计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.201100214

云环境下基于属性的多关键字可搜索加密方案

高诗尧　陈燕俐　许玉岚
南京邮电大学计算机学院 软件学院 网络空间安全学院　南京 210003
(1018041101@njupt.edu.cn)

摘　要　可搜索加密技术可在不解密数据密文的同时实现密文关键字的检索,很好地保护了数据存储方的隐私。针对目前大多数可搜索加密方案无法支持用户自定义搜索策略的问题,提出了一种安全、高效、可支持任意表达的基于属性可搜索加密方案。该方案首先基于LSSS搜索结构,支持任意合取、析取或单调布尔表达式的多关键字搜索策略,用户使用私钥为LSSS搜索策略生成陷门,云服务器通过陷门可以搜索包含满足特定关键字搜索策略的密文;其次,通过与基于属性加密方案结合,可以实现对云中加密数据的细粒度访问控制;另外,该方案通过将关键字拆分成关键字名和关键字值以及"线性拆分"技术,使得攻击者无法从密文和陷门中推测出关键字值敏感信息;最后,通过将部分解密工作转移到云服务器来降低用户的计算负担。基于DBDH、(q-2)和判定线性假设证明了所提方案的安全性,理论分析和实验结果也表明了该方案的有效性。

关键词:云计算;数据共享;属性加密;可搜索加密;关键字搜索策略
中图法分类号　TP309

Expressive Attribute-based Searchable Encryption Scheme in Cloud Computing

GAO Shi-yao,CHEN Yan-li and XU Yu-lan
School of Computer Science,School of Software,School of Cyberspace Security,Nanjing University of Posts and Telecommunications,Nanjing 210003,China

Abstract　Searchable encryption technology can realize keyword search without decrypting the data,and thus well protects user's private information. Aiming at the problem that most current searchable encryption schemes cannot support user-defined search strategies,this paper proposes an attribute-based searchable encryption scheme which is secure,efficient and can support arbitrary search expressions. Firstly,the scheme,based on LSSS access structure,allows keyword search policy to be represented by conjunction,disjunction or any monotone Boolean expression,user generates trapdoor for LSSS search policy by utilizing the private key,and cloud server can search ciphertexts that satisfy specific keywords search policy through trapdoor. Secondly,it can realize fine-grained access control of encrypted data in cloud through combining with attribute-based encryption scheme. In addition,attackers cannot infer the sensitive information of keyword values from ciphertext and trapdoor by splitting keywords into keyword names and values through "linear splitting" technology. Finally,the computing burden of users is reduced due to part of decryption work is transfered to cloud server. The security of the proposed scheme is proved based on BDHE,(q-2) assumption. Theoretical analysis and experimental results also show that the scheme is effective.

Keywords　Cloud computing,Data sharing,Attribute-based encryption,Searchable encryption,Keywords search policy

1　引言

自Google提出"云计算"概念以来,云计算逐渐成为一种成熟的商业模式,具有服务更精准、计算资源灵活、计算效率高、管理开销低等优势。云服务器(Cloud Service,CS)可以为用户提供外包计算、数据存储等各种服务,数据属主(Data Owner,DO)可以将大量数据存储在云服务器中,并与其他数据用户(Data User,DU)共享数据。为了保障存储数据的安全性和用户隐私,数据通常以加密的形式存储在云服务器中。但是在这种环境下,DU会遇到无法在海量数据中搜索关键字的问题,在某种程度上限制了云环境下文件共享的灵活性。为了解决云环境中对加密数据搜索困难的问题,专家们提出了可搜索加密(Searchable Encryption,SE)技术,SE技术主要解决了在云服务器不完全可信的情况下DU如何使用云服务器完成对密文关键字搜索的问题。DU若想要获取包含指定关键字的密文,需要使用其私钥和欲搜索的关键字产生陷门,并将陷门交予云服务器,云服务器根据陷门进行密文搜索匹配操作。在整个过程中,云服务器无法从陷门、密文或搜索

到稿日期:2020-11-30　返修日期:2021-04-10　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61572263,61272084)
This work was supported by the National Natural Science Foundation of China (61572263,61272084).
通信作者:陈燕俐(chenyl@njupt.edu.cn)

过程中得到任何关于密文的消息。根据所使用的密码体制以及构造算法的不同，可以将 SE 分为两类：对称可搜索加密[1](Symmetric Searchable Encryption，SSE)和公钥可搜索加密[2](Public Encryption with Keyword Search，PEKS，也称为非对称可搜索加密)。前者与对称加密算法相类似，其加密私钥与解密私钥是相同的，但通信模式为“一对一”，更适合于单用户模型；后者基于双线性映射等，将安全问题建立在一些复杂性假设上，解决了对称可搜索加密“一对一”通信模式的问题，可以面向第三方服务器的密文搜索。

可搜索加密支持用户在密文中搜索关键字，可为用户节省大量的网络和计算开销，充分利用了云服务器巨大的计算能力，目前已有大量单关键字搜索方案[3-5]、排序关键字搜索方案[6-8]和多关键字搜索方案[9-12]被提出。但如何在降低本地计算负荷的同时提高关键字搜索效率、灵活性和精确度仍然是一个亟待解决的问题。考虑到在很多云环境实际应用场景中，用户想要搜索的关键字是合取、析取或任何布尔表达式的组合，传统的单关键字、联合多关键字的搜索策略无法满足用户特定的搜索需求，即支持任意布尔表达式搜索策略的需求。以个人电子健康记录(E-Health Record，EHR)为例，患者为了在大量密文中进行灵活的搜索，制定“疾病”“年龄”和“体重”之间关系的关键字搜索策略，如“(疾病：心脏病 AND (年龄：60 OR 体重：100-150))”，通过灵活表达的搜索策略，患者可以实现更细粒度的关键字搜索，云服务器返回的搜索结果也更准确。为了实现支持任意表达的可搜索加密，文献[13-17]提出了可支持任意表达的多关键字可搜索加密方案(Expressive Public key Encryption with Keyword Search，EPEKS)，但这些方案存在存储、计算开销较大或者不能很好地抵抗关键字猜测攻击的安全性问题，在存储开销、计算效率、安全性、功能性等方面未能达到很好的平衡。

