\}$ 表示通配符在 $\boldsymbol{A}$ 中出现的位置.

命题 $\forall i\in[1,L],v_1=z_i\vee v_i=*$,可表述为

$$\sum_{i=1,i\notin J}^{L}v_i\prod_{j\in J}(i-j)=\sum_{i=1}^{L}z_i\prod_{j\in J}(i-j).\tag{1}$$

展开 $\prod_{j\in J}(i-j)$ 可得:

$$\prod_{j\in J}(i-j)=\sum_{m=0}^{n}\lambda_m i^m,\tag{2}$$

其中,λ_m 为与集合 J 相关的系数. 可通过韦达定理构造 $\lambda_m:\lambda_{n-m}=(-1)^m\sum_{1\leqslant i_1<i_2<\cdots<i_m\leqslant n}j_{i_1}j_{i_2}\cdots j_{i_m}$, $0\leqslant m\leqslant n$.

将式(2)代入式(1)中可得:

$$\sum_{i=1,i\notin J}^{L}v_i\prod_{j\in J}(i-j)=\sum_{m=0}^{n}\lambda_m\sum_{i=1}^{L}z_i i^m.\tag{3}$$

引入随机群元素 H_i 隐藏式(3)中的运算,可得:

$$\prod_{i=1,i\notin J}^{L}H_i^{v_i\prod_{j\in J}(i-j)}=\prod_{m=0}^{n}\left(\prod_{i=1}^{L}H_i^{z_i i^m}\right)^{\lambda_m}.\tag{4}$$

2　算法定义及安全模型

2.1　系统模型

系统中包含 4 类实体,即授权机构(authorized authority, AA)、搜索服务器(search server, SS)、数据拥有者(data owner, DO)和数据使用者(data user, DU),系统结构如图 1 所示:

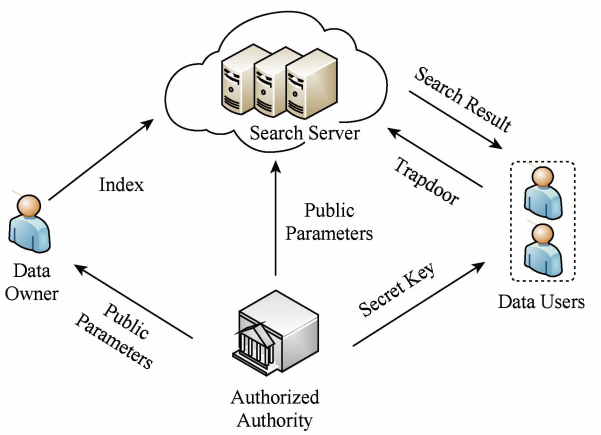

Fig. 1　System model

图 1　系统模型

1) 授权机构

授权机构是系统中唯一的可信第三方,负责系统建立和密钥生成工作.

2) 搜索服务器

搜索服务器是"诚实但具有好奇心的",为用户提供关键词搜索服务.

3) 数据拥有者

从授权机构处获取公开参数后,数据拥有者为敏感数据选取关键词,对该关键词加密生成索引并上传至云端.

4) 数据使用者

从授权机构获取密钥后,通过生成搜索陷门,数据使用者可从搜索服务器处获取关键词搜索服务.

2.2 算法定义

定义 5. 本文提出的方案包括 6 个算法,定义为

$Setup(1^{\lambda})\rightarrow(PP,MSK)$ 系统建立算法由授权机构运行.算法输入为安全参数,输出为系统公开参数 PP 以及系统主密钥 MSK.

$SSKeyGen(PP)\rightarrow(SK_S,PK_S)$ 搜索服务器密钥生成算法由授权机构运行.算法输入为系统公开参数 PP,输出为搜索服务器公私钥对 (SK_S,PK_S).

$KeyGen(PP,MSK,S)\rightarrow SK$ 密钥生成算法由授权机构运行.算法输入为系统公开参数 PP、系统主密钥 MSK 以及用户属性集 S,输出为用户密钥 SK.

$EncIndex(PP,KW,W,PK_S)\rightarrow IX$ 索引算法由数据所有者运行.算法输入为系统公开参数 PP、数据拥有者为数据选取的关键词 KW、为索引制定的访问结构 W 以及搜索服务器公钥 PK_S,算法输出为索引 IX.

$GenTrapdoor(PP,SK,SKW)\rightarrow TR$ 陷门算法由数据使用者运行.算法输入为系统公开参数 PP、数据使用者的密钥 SK 和待搜索关键词 SKW,算法输出为陷门 TR.

$Search(IX,TR,SK_S)\rightarrow SR$ 搜索算法由搜索服务器运行.算法输入为索引 IX、陷门 TR 及搜索服务器私钥 SK_S,算法输出为搜索结果 SR.

2.3 安全模型

定义 6. 选择关键词攻击安全游戏[6].为保证索引不会泄漏数据拥有者为云端存储数据选取的关键词信息,方案需要达到选择关键词明文攻击的不可区分性安全(IND-CKA).攻击者和挑战者之间在选择模型下的攻击游戏定义如下:

初始化:敌手选取待挑战的访问结构 W^*.