针对目前 EPEKS 方案存在的以上问题，本文提出了一种安全高效、可支持任意表达的基于属性多关键字的可搜索加密方案(Expressive Attribute-Based Searchable Encryption，EABSE)。本文的主要贡献如下：

(1)将基于属性加密与可搜索加密相结合，共享数据的加密采用了 CP-ABE 方案，关键字加密采用了 KP-ABE 方案，支持用户在生成陷门时根据需求以合取、析取或任意布尔表达式制定关键字搜索策略，实现更加高效的多关键字细粒度搜索。将搜索属性关键字拆分为关键字名和关键字值，用户可通过公开的关键字名高效地进行访问结构的匹配。另外通过引入“线性拆分”的技术将每个关键字值相对应的密文和陷门组件拆分成两个随机化的互补成分，使得攻击者无法从密文和陷门中猜测出关键字值的有效信息。因此该方案可以很好地抵抗关键字猜测攻击，安全性较高。

(2)关键字搜索功能是由云服务器完成的，并且解密的一部分计算任务被转移到云服务器上，从而降低了用户的计算负担，而云服务器在整个过程中不会得到与关键字有关的有用信息。

2 相关工作

2.1 基于属性加密

基于属性的加密(Attribute-Based Encryption，ABE)[18]体制是由 Sahai 等于 2005 年提出的。为了解决基于身份加密(Identity Based Encryption，IBE)[19]系统的容错性能，他们在 IBE 方案中使用了生物识别技术，提出了基于模糊身份的加密方案[18](Fuzzy Identity-Based Encryption，Fuzzy IBE)。为了提供更好的灵活性，Sahai 引入访问结构(Access Structure)的概念，进一步提出了 ABE 机制。基于属性的加密方案的提出使得用户的身份不再局限于身份信息，而是可以由若干属性组成的集合代表。2006 年，Goyal 等提出了细粒度的 ABE 方案[20]。他们将基于属性的密码系统进一步细分为密文策略的基于属性的加密方案(Ciphertext Policy Attribute-Based Encryption，CP-ABE)以及密钥策略的基于属性的加密方案(Key Policy Attribute-Based Encryption，KP-ABE)。

2.2 可搜索加密

可搜索加密是保护关键字隐私的重要加密原语，可在保证密文安全性的前提下使用户在大量加密数据中搜索到相应的密文。2000 年，Song 等[1]首次提出可搜索加密的概念，并在对称加密系统下实现了一种可搜索加密方案，该方案允许数据属主生成相应关键字的搜索陷门。Boneh 等[2]在 2004 年提出第一个公钥可搜索加密(PEKS)方案，并根据基于身份的加密(IBE)提出了 PEKS 的通用构造。为了提高搜索的准确性，用户搜索的关键字通常是多关键字。2005 年，Park 等[21]首次提出多关键字 PEKS 方案，该方案支持用户以关键字合取的方式生成陷门。

2012 年，Han 等[22]根据文献[23]的匿名 IBE 方案转换到 PEKS 方案的形式，提出了从 KP-ABE 到可搜索加密的一般性转换。2013 年，Kaushik 等[24]第一次将属性加密和可搜索加密相结合，提出基于属性的可搜索加密(Attribute-Based Searchable Encryption，ABSE)，只有属性符合树形访问结构的用户才能对关键字进行搜索。同年，Xiong 等[25]将一个简单高效的同态可搜索加密方案与传统的 CP-ABE 方案相结合，提出了一个 CP-ABSE 方案，该方案巧妙地将同态加密算法中的加密算法作为其加密算法，并使用基于属性的加密算法加密同态加密中的密钥，最终密文由消息密文与密钥密文构成。

2019 年，He 等[26]提出了一种轻量级的基于属性的多关键字可搜索加密搜索方案，该方案将部分计算外包给私有云，减轻了数据属主的计算负担，但其不支持子集多关键字查询。2019 年，Wang 等[27]提出了一种的基于属性的多关键字可搜索加密方案，该方案支持任意子集的多关键字搜索并保证了用户的搜索隐私。同年，Sun 等[28]通过结合 CP-ABE 和审计思想，提出了一种可验证的多关键字可搜索加密方案，该方案引入了受信任的第三方实体，使用签名机制来验证云服务器返回的搜索结果的完整性。2020 年，Liu 等[29]提出了支持重复数据删除和数据完整性验证的可搜索加密方案。2021 年，Liu 等[30]提出一种匿名密钥的多关键字可搜索加密方案，该方案为避免密钥托管，为用户生成一个匿名密钥，同时隐藏了访问策略以确保数据用户的匿名性和访问策略的机密性。

但以上的方案都不支持用户在陷门中自定义搜索策略，无法实现灵活的搜索策略。2013 年，Lai 等[13]将 KP-ABE 中的属性视为关键字，首次提出了可支持任意表达的多关键字