系统建立:挑战者运行系统建立算法,将系统公开参数 PP 交给敌手.

阶段 1:敌手发起多项式次数的密钥查询.敌手向挑战者提交待查询的属性集合 S,若 S 不满足 W^*,挑战者运行密钥生成算法,将该属性集合对应的密钥 SK 交给敌手;否则,挑战者不响应此次查询.

挑战:敌手向挑战者提交关键词 KW_0,KW_1.挑战者随机选取 $rand\in\{0,1\}$,运行索引算法,将索引 $IX_{KW_{rand}}$ 交给敌手.

阶段 2:阶段 2 与阶段 1 相同,敌手不能查询满足访问结构 W^* 的属性集合 S 对应的密钥.

猜测:敌手输出对 $rand$ 的猜测 $rand'$.

若对所有多项式时间敌手 $\mathcal{A}$,在游戏中的优势 $Adv_{\mathcal{A}}^{\text{IND-CKA}}(k)=|Pr[rand'=rand]-\frac{1}{2}|$ 是可忽略的,则方案是选择关键词攻击安全的.

定义 7. 关键词安全性游戏[6].为保证数据使用者生成的陷门不会泄漏其搜索的关键词信息,方案需要保证陷门中关键词的安全性.攻击者和挑战者之间在选择模型下的攻击游戏定义如下:

系统建立:挑战者运行系统建立算法,将系统公开参数 PP 交给敌手.

阶段 1:敌手发起多项式次数的密钥和陷门查询.

$\mathcal{O}_{KeyGen}$ 敌手向挑战者提交待查询的属性集合 S,挑战者运行密钥生成算法,将该属性集合对应的密钥 SK 交给敌手.

$\mathcal{O}_{Trapdoor}$ 敌手向挑战者提交待查询的属性集合 S 和待查询关键词,挑战者运行密钥生成算法与陷门生成算法,将相应的陷门 TR 交给敌手.

挑战:敌手向挑战者提交待挑战的属性集合 S^* 及关键词 KW_1^*,KW_2^*,阶段 1 中敌手未查询 S^* 对应的密钥及陷门.挑战者选取随机数 $rand\in\{0,1\}$,运行密钥生成算法与陷门生成算法生成陷门 $TR_{KW_{rand}^*}$,将该陷门交给敌手.

阶段 2:阶段 2 与阶段 1 相同,敌手不能查询属性集合 S^* 对应的密钥及陷门.

猜测:敌手输出对 $rand$ 的猜测 $rand'$.

若对所有多项式时间敌手 $\mathcal{A}$,在游戏中的优势 $Adv_{\mathcal{A}}^{\text{IND-KGA}}(k)=|Pr[rand'=rand]-\frac{1}{2}|$ 是可忽略的,则方案满足关键词安全性.

3 方案设计

3.1 ABKS 方案

本节提出一种高效的基于属性的关键词搜索加密方案,具体设计如下:

$Setup(1^{\lambda})\rightarrow(PP,MSK)$.

系统属性集合为 U,定义访问结构中通配符的最大数量为 N_1,正属性的最大数量为 N_2,负属性的最大数量为 N_3.输入安全参数后,授权机构按照下列步骤执行系统建立算法:

1) 选取阶为素数 p 的乘法循环群 G_1,G_2,G_T,存在双线性映射 $e:G_1\times G_2\rightarrow G_T$,生成元 $g_1\in G_1$,$g_2\in G_2$.

2) 随机选取 $\alpha,\beta,\gamma\in\mathbb{Z}_p$,计算 $y=g_1^{\alpha}$,$y'=g_1^{-\alpha}$,$f_1=g_1^{\beta}$,$f_2=g_1^{\gamma}$,$f_1'=g_2^{\beta}$,$f_2'=g_2^{\gamma}$.

3) 对属性集合中的所有属性,随机选取 $\forall_{i\in U}a_i\in\mathbb{Z}_p$,计算 $A_{i,1}=g_1^{a_i}$,$A_{i,2}=g_2^{a_i}$.

4) 选取密码学散列函数:$H:\{0,1\}^*\rightarrow\mathbb{Z}_p$.

5) 授权机构公布系统公开参数为 $PP=\{G_1,G_2,G_T,e,g_1,g_2,f_1',f_2',\{A_{i,2}\}_{i=1}^{u},H\}$,并秘密保存系统主密钥 $MSK=\{y,y',f_1,f_2,\{A_{i,1}\}_{i=1}^{u}\}$.

$SSKeyGen(PP)\rightarrow(SK_S,PK_S)$.

搜索服务器选取 $b\in\mathbb{Z}_p$,其私钥为 $SK_S=b$,计算 $PK_{S,1}=g_1^b$,$PK_{S,2}=g_2^b$,公钥 $PK_S=\{PK_{S,1},PK_{S,2}\}$,秘密保存私钥,并公开其公钥.