可搜索加密方案,该方案支持使用"与(AND)""或(OR)"表达式表示陷门中的多关键字搜索策略,但关键字在该方案中公开,导致关键字隐私泄漏。2014 年,Lv 等[14]在此基础上提出了安全的 EPEKS 方案,该方案将关键字拆分为关键字名和关键字值,将关键字公开并将关键字值隐藏,避免了关键字隐私泄漏问题。上述两个方案都是基于复合阶群,因为复合阶群中的元素长度较素数阶群长,所以计算成本和存储开销高。2018 年,Cui 等[15]提出了素数阶群上的 EPEKS,减少了计算成本和存储开销,该方案为了在密文和陷门中隐藏关键字,引入了"线性拆分"技术,将每个关键字相对应的密文成分拆分成两个随机化的互补成分,即使密文仍然包含有关关键字的信息,但由该信息无法推断出敏感信息。我们发现该方案中仍然存在陷门关键字猜测攻击的问题,敌手可以通过双线对和乘积运算对陷门中的组件进行关键字猜测,导致关键字信息泄漏。2019 年,Hao 等[16]在 Cui 等[15]的基础上,提出了一种在密文和陷门中引入虚拟属性的 EPEKS 方法,以防止云服务器在执行密文搜索时获取密文和陷门中的关键字,但该方案的访问结构为树形结构,由于采用递归和拉格朗日差值计算,效率较低,计算和存储开销较大。2020 年,Shen 等[17]提出一种将属性匿名 KP-ABE 转换为 EPEKS 方案的通用方法,其中属性匿名仍然采用将属性分为属性名和属性值的方法,由于该方案没有采用"线性拆分"技术,也存在关键字猜测攻击的问题。

3 预备知识

3.1 相关定义

定义 1(双线性映射[19]) 设置两个阶为素数 p 的乘法循环群 G 和 G_T,g 是 G 的一个生成元。存在一个双线性映射 $e:G_0\times G_0\rightarrow G_T$,必须满足以下 3 个条件:

(1)双线性。对于任意 $u,v\in G$,任意 $a,b\in Z_p$ 都有 $e(u^a,v^b)=e(u,v)^{ab}$。

(2)非退化性。存在 $u,v\in G$ 满足 $e(u,v)\neq 1$。

(3)可计算性。对于任意 $u,v\in G$,$e(u,v)$ 可有效计算。

定义 2(访问结构[18]) 令 $\{P_1,P_2,\cdots,P_n\}$ 为 n 个参与者的集合,如果 $\forall B,C$ 满足 $B\in A,B\subseteq C$,则 $C\in A$,集合 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$ 是单调的。其中属于 A 的集合称为授权集合。

通常,数据用户由属性描述。授权集合包含在 A 中。除非另有说明,否则该方案将使用单调形式的访问结构。

定义 3(线性秘密共享矩阵(LSSS)[31]) 令 $\{P_1,P_2,\cdots,P_n\}$ 为 n 个参与者的集合,这一组参与者上的秘密共享方案 π 是线性的,如果:

(1)各方的秘密因子构成了 Z_p 上的向量。

(2)存在一个 l 行 n 列的矩阵 $\boldsymbol{M}$,称为 π 的共享生成矩阵。对于所有 $i=1,2,\cdots,l$,$\boldsymbol{M}$ 的第 i 行为 $\boldsymbol{M}_i$,令函数 ρ 将参与者所在的行 i 定义为 $\rho(i)$。考虑列向量 $\boldsymbol{v}=(s,r_2,\cdots,r_n)$,其中 $s\in Z_p$ 是要共享的秘密值,$r_2,\cdots,r_n\in Z_p$ 是随机选择的,则 $\boldsymbol{M}\cdot\boldsymbol{v}$ 是 l 个秘密因子的向量。每个秘密因子 $\lambda_i=\boldsymbol{M}_i\cdot\boldsymbol{v}$ 属于参与者 $\rho(i)$。

文献[32]表明,根据上述定义,每个线性秘密共享方案都具有线性重构属性,定义如下:假设 π 是访问结构 A 的 LSSS。$\varphi\in A$ 为任意授权集合,令 $I\in\{1,2,\cdots,l\}$,定义为 $I=\{i:\rho(i)\in\varphi\}$。存在常数 $\{\omega_i\in Z_p\}_{i\in I}$,满足 $\sum_{i\in I}\omega_i\cdot\boldsymbol{M}_i=(1,0,\cdots,0)$,如果 $\{\lambda_i\}$ 是根据 π 的任何秘密值的有效秘密因子,则有 $\sum_{i\in I}\omega_i\cdot\lambda_i=t$。

3.2 困难假设

定义 4(DBDH 假设(Decisional Bilinear Diffie-Hellman Assumption)[20]) 根据系统安全参数选择一个阶为素数 p 的乘法循环群 G,g 是 G 的一个生成元。随机选择 $a,b,c\in Z_p$,假设 DBDH 问题是给定多元组 $(g,g^a,g^b,g^c,e(g,g)^{abc})$,如果不存在一种算法能够在多项式时间内以不可忽略的概率区分 (g,g^a,g^b,g^c,Z),其中 $Z\in G_T$,则 DBDH 假设成立。

定义 5(决策(q-2)假设(Decisional (q-2) Assumption)[33])
设 q 为整数,随机选择 $x,y,z,b_1,\cdots,b_q\in Z_p$,计算

$$\vec{A}=\left\{\begin{array}{l} g,g^x,g^y,g^{(xy)^2} \\ \{g^{b_i},g^{xzb_i},g^{xz/b_i},g^{x^2zb_i},g^{y/b_i^2},g^{y^2/b_i^2}\}\ \forall i\in[q] \\ \{g^{xzb_i/b_j},g^{yb_i/b_j^2},g^{xyzb_i/b_j}\}\ \forall i,j\in[q],i\neq j \end{array}\right\}$$