$KeyGen(PP,MSK,S)\rightarrow SK$.

授权机构审核用户提交的属性集合 S,若通过审核,授权机构按照下述步骤执行密钥生成算法:

属性集合 S 中包含 n_2' 个正属性和 n_3' 个负属性,其中正属性出现的位置为 $V'=\{v_1',v_2',\cdots,v_{n_2'}'\}$,负属性出现的位置为 $Z'=\{z_1',z_2',\cdots,z_{n_3'}'\}$.随机选取 $k\in\mathbb{Z}_p$,计算:

$$K_1=\{K_{1,m}\}_{m=0}^{N_1}=\{y(f_1\prod_{i\in V'}A_{i,1}^{i^m})^k\}_{m=0}^{N_1},$$

$$K_2=\{K_{2,m}\}_{m=0}^{N_1}=\{y'(f_2\prod_{i\in Z'}A_{i,1}^{i^m})^k\}_{m=0}^{N_1},$$

$$K_3=PK_{S,1}^{k}.$$

通过安全信道将密钥 $SK=\{K_1,K_2,K_3\}$ 发送给用户.

$EncIndex(PP,KW,W,PK_S)\rightarrow IX$.

数据拥有者为敏感数据选定的关键词 KW,为索引制定的访问结构为 W.W 中包含 n_1 个通配符,n_2 个正属性和 n_3 个负属性,其中,通配符出现的位置为 $J=\{w_1,w_2,\cdots,w_{n_1}\}$,正属性出现的位置为 $V=\{v_1,v_2,\cdots,v_{n_2}\}$,负属性出现的位置为 $Z=\{z_1,z_2,\cdots,z_{n_3}\}$.根据通配符位置 $J=\{w_1,w_2,\cdots,w_{n_1}\}$,通过韦达定理计算 1.3 节式(2)中的 $\lambda=\{\lambda_0,\lambda_1,\cdots,\lambda_{n_1}\}$,令 $t_w=\sum_{m=0}^{n_1}\lambda_m$.随机选取 $t_1,t_2\in\mathbb{Z}_p$,计算:

$$IX_1=PK_{S,2}^{\frac{t_1}{H(KW)t_w}},$$

$$IX_2=g_2^{\frac{t_2}{H(KW)t_w}},$$

$$IX_3=(f_1'(\prod_{i\in V}A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{t_1+t_2},$$

$$IX_4=(f_2'(\prod_{i\in Z}A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{t_1+t_2},$$

索引为

$$IX=\{J,IX_1,IX_2,IX_3,IX_4\}.$$

$GenTrapdoor(PP,SK,SKW)\rightarrow TR$.

数据使用者输入密钥 SK 和待搜索关键词 SKW.选取随机数 $s\in\mathbb{Z}_p$,计算 $T_1=K_1^s$,$T_2=K_2^s$,$T_3=K_3^{\frac{s}{H(SKW)}}$.搜索陷门为 $TR=\{T_1,T_2,T_3\}$.

$Search(IX,TR,SK_S)\rightarrow SR$.

搜索服务器根据索引中通配符出现的位置 $J=\{w_1,w_2,\cdots,w_{n_1}\}$,通过韦达定理计算 1.3 节式(2)中的 $\lambda=\{\lambda_0,\lambda_1,\cdots,\lambda_{n_1}\}$,计算:

$$L=e(IX_1,\prod_{m=0}^{n_1}T_{1,m}^{\lambda_m})e(IX_2,\prod_{m=0}^{n_1}T_{1,m}^{SK_S\lambda_m})\times e(IX_1,\prod_{m=0}^{n_1}T_{2,m}^{\lambda_m})e(IX_2,\prod_{m=0}^{n_1}T_{2,m}^{SK_S\lambda_m}),$$

$$R=e(IX_3,T_3)e(IX_4,T_3),$$

测试 $L=R$ 是否成立,若成立,$SR=1$,否则 $SR=0$.

3.2　正确性分析

分别计算等式左侧和右侧,可得:

$$L=e(IX_1,\prod_{m=0}^{n_1}T_{1,m}^{\lambda_m})e(IX_2,\prod_{m=0}^{n_1}T_{1,m}^{SK_S\lambda_m})\times e(IX_1,\prod_{m=0}^{n_1}T_{2,m}^{\lambda_m})e(IX_2,\prod_{m=0}^{n_1}T_{2,m}^{SK_S\lambda_m})=$$

$$e(PK_{S,2}^{\frac{t_1}{H(KW)t_w}},\prod_{m=0}^{n_1}K_{1,m}^{s\lambda_m})e(g_2^{\frac{t_2}{H(KW)t_w}},\prod_{m=0}^{n_1}K_{1,m}^{bs\lambda_m})\times e(PK_{S,2}^{\frac{t_1}{H(KW)t_w}},\prod_{m=0}^{n_1}K_{2,m}^{s\lambda_m})e(g_2^{\frac{t_2}{H(KW)t_w}},\prod_{m=0}^{n_1}K_{2,m}^{bs\lambda_m})=$$