假设决策(q-2)问题是给定 $(\vec{A},e(g,g)^{xyz})$,如果不存在一种算法能够在多项式时间内以不可忽略的概率区分 $(\vec{A},Z)$,其中 $Z\in G_T$,则决策(q-2)假设成立。

4 EABSE 方案的形式化定义及安全模型

4.1 形式化定义

定义 6 EABSE 由 6 种算法组成,如下所示:

(1)$Setup(1^\lambda)\rightarrow(PK,MSK)$:输入参数为系统的安全参数 λ,输出公开参数 PK 和主密钥 MSK。公开 PK,保留 MSK。

(2)$Kengen(PK,MSK,\varphi)\rightarrow(SK)$:输入参数为公开参数 PK、主密钥 MSK 和用户属性集 φ,为用户生成属性密钥 SK。

(3)$Encrypt(PK,A,F,KW)\rightarrow(CT)$:输入参数为公开参数 PK、访问结构 A、共享数据文件 F、关键字集 KW。生成包含共享数据文件密文和关键字密文的密文 CT。

(4)$Trapgen(PK,SK,P)\rightarrow(T)$:输入公开参数 PK、用户密钥 SK、查询关键字集的访问结构 P,输出与 P 相关的陷门 T。

(5)$Search(PK,T,CT)\rightarrow(Z/\perp)$:输入公开参数 PK、密文 CT 和陷门 T。判断密文中的关键字集是否与查询关键字集的访问结构 P 匹配,如果关键字匹配成功,查询到文件,再判断用户的属性集是否满足密文中的访问结构 A。如果没有找到匹配的文件或者文件不在用户能够解密的范围内,输出 $\perp$;否则,CSP 返回已完成部分解密的文件 Z。

(6)$Decrypt(PK,SK,Z)\rightarrow(F)$:输入公开参数 PK、用户的属性私钥 SK、部分解密密文 Z,输出共享数据文件 F。

4.2 安全模型

在本文的 EABSE 方案中,假定授权中心是受信任的实体,且配备有单独的身份验证机制,在为数据用户生成陷门之前验证数据用户的身份,而云服务器是"诚实但好奇"的实体,即它会诚实地为用户提供服务,但也会利用其拥有的信息从密文及陷门中探寻任何私有信息。假定数据属主诚实地存储

他们的数据，而数据用户不受信任，他们可以与恶意的云服务器合谋探寻其他用户的私有信息。此外，本方案假设所有对手的计算能力都有限，因此他们无法攻克上述难题。

本文 EABSE 方案的语义安全性确保加密的文件不会泄漏有关共享数据和关键字的任何信息，即本方案具有 IND-CKA 安全性(Indistinguishability against Chosen Keyword-set Attack)

根据文献[2,31]中介绍的安全模型，本文给出 EABSE 的安全性定义以确保本文方案不会在密文和陷门中泄漏有关关键字值的任何信息，称之为 IND-CKA 安全。接下来本文在敌手 A 和挑战者 B 之间定义 IND-CKA 安全游戏。

挑战者 B 与敌手 A 之间的安全游戏是为了确保在没有关键字密文满足陷门中访问结构的情况下，云服务器搜索时无法推断出关键字集的信息。因为一旦为云服务器提供了关键字密文可以满足的陷门，则云服务器将确定该密文至少包含与给定陷门中与访问结构关联的关键字。

系统建立。$\mathcal{B}$ 运行 EABSE 的 *Setup* 阶段，输出公共参数 PK 和主私钥 MSK，并将 PK 发送给 $\mathcal{A}_1$，保留 MSK。

询问阶段 1。$\mathcal{A}$ 自适应地向 $\mathcal{B}$ 发出针对相应搜索结构 $(\boldsymbol{N}_1,\pi_1,\{W_{\pi_1(i)}\}),\cdots,(\boldsymbol{N}_{q_1},\pi_{q_1},\{W_{\pi_{q_1}(i)}\})$ 的陷门查询。对于每一个 $(\boldsymbol{N}_j,\pi_j,\{W_{\pi_j(i)}\}),j\in[1,q_1]$，$\mathcal{B}$ 运行 Trapgen 算法，并将 T 发送给 $\mathcal{A}$。

挑战。$\mathcal{A}$ 选择两个相同大小的关键字集 W_0^* 和 W_1^*，$W_0^*,W_1^*\notin L_{kw}$，即它们无法在 O_{Trapgen} 中被查询。$\mathcal{B}$ 随机选择 $\beta\in\{0,1\}$，并且运行 Encrypt 算法，将 W_β^* 加密为 CT^*，最后将 CT^* 发送给 $\mathcal{A}$。

询问阶段 2。$\mathcal{A}$ 重复询问阶段 1 的步骤，向 $\mathcal{B}$ 发出针对相应搜索结构 $(\boldsymbol{N}_{q_1+1},\pi_{q_1+1},\{W_{\pi_{q_1+1}(i)}\}),\cdots,(\boldsymbol{N}_q,\pi_q,\{W_{\pi_q(i)}\})$ 的陷门查询。但是有一个限制，对于任意 $(\boldsymbol{N}_j,\pi_j,\{W_{\pi_j(i)}\}),j\in[1,q_1]$，$W_0^*$ 和 W_1^* 都无法满足。

猜测阶段。$\mathcal{A}$ 输出一个 β 的猜想 β'，若 $\beta=\beta'$，则敌手 $\mathcal{A}_1$ 赢得比赛。上述游戏中的优势 $\mathcal{A}$ 可以描述为 $Adv_{\mathcal{A}}^{\text{IND}}(\lambda)\overset{def}{=}\left|\Pr[\rho=\rho']-\frac{1}{2}\right|$。

5 EABSE 方案

本文基于 KP-ABE、CP-ABE 和可搜索加密技术，提出了一种可支持任意表达搜索策略的多关键字可搜索加密 EABSE 方案。该方案由一个可信的授权中心 AA 发布公共参数，并对主密钥保密，数据属主 DO 将加密文件(包括共享数据加密文件和多个加密关键字索引)上传到云服务器 CSP 存储。为了检索文件关键字符合检索策略，例如“院名＝计算机学院”AND“职称＝教授”的所有加密文件，用户 DU 根据该访问策略构建 LSSS 结构，并生成相应的陷门，传送给云服务器 CSP，CSP 根据陷门对加密关键字进行检索，检索出符合搜索策略的加密文件，并对用户属性满足加密文件的访问结构进行部分解密，最后传送给用户解密，得到共享数据文件。

共享数据文件的加密采用 CP-ABE 加密算法，共享数据文件的访问结构嵌入在密文中，用户的私钥与其属性相关，保证了只有具有满足共享数据访问结构属性的用户才能解密密文并得到共享数据文件。对于密文关键字搜索，本文方案中将关键字视为属性，支持用户在生成陷门时根据需求以合取、析取或任意布尔表达式制定 LSSS 关键字搜索策略，云服务器可以通过陷门搜索到满足 LSSS 搜索策略的关键字密文，实现更加高效的细粒度多关键字搜索功能。为了不泄漏密文关键字和陷门中的访问策略关键字，将关键字拆分成关键字名和关键字值，设关键字集为 $\{N_1=W_1,N_2=W_2,\cdots,N_m=W_m\}$，$N_i$ 为第 i 个关键字的关键字名，W_i 为其对应的关键字值，关键字名可以公开送给云服务器，云服务器可以迅速通过关键字名找到符合 LSSS 搜索策略的关键字集合。另外，关键字值的隐藏通过“线性拆分”技术实现，密文中的随机化互补因子使得攻击者无法从密文和陷门中推测出关键字值敏感信息。另外，该方案还在陷门生成时对用户私钥进行重新随机化，保证了用户属性密钥的安全性。

本文 EABSE 方案实现了基于属性加密和支持任意布尔表达式可搜索加密的有机结合，支持用户在生成陷门时根据关键字的布尔表达式制定相应的搜索策略，使得用户搜索更加灵活。另外，只有与关键字匹配的密文才需要解密，减少了解密开销和密文下载的通信开销。

5.1 系统模型

本文 EABSE 方案的系统模型如图 1 所示，该系统主要涉及 4 种不同类型的实体：授权中心(Attribute Authority，AA)、数据属主(Data Owner，DO)、数据用户(Data User，DU)和云服务提供商(Cloud Server Provider，CSP)。

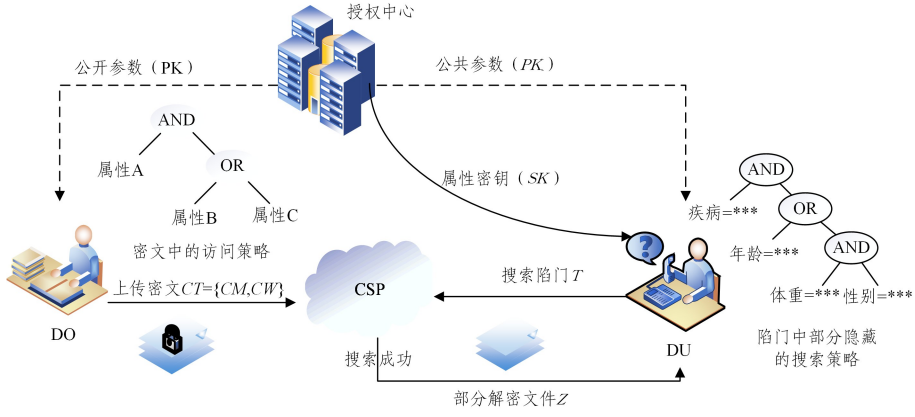

图 1 系统模型

Fig. 1 System model

AA：授权中心是一个完全可信的实体，负责管理系统中的属性。AA 根据每个 DU 的属性为其分配属性密钥。此外，授权中心还负责协助 DU 生成搜索陷门。

DO：数据属主负责加密共享数据文件和关键字集索引，生成共享数据密文和关键字密文，将相关的密文上传到 CSP。

DU：每一个数据用户都有与其属性集相关的私钥。DU 可以在 AA 的协助下生成欲搜索关键字的搜索陷门，然后交予云服务器，利用云服务器查找搜索相关数据。一旦从 CSP 接收到匹配的密文，如果 DU 的属性集满足密文中的访问策略，则可以对密文进行解密。

CSP：云服务器提供商是一个诚实但好奇的半可信实体。CSP 会好奇存储在云上的数据，但是绝对忠诚，会严格履行特定的服务，不会恶意删除数据或者拒绝响应用户的请求。在本系统中，CSP 负责密文存储、关键字检索和部分解密工作。