$$e(g_2,f_1f_2)^{bsk\frac{t_1+t_2}{H(KW)}}e(g_2,\prod_{m=0}^{n_1}\prod_{i\in V',Z'}A_{i,1}^{i^m\lambda_m})^{bsk\frac{t_1+t_2}{H(KW)t_w}},$$

$$R=e(IX_3,T_3)e(IX_4,T_3)=$$

$$e((f_1'(\prod_{i\in V}A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{t_1+t_2},K_3^{\frac{s}{H(SKW)}})\times e((f_2'(\prod_{i\in Z}A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{t_1+t_2},K_3^{\frac{s}{H(SKW)}})=$$

$$e(f_1'f_2',g_1)^{bsk\frac{t_1+t_2}{H(SKW)}}e(\prod_{i\in V,Z}A_{i,2}^{\prod_{j=1}^{n_1}(i-w_j)},g_1)^{bsk\frac{t_1+t_2}{H(SKW)t_w}}.$$

当用户属性满足关键词索引中制定的访问结构,即除访问结构中通配符位置的元素以外,向量 $\boldsymbol{V}$ 中的元素与 $\boldsymbol{V}'$ 中相同且向量 $\boldsymbol{Z}$ 中的元素与 $\boldsymbol{Z}'$ 中的元素相同,由 1.3 节中的式(4)可得 $\prod_{i\in V,Z} g^{a_i \prod_{j=1}^{n_1}(i-w_j)} = \prod_{m=0}^{n_1}\prod_{i\in V',Z'} g^{a_i i^m \lambda_m}$;当搜索陷门与关键词索引中对应同一个关键词,即 $H(SKW)=H(KW)$. 因此 $L=R$,可成功解密.

4 方案分析

4.1 安全性证明

定理 1. 因此若多项式时间敌手 $\mathcal{A}$ 以不可忽略优势 ε 攻破该方案的 IND-CKA 安全性,则挑战者 $\mathcal{C}$ 能构造仿真器 $\mathcal{B}$ 以优势 $\frac{\varepsilon}{2}$ 解决 DLIN 问题.

证明. 挑战者 $\mathcal{C}$ 通过构造仿真器 $\mathcal{B}$ 来模拟不可区分游戏. 挑战者 $\mathcal{C}$ 将 DLIN 数组 $y_{\mathrm{DLIN}}=(g_1, g_1^a, g_1^b, g_1^{ac}, g_1^d, g_2, g_2^a, g_2^b, g_2^{ac}, g_2^d, Z)$ 交给仿真器 $\mathcal{B}$.

敌手 $\mathcal{A}$ 与仿真器 $\mathcal{B}$ 之间的游戏如下:

初始化:敌手 $\mathcal{A}$ 选取待挑战的访问结构 W^*, W^* 中包含 n_1 个通配符、n_2 个正属性和 n_3 个负属性,其中,通配符出现的位置为 $J=\{w_1, w_2, \cdots, w_{n_1}\}$,正属性出现的位置为 $V=\{v_1, v_2, \cdots, v_{n_2}\}$,负属性出现的位置为 $Z=\{z_1, z_2, \cdots, z_{n_3}\}$.

根据通配符出现位置 $J=\{w_1, w_2, \cdots, w_{n_1}\}$ 计算 $\lambda=\{\lambda_0, \lambda_1, \cdots, \lambda_{n_1}\}$.

系统建立:仿真器 $\mathcal{B}$ 运行系统建立算法,设置访问结构中通配符数量最多为 $N_1 \geqslant n_1$ 个. 选取 β, $\gamma\in\mathbb{Z}_p$,对系统中的属性选取 $a_i\in\mathbb{Z}_p$, $A_{i,2}=g_2^{a_i}$. 令

$$f_1' = (g_2^b)^{\beta} g_2^{-\sum_{att_i\in W_i^*, i\in V} \frac{a_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}},$$

$$f_2' = (g_2^b)^{\gamma} g_2^{-\sum_{att_i\in W_i^*, i\in Z} \frac{a_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}}.$$

令搜索服务器公钥为 $PK_{S,1}=g_1^a$, $PK_{S,2}=g_2^a$. 将系统公开参数 PP 交给敌手 $\mathcal{A}$.