5.2 EABSE 方案的具体构造

(1)初始化算法 $Setup(1^\lambda)\rightarrow(PK,MSK)$

由 AA 执行，输入安全参数 λ，生成阶为素数 p 的乘法循环群 G 和 G_T，给定双线性映射 $e:G\times G\rightarrow G_T$，$g$ 为 G 的生成元。AA 定义两个哈希函数 $H_1:\{0,1\}^*\rightarrow G, H_2:\{0,1\}^*\rightarrow G$。随机选择 $\alpha,\beta,t_1,t_2,t_3,t_4\in Z_p$，生成系统的公共参数 PK 和主密钥 MSK，PK 由 AA 公开，MSK 由 AA 秘密保存。

$$PK=\{e(g,g)^{t_1t_2\alpha}, e(g,g)^{\beta}, g^{\alpha}, g^{t_1}, g^{t_2}, g^{t_3}, g^{t_4}, H_1, H_2\}$$

$$MSK=\{\alpha,\beta,t_1,t_2,t_3,t_4\}$$

(2)用户密钥生成算法 $Kengen(PK,MSK,\varphi)\rightarrow(SK)$

由 AA 执行，输入公共参数 PK、主密钥 MSK 和用户的属性集 φ。当用户加入时，根据用户属性集 φ，AA 选择一个随机值 $r\in Z_p$，计算 $D_1=g^{\beta}g^{ar}, D_2=g^r$，对每一个属性 $x\in\varphi$ 计算 $D_x=H_1(x)^r$。生成 DU 的属性密钥 SK，并通过安全信道传送给用户。

$$SK=\{D_1=g^{\beta}g^{ar}, D_2=g^r, \{D_x=H_1(x)^r\}_{x\in\varphi}\}$$

(3)共享数据文件和关键字加密算法 $Encrypt(PK,A,F,KW)\rightarrow(CT)$

加密算法由 DO 执行，算法输入公共参数 PK、共享数据文件 F、关键字集 KW(每一个关键字表示为 $N_i=W_i$，其中 N_i 是通用的关键字名，随密文公开；W_i 是敏感的关键字值，需隐藏在密文中)以及共享数据文件访问结构 $A=(\boldsymbol{M},\rho)$，其中，$\boldsymbol{M}$ 是 $l_s\times n_s$ 的矩阵，l_s 是访问结构矩阵 $\boldsymbol{M}$ 中的属性个数。

1)共享数据密文的生成

首先用对称密钥 ck 加密共享数据文件 F，得到共享数据密文 $CF=Enc(F,ck)$(此处 Enc 是一种对称加密算法)。随机选择 $t,y_2,\cdots,y_{l_s},r_1,.,r_{l_s}\in Z_p$，令向量 $\boldsymbol{u}=(t,y_2,\cdots,y_{l_s})$，对于 $i=1,2,\cdots,l_s$ 计算 $\lambda_i=\boldsymbol{M}_i\cdot\boldsymbol{u}$。最后采用 CP-ABE 加密机制对对称密钥 ck 进行加密，生成密文如下：

$$C=ck\cdot e(g,g)^{\beta t}, \hat{C}=g^t, \{C_{i1}=g^{\omega\lambda_i}H_1(\rho(i))^{-r_i}, C_{i2}=g^{r_i}\}_{i=1,2,\cdots,l_s}$$

得到与共享数据相关的密文 $C_F=\{CF, C, \hat{C}, C_{i1}, C_{i2}\}_{i=1,2,\cdots,l_s}$。

2)关键字密文的生成

假设关键字集的大小为 m，则 $W_1,W_2,\cdots,W_m$ 是一系列关键字值，随机选择 $s,s_1,s_2\in Z_p$，对于 $i=1,2,\cdots,m$，DO 计算 $C_i'=H_2(W_i)^{-s}$，生成关键字密文如下：

$$C_0=e(g,g)^{t_1t_2\omega s}, C_1=g^{t_1(s-s_1)},$$

$$C_2=g^{t_2s_1}, C_3=g^{t_3(s-s_2)}, C_4=g^{t_4s_2},$$

$$\{C_{W_i}=H_2(W_i)^{-s}\}_{i=1,2,\cdots,m}$$

得到关键字密文 $C_W=\{C_0,C_1,C_2,C_3,C_4,\{C_{W_i}\}_{i=1,2,\cdots,m}\}$。

最后，DO 将密文 $CT=\{C_F,C_W\}$ 上传到 CSP。

(4)陷门生成算法 $Trapgen(PK,SK,P)\rightarrow(TP)$

算法输入公共参数 PK、用户的私钥 SK、用户关键字集访问结构 $P=(N,\pi,W_{\pi(i)})$，其中 $\boldsymbol{N}$ 是 $l_o\times k_o$ 的矩阵，l_o 是该访问结构中关键字值的个数，函数 π 将矩阵的行映射为该行对应的通用关键字名，$W_{\pi(i)}$ 为该行对应的关键字值。DU 和 AA 合作执行该算法。首先 AA 随机选择 $z_2,z_3,\cdots,z_{k_o},r_1,r_2\in Z_p$，令向量 $\boldsymbol{v}=(\alpha,z_2,z_3,\cdots,z_{k_o})$，对于 $i=1,2,\cdots,l_o$，计算 $\sigma_i=\boldsymbol{N}_i\cdot\boldsymbol{v}_i$。生成部分搜索关键字陷门如下并通过安全信道传送给 DU：

$$K=g^{r_1t_1t_2+r_2t_3t_4}$$

$$\{\hat{K}_{i1}=g^{t_2\sigma_i}H_2(W_{\pi(i)})^{-r_1t_2}, \hat{K}_{i2}=g^{t_1\sigma_i}H_2(W_{\pi(i)})^{-r_1t_1},$$

$$\hat{K}_{i3}=H_2(W_{\pi(i)})^{-r_2t_4}, \hat{K}_{i,4}=H_2(W_{\pi(i)})^{-r_2t_3}\}_{i=1},\cdots,l_o$$

DU 随机选择盲化值 $\zeta\in Z_p$，将属性私钥中的部分组件盲化：

$$D_2'=D_2^{\zeta}=g^{r\zeta}$$

$$\{D_x'=D_x^{\zeta}=H_1(x)^{r\zeta}\}_{x\in\varphi}$$

盲化值 ζ 由用户自己秘密保留。最后 DU 将完整的陷门 $T=\{(N,\pi),K,\{\hat{K}_{i1},\hat{K}_{i2},\hat{K}_{i3},\hat{K}_{i4}\}_{i=1,2,\cdots,l_o},D_2',\{D_x'\}_{x\in\varphi}\}$ 发送给 CSP。

(5)搜索算法 $Search(PK,TP,CT)\rightarrow(Z/\perp)$

CSP 执行该算法，算法输入公共参数 PK、密文 CT 以及陷门 T。CSP 首先通过和密文一起传送的关键字名集计算出满足陷门中搜索策略$(\boldsymbol{N},\pi)$的一系列最小关键字子集 I_o，然后验证以下等式是否成立：

$$\prod_{i\in I_o}(e(K,C'_{\pi(j)})\cdot e(\hat{K}_{i1},C_1)\cdot e(\hat{K}_{i2},C_2)\cdot e(\hat{K}_{i3},C_3)\cdot e(\hat{K}_{i4},C_4))^{v_i}\stackrel{?}{=}C_0$$

如果上述等式成立，说明密文中的关键字集满足陷门中的搜索策略 P，即搜索到包含查询关键字的文件，进行下一步操作。如果不成立，输出 $\perp$，表示关键字搜索失败。

当搜索成功后，CSP 检查 DU 的属性集 φ 是否满足密文中的访问策略，如果不满足，则输出 $\perp$，表示该用户无法访问文件。如果用户属性集 φ 满足策略，则 CSP 进行部分解密。CSP 定义 $I\subset\{1,2,\cdots,l\}$ 为 $I=\{x:\rho(x)\in\varphi\}$，然后令 $\{\omega_x\in Z_p\}, x\in I$ 为一组常数，使得 $\sum_{x\in I}\omega_x\cdot\lambda_x=t_i$，计算：

$$\begin{aligned}Z&=\prod_{i\in I_s}e(C_{i1},K)\cdot e(C_{i2},K_{\rho(i)})^{\mu_i}\\&=\prod_{i\in I_s}(e(g^{a\lambda_i}H_1(\rho(i))^{-r_i},g^{r\zeta})\cdot e(g^{r_i},H_1(\rho(i))^{r\zeta}))^{\mu_i}\\&=\prod_{i\in I_s}e(g^{\omega\lambda_i},g^{r\zeta})^{\mu_i}\\&=e(g,g)^{ar\zeta t}\end{aligned}$$

CSP 得到部分解密密文 Z 并发送给 DU。

(6)解密算法 $Decrypt(PK,SK,Z)\rightarrow(F)$

解密算法由用户执行,算法输入密文 CT、部分解密密文 Z 和用户私钥 SK。DU 计算得到相应的对称密钥:

$$\frac{C\cdot Z^{1/\zeta}}{e(\hat{C},D_1)}=\frac{ck\cdot e(g,g)^{\beta t}\cdot e(g,g)^{\alpha rt}}{e(g^t,g^{\beta}g^{ar})}=ck$$

从而使用对称密钥 ck 解密得到共享数据文 F。

6 安全性分析

6.1 正确性分析

(1)关键字搜索匹配的正确性

判断:

$$\prod_{i\in I_c}(e(K,C'_{\pi(j)})\cdot e(\hat{K}_{i1},C_1)\cdot e(\hat{K}_{i2},C_2)\cdot e(\hat{K}_{i3},C_3)\cdot e(\hat{K}_{i4},C_4))^{v_i}\overset{?}{=}C_0$$

$$\begin{aligned}
\text{左边}&=\prod_{i\in I_c}(e(K,C'_{\pi(j)})\cdot e(\hat{K}_{i1},C_1)\cdot e(\hat{K}_{i2},C_2)\cdot e(\hat{K}_{i3},C_3)\cdot e(\hat{K}_{i4},C_4))^{v_i}\\
&=\prod_{i\in I_c}(e(g^{r_1t_1t_2+r_2t_3t_4},H_2(\pi(j))^{-s})\cdot e(g^{t_2\sigma_i}H_2(\pi(j))^{-r_1t_2},g^{t_1(s-s_1)})\cdot e(g^{t_1\sigma_i}H_2(\pi(j))^{-r_1t_1},g^{t_2s_1})\cdot e(H_2(\pi(i))^{-r_2t_4},g^{t_3(s-s_2)})\cdot e(H_2(\pi(i))^{-r_2t_3},g^{t_4s_2}))^{v_i}\\
&=\prod_{i\in I_c}(e(g,H_2(\pi(i)))^{-(r_1t_1t_2+r_2t_3t_4)s}\cdot e(g,g)^{t_2\sigma_it_1(s-s_1)}\cdot e(g,H_2(\pi(i)))^{-r_1t_1t_2(s-s_1)}\cdot e(g,g)^{t_1t_2s_1\sigma_i}\cdot e(g,H_2(\pi(i)))^{-r_1t_1t_2s_1}\cdot e(g,H_2(\pi(i)))^{-r_2t_3t_4(s-s_2)}\cdot e(g,H_2(\pi(i)))^{-r_2t_3t_4s_2})^{v_i}\\
&=\prod_{i\in I_c}(e(g,H_2(\pi(i)))^{-(r_1t_1t_2+r_2t_3t_4)s}\cdot e(g,g)^{t_1t_2s\sigma_i}\cdot e(g,H_2(\pi(i)))^{-r_1t_1t_2s}\cdot e(g,H_2(\pi(i)))^{-r_2t_3t_4s})^{v_i}\\
&=\prod_{i\in I_c}(e(g,g)^{t_1t_2s\sigma_i})^{v_i}\\
&=e(g,g)^{t_1t_2s\alpha}
\end{aligned}$$