阶段 1:敌手 $\mathcal{A}$ 向仿真器 $\mathcal{B}$ 提交待查询的属性集合 S,若 S 不满足 W^*,仿真器 $\mathcal{B}$ 按照正负属性出现的位置,将 S 解析为 $V'=\{v_1', v_2', \cdots, v_{n_2'}'\}$ 和 $Z'=\{z_1', z_2', \cdots, z_{n_3'}'\}$,选取 $k\in\mathbb{Z}_p$,计算:

$$K_1 = \{K_{1,m}\}_{m=0}^{N_1} = \{y(f_1 \prod_{i\in V'} A_{i,1}^{i^m})^k\}_{m=0}^{N_1} = \{y((g_1^b)^{\beta} g_1^{-\sum_{att_i\in W_i^*, i\in V} \frac{a_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{i\in V'} A_{i,1}^{i^m})^k\}_{m=0}^{N_1},$$

$$K_2 = \{K_{2,m}\}_{m=0}^{N_1} = \{y(f_2 \prod_{i\in Z'} A_i^{i^m})^k\}_{m=0}^{N_1} = \{y((g_1^b)^{\gamma} g_1^{-\sum_{att_i\in W_i^*, i\in Z} \frac{a_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{i\in Z'} A_{i,1}^{i^m})^k\}_{m=0}^{N_1},$$

$$K_3 = PK_{S,1}^k = (g_1^a)^k.$$

将密钥 $SK=\{K_1, K_2, K_3\}$ 发送给用户;若 S 满足 W^*,仿真器 $\mathcal{B}$ 不响应此次查询. 敌手 $\mathcal{A}$ 进行多项式次数的查询.

挑战:敌手 $\mathcal{A}$ 向仿真器 $\mathcal{B}$ 提交关键词 KW_0, KW_1. 仿真器 $\mathcal{B}$ 随机地选取 $rand\in\{0,1\}$,生成关键词 KW_{rand} 对应的索引. 仿真器 $\mathcal{B}$ 根据通配符出现位置 $\lambda=\{\lambda_0, \lambda_1, \cdots, \lambda_{n_1}\}$,令 $t_w=\sum_{m=0}^{n_1}\lambda_m$. 令 $t_1=c$, $t_2=d$,计算:

$$IX_1 = (g_2^{ac})^{\frac{1}{H(KW_{rand})t_w}},$$

$$IX_2 = (g_2^{d})^{\frac{1}{H(KW_{rand})t_w}},$$

$$IX_3 = (f_1'(\prod_{i\in V} A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{t_1+t_2} = ((g_2^b)^{\beta} g_2^{-\sum_{att_i\in W_i^*, i\in V} \frac{a_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} (\prod_{i\in V} A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{c+d} = Z^{\beta},$$

$$IX_4 = (f_2'(\prod_{i\in Z} A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{t_1+t_2} = ((g_2^b)^{\gamma} g_2^{-\sum_{att_i\in W_i^*, i\in Z} \frac{a_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} (\prod_{i\in Z} A_{i,2}^{\frac{\prod_{j=1}^{n_1}(i-w_j)}{t_w}}))^{c+d} = Z^{\gamma},$$

将 $IX_{KW_{rand}}$ 交给敌手 $\mathcal{A}$.

阶段 2:阶段 2 与阶段 1 相同,敌手 $\mathcal{A}$ 不能查询满足访问结构 W^* 的属性集合 S 对应的密钥.

猜测:挑战者 $\mathcal{C}$ 根据仿真器 $\mathcal{B}$ 输出的结果回答 DLIN 问题. 将敌手 $\mathcal{A}$ 对 $rand$ 的猜测结果表示为 $rand'$,若 $rand=rand'$, $\mathcal{B}$ 输出 $Z=g_2^{b(c+d)}$;否则, $\mathcal{B}$ 输出 $Z\neq g_2^{b(c+d)}$.

1) 若 $rand'\neq rand$,则:

$$Pr[rand'\neq rand \mid Z=g_2^z] = \frac{1}{2};$$

2) 若 $rand'=rand$,敌手的优势为 ε,则:

$$Pr[rand'=rand|Z=g_2^{b(c+d)}]=\frac{1}{2}+\varepsilon.$$

故挑战者 $\mathcal{C}$ 在 DLIN 游戏中的优势为

$$Adv=Pr[rand'=rand]-\frac{1}{2}=$$

$$\frac{1}{2}(Pr[rand'\neq rand|Z=g_2^z]+$$

$$Pr[rand'=rand|Z=g_2^{b(c+d)}])-\frac{1}{2}=\frac{\varepsilon}{2}.$$

证毕.

定理 2. 因此若多项式时间敌手 $\mathcal{A}$ 以不可忽略优势 ε 攻破该方案的关键词安全性,则挑战者 $\mathcal{C}$ 能构造仿真器 $\mathcal{B}$ 以优势 $\frac{\varepsilon}{2}$ 解决 DDDH 问题.

证明. 挑战者 $\mathcal{C}$ 通过构造仿真器 $\mathcal{B}$ 来模拟不可区分游戏. 挑战者 $\mathcal{C}$ 将将群 G_1 中的 DDDH 数组 $y_{\mathrm{DDDH}}=(g,g^a,g^b,Z)$ 交给仿真器 $\mathcal{B}$.

敌手 $\mathcal{A}$ 与仿真器 $\mathcal{B}$ 之间的游戏如下:

系统建立:仿真器 $\mathcal{B}$ 运行系统建立算法. 选取 $\beta,\gamma\in\mathbb{Z}_p$, $y=g^a$,令 $f_1=g^\beta$, $f_2=g^\gamma$,选取 $a_i\in\mathbb{Z}_p$, $A_i=g^{a_i}$. 选取 $b'\in\mathbb{Z}_p$ 令搜索服务器公钥为 $PK_S=(g^b)^{b'}$. 将系统公开参数 PP 交给敌手 $\mathcal{A}$.

阶段 1:敌手 $\mathcal{A}$ 发起多项式次数的密钥和陷门查询.

$\mathcal{O}_{KeyGen}$:敌手 $\mathcal{A}$ 向仿真器 $\mathcal{B}$ 提交待查询的属性集合 S,仿真器 $\mathcal{B}$ 按照正负属性出现的位置,将 S 解析为 $V'=\{v_1',v_2',\cdots,v_{n_2'}'\}$ 和 $Z'=\{z_1',z_2',\cdots,z_{n_3'}'\}$,选取 $k'\in\mathbb{Z}_p$,令 $k=bk'$,计算:

$$K_1=\{K_{1,m}\}_{m=0}^{N_1}=\{g^a((g^b)^\beta\prod_{i\in V'}(g^b)^{a_i i^m})\}_{m=0}^{N_1},$$

$$K_2=\{K_{2,m}\}_{m=0}^{N_1}=\{g^{-a}((g^b)^\gamma\prod_{i\in Z'}(g^b)^{a_i i^m})\}_{m=0}^{N_1},$$

$$K_3=PK_S^k=(g^b)^{b'k},$$

将密钥 $SK=\{K_1,K_2,K_3\}$ 发送给用户. 敌手 $\mathcal{A}$ 进行多项式次数的查询.

$\mathcal{O}_{Trapdoor}$:敌手 $\mathcal{A}$ 向仿真器 $\mathcal{B}$ 提交待查询的属性集合 S 和关键词 SKW,仿真器 $\mathcal{B}$ 运行密钥生成算法与陷门生成算法,选取随机数 $s\in\mathbb{Z}_p$,计算:

$$T_1=K_1^s=\{(g^a)^s((g^b)^{\beta s}\prod_{i\in V'}(g^b)^{sa_i i^m})\}_{m=0}^{N_1},$$

$$T_2=K_2^s=\{(g^{-a})^s((g^b)^{\gamma s}\prod_{i\in Z'}(g^b)^{sa_i i^m})\}_{m=0}^{N_1},$$

$$T_3=(g^b)^{\frac{b'sk}{H(SKW)}}.$$

将相应的陷门 TR 交给敌手 $\mathcal{A}$.

挑战:敌手 $\mathcal{A}$ 向仿真器 $\mathcal{B}$ 提交待挑战的属性集合 S^* 及关键词 SKW_1,SKW_2,阶段 1 中敌手 $\mathcal{A}$ 未查询 S^* 对应的密钥及陷门. 仿真器 $\mathcal{B}$ 选取随机数 $rand\in\{0,1\}$,运行密钥生成算法与陷门生成算法. 选取随机数 $s'\in\mathbb{Z}_p$,令 $s=\frac{s'}{b}$,计算:

$$T_1=K_1^s=\{Z^{s'}(g^{\beta s'}\prod_{i\in V'}g^{s'a_i i^m})\}_{m=0}^{N_1},$$

$$T_2=K_2^s=\{Z^{s'}(g^{\gamma s'}\prod_{i\in Z'}g^{s'a_i i^m})\}_{m=0}^{N_1},$$

$$T_3=g^{\frac{b's'k}{H(SKW_{rand})}},$$

将陷门 $TR_{SKW_{rand}}$ 交给敌手 $\mathcal{A}$.

阶段 2:阶段 2 与阶段 1 相同,敌手 $\mathcal{A}$ 不能查询属性集合 S^* 对应的密钥及陷门.

猜测:挑战者 $\mathcal{C}$ 根据仿真器 $\mathcal{B}$ 输出的结果回答 DDDH 问题. 将敌手 $\mathcal{A}$ 对 $rand$ 的猜测结果表示为 $rand'$,若 $rand=rand'$, $\mathcal{B}$ 回答 $Z=g^{\frac{a}{b}}$;否则, $\mathcal{B}$ 回答 $Z\neq g^{\frac{a}{b}}$.

1) 若 $rand'\neq rand$,则:

$$Pr[rand'\neq rand|Z=g^z]=\frac{1}{2};$$

2) 若 $rand'=rand$,敌手的优势为 ε,则:

$$Pr[rand'=rand|Z=g^{\frac{a}{b}}]=\frac{1}{2}+\varepsilon.$$

故挑战者 $\mathcal{C}$ 在 DDDH 游戏中的优势为

$$Adv=Pr[rand'=rand]-\frac{1}{2}=$$

$$\frac{1}{2}(Pr[rand'\neq rand|Z=g^z]+$$

$$Pr[rand'=rand|Z=g^{\frac{a}{b}}])-\frac{1}{2}=\frac{\varepsilon}{2}.$$ 证毕.

4.2　效率分析

方案效率对于资源受限的移动设备具有重要影响,表 1 从计算开销和通信开销 2 个方面将本文方案与近年来的经典方案[5,7,19]进行效率对比.

表 1 中 E_1,E_2 分别表示执行一次群 G,G_T 上指数运算的时间, P 表示执行一次双线性对运算的时间,由于上述运算的计算复杂度远远高于算法中的其他运算,因此计算复杂度对比主要考虑上述运算; N 表示系统中的属性总数, n_i 表示多值与门结构中每个属性的属性值数量, M 表示访问结构中使用的通配符数量上限,其中 $M\ll N$; $|G|$ 表示群 G 中元素的长度, $|G_T|$ 表示群 G_T 中元素的长度.

计算开销对比如表 1 中的列 2～4 所示. 由于索引算法、陷门算法由用户在移动终端上执行,搜索算法需要搜索服务器与多个用户进行交互,这 3 个算法的计算开销对用户体验的影响最大,因此主要对比这 3 个算法的计算复杂度. 如表 1 所示,本文方案中索引算法的计算复杂度与系统属性线性相关,

较文献[7,19]中的方案具有一定的优势,陷门算法和搜索算法与访问结构中可使用的通配符数量上限成正比,由于访问结构中可使用的通配符数量往往远小于系统中的属性数量,因此较其他方案本文方案中的陷门算法和搜索算法较其他方案具有较低的计算复杂度.

通信开销对比如表 1 中的后 4 列所示. 在搜索过程中,移动终端用户与授权机构、搜索服务器之间需要传输密钥、索引等参数,这些参数的长度将给带宽受限的移动设备带来一定的负担,通信开销主要对公开参数、密钥、索引和陷门的长度进行对比. 本文方案中索引长度定长,密钥长度和陷门长度与访问结构中可使用的通配符数量上限成正比,由于 $M \ll N$,本文方案中密钥长度和陷门长度较其他方案也具有较短的长度. 此外,本文与文献[19]移除了安全信道,进一步降低了通信开销.

Table 1 Efficiency Comparisons of Different ABKS

表 1 不同 ABKS 方案效率对比

Schemes	*EncIndex* Time	*GenTrapdoor* Time	*Search* Time	*PP* Size	*SK* Size	*IX* Size	*TR* Size
Ref[5]	$(N+1)E_1+E_2$	$(2N+1)E_1$	$(N+1)P+E_2$	$(3N+1)\|G\|+\|G_T\|$	$(2N+1)\|G\|$	$(N+1)\|G\|+\|G_T\|$	$(2N+1)\|G\|$
Ref[7]	$(2N+1)E_1+E_2$	$(2N+1)E_1+2E_2$	$(2N+1)P+E_2$	$(\sum_{i=1}^{n} n_i+3)\|G\|+\|G_T\|$	$(2N+1)\|G\|$	$(2N+1)\|G\|+\|G_T\|$	$(2N+1)\|G\|$
Ref[19]	$(2N+4)E_1$	$(2N+5)E_1$	$(2N+3)P+E_1$	$3\|G\|$	$(2N+1)\|G\|$	$(2N+3)\|G\|$	$(2N+4)\|G\|$
Ours	$(N-M+4)E_1$	$(2M+3)E_1$	$3P+(2M+2)E_1$	$(N+4)\|G\|$	$(2M+3)\|G\|$	$4\|G\|$	$(2M+3)\|G\|$

本文通过仿真实验对算法进行评估,实验的硬件环境为 Intel Core i5,2.4 GHz 处理器,操作系统为环境为 64 位 Windows10 操作系统,实验基于 Charm[20]架构,选用 JPBC 中的 D 类椭圆曲线. 选取系统属性总量 $N=50$,令通配符总量 M 从 1～10 变化. 实验结果如图 2 所示,索引算法随通配符数量增加呈线性减少趋势,而陷门和搜索算法随之呈线性增长趋势.

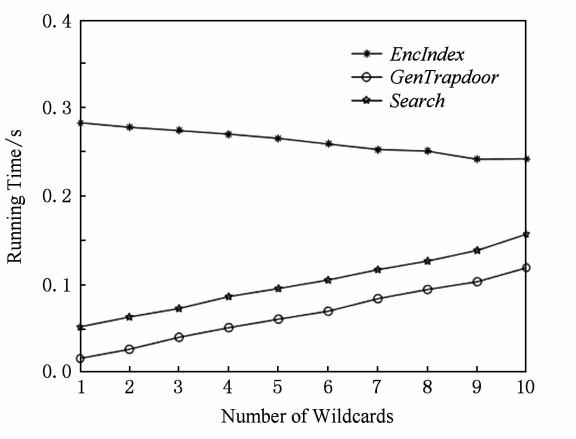

Fig. 2 The influence of wildcards number on running time

图 2 通配符数量对方案运行时间的影响

5 总 结

针对现有 ABKS 方案计算开销和通信开销较大,不能较好地支持移动设备的问题,本文提出一个适用于移动云存储环境的 ABKS 方案,该方案在标准模型下满足 IND-CKA 安全性和关键词安全性. 与经典方案相比,本方案具有较低的计算开销和通信开销. 本文的 IND-CKA 安全性证明是在选择模型下进行的,在未来研究中将对方案的安全性进行进一步提升,构造标准模型下完全安全的新方案.

参 考 文 献

[1] Cui Yong, Song Jian, Miao Congcong, et al. Mobile cloud computing research progress and trends [J]. Chinese Journal of Computers, 2017, 40(2): 273-295 (in Chinese)
(崔勇, 宋健, 缪葱葱, 等. 移动云计算研究进展与趋势[J]. 计算机学报, 2017, 40(2): 273-295)

[2] Sahai A, Waters B. Fuzzy identity-based encryption [G] // LNCS 3494: Proc of the 24th Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457-473

[3] Li Hui, Sun Wenhai, Li Fenghua, et al. Secure and privacy-preserving data storage service in public cloud [J]. Journal of Computer Research and Development, 2014, 51(7): 1397-1409 (in Chinese)
(李晖, 孙文海, 李凤华, 等. 公共云存储服务数据安全及隐私保护技术综述[J]. 计算机研究与发展, 2014, 51(7): 1397-1409)

[4] Dan B, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search [G] //LNCS 3027: Proc of the 23rd Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522

[5] Sun Wenhai, Yu Shucheng, Lou Wenjing, et al. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud [J]. IEEE Trans on Parallel & Distributed Systems, 2016, 27(4): 1187-1198

[6] Zheng Qingji, Xu Shouhuai, Ateniese G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data [C] //Proc of the 33rd IEEE Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2014: 522-530

[7] Qiu Shuo, Liu Jiqiang, Shi Yanfeng, et al. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack [J]. Science China Information Sciences, 2017, 60(5): 052105

[8] Cheung L, Newport C. Provably secure ciphertext policy ABE [C] //Proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM, 2007: 456-465

[9] Emura K, Miyaji A, Omote K, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length [J]. International Journal of Applied Cryptography, 2010, 2(1): 46-59

[10] Zhang Yinghui, Dong Zheng, Chen Xiaofeng, et al. Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts [G]//LNCS 8782: Proc of the 8th Int Conf on Provable Security. Berlin: Springer, 2014: 259-273

[11] Xiao Siyu, Ge Aijun, Ma Chuangui. Decentralized attribute-based encryption scheme with constant-size ciphertexts [J]. Journal of Computer Research and Development, 2016, 53(10): 2207-2215 (in Chinese)
(肖思煜, 葛爱军, 马传贵. 去中心化且固定密文长度的基于属性加密方案[J]. 计算机研究与发展, 2016, 53(10): 2207-2215)

[12] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [G]//Proc of the 5th Int Conf on Applied Cryptography and Network Security. Berlin: Springer, 2008: 111-129

[13] Lai Junzuo, Deng R H, Li Yingjun. Fully secure cipertext-policy hiding CP-ABE [G]//LNCS 6672: Proc of the 7th Int Conf on Information Security Practice and Experience. Berlin: Springer, 2011: 24-39

[14] Phuong T V X, Yang Guomin, Susilo W. Hidden ciphertext policy attribute-based encryption under standard assumptions [J]. IEEE Trans on Information Forensics & Security, 2015, 11(1): 35-45

[15] Jin Cancan, Feng Xinyu, Shen Qingni. Fully secure hidden ciphertext policy attribute-based encryption with short ciphertext size [C] //Proc of the 16th Int Conf on Communication and Network Security. New York: ACM, 2016: 91-98

[16] Baek J, Safavinaini R, Susilo W. Public key encryption with keyword search revisited [G] //LNCS 5072: Proc of the 6th Int Conf on Computational Science and Its Applications. Berlin: Springer, 2008: 1249-1259

[17] Rhee H S, Susilo W, Kim H. Secure searchable public key encryption scheme against keyword guessing attacks [J]. IEICE Electronics Express, 2009, 6(5): 237-243

[18] Fang Liming, Susilo W, Ge Chunpeng, et al. Public key encryption with keyword search secure against keyword guessing attacks without random oracle [J]. Information Sciences, 2013, 238(7): 221-241

[19] Lin Peng, Jiang Jie, Chen Tieming. Application of keyword searchable encryption in cloud [J]. Journal on Communications, 2015, 36(S1): 259-265 (in Chinese)
(林鹏, 江颉, 陈铁明. 云环境下关键词搜索加密算法研究[J]. 通信学报, 2015, 36(S1): 259-265)

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

Su Hang, born in 1994. Master candidate. Her main research interests include public key encryption.

Zhu Zhiqiang, born in 1961. PhD, professor. His main research interests include cloud computing and information security (zhiqiang_zhu_zz@163.com).

Sun Lei, born in 1973. PhD, professor. His main research interests include cloud computing and information security (sl0221@sina.com).