右边 $=C_0=e(g,g)^{t_1t_2s\alpha}$

综上搜索匹配正确性得证。

(2)解密的正确性

1)部分解密

$$\begin{aligned}
Z&=\prod_{i\in I_s}e(C_{i1},K)\cdot e(C_{i2},K_{\rho(i)})^{\mu_i}\\
&=\prod_{i\in I_s}(e(g^{a\lambda_i}H_1(\rho(i))^{-r_i},g^{r\zeta})\cdot e(g^{r_i},H_1(\rho(i))^{r\zeta}))^{\mu_i}\\
&=\prod_{i\in I_s}e(g^{a\lambda_i},g^{r\zeta})^{\mu_i}\\
&=e(g,g)^{\alpha r\zeta t}
\end{aligned}$$

2)用户解密

$$\frac{C\cdot Z^{1/\zeta}}{e(\hat{C},D_1)}=\frac{ck\cdot e(g,g)^{\beta t}\cdot e(g,g)^{\alpha rt}}{e(g^t,g^{\beta}g^{ar})}=ck$$

综上,解密的正确性得证。

6.2 安全性分析

下面对方案的密文和陷门中的关键字隐私进行安全性分析。若直接将 KP-ABE 转化为可搜索方案,则存在密文中关键字猜测攻击。为了抵抗密文中关键字猜测攻击,本文 EABSE 方案参考文献[15]中的方案首先将每个关键字分为可公开的通用名称和隐藏的关键字值,其次通过“线性拆分”技术[34]隐藏密文中的关键字值以及陷门 LSSS 矩阵中的搜索关键字值。对关键字值密文中的组件进行了“线性拆分”,并根据陷门中的关键字值将密文组件重新随机化,这样可抵抗密文和陷门中的关键字猜测攻击。

但我们发现文献[15]的方案仍然存在云服务器通过双线性对运算从陷门中猜测出搜索关键字的问题,具体如下。

文献[15]的方案中,陷门生成算法 Trapdoor 的输入为公共参数 $pars$、云服务器公钥 pk_s、主密钥 msk 以及 LSSS 访问结构 $(\boldsymbol{M},\rho,\{W_{\rho(i)}\})$,其中 $\boldsymbol{M}$ 是 $l\times n$ 的矩阵,ρ 将矩阵的每一行映射为通用关键字名,$W_{\rho(i)}$ 为该行的对应关键字值。系统随机选择 $y_2,\cdots,y_n,r,r',t_{1,1},t_{1,2},\cdots,t_{l,1},t_{l,2}\in Z_p$,令向量 $\vec{y}=(\alpha,y_2,\cdots,y_n)$,并计算 $T=g^r$,$T'=g^{r'}$,对于 $i=1,\cdots,l$ 计算 $v_i=\boldsymbol{M}_i\cdot\vec{y}$($\boldsymbol{M}_i$ 表示矩阵 $\boldsymbol{M}$ 的第 i 行)。算法输出陷门 $T_{M,\rho}=\{(\boldsymbol{M},\rho),T,T',\{T_{i,1},T_{i,2},T_{i,3},T_{i,4},T_{i,5},T_{i,6}\}_{i\in[1,l]}\}$。其中,

$$\begin{aligned}
&T_{i,1}=g^{v_i}w^{d_1d_2t_{i,1}+d_3d_4t_{i,2}}\\
&T_{i,2}=H(\hat{e}(pk_s,T')^r)\cdot g^{d_1d_2t_{i,1}+d_3d_4t_{i,2}}\\
&T_{i,3}=((u^{W_{\rho(i)}}h)^{t_{i,1}})^{-d_2},T_{i,4}=((u^{W_{\rho(i)}}h)^{t_{i,1}})^{-d_1}\\
&T_{i,5}=((u^{W_{\rho(i)}}h)^{t_{i,2}})^{-d_4},T_{i,6}=((u^{W_{\rho(i)}}h)^{t_{i,2}})^{-d_3}
\end{aligned}$$

云服务器在接收到陷门 $T_{M,\rho}$ 之后,为了猜测陷门中用户欲搜索的关键字 $W_{\rho(i)}$,选取猜测的关键字 W_i,通过以下双线对运算等式来猜测陷门中用户欲搜索的关键字(为了方便计算,忽略陷门中云服务的公私钥对):

$$e(T_{i,3}T_{i,4}T_{i,5}T_{i,6},g)\overset{?}{=}e(T_{i,2}^{-1},u^{W_i}h)$$

$$\begin{aligned}
\text{左边}&=e(T_{i,3}T_{i,4}T_{i,5}T_{i,6},g)\\
&=e(u^{W_{\rho(i)}}h,g)^{-(d_1d_2t_{i,1}+d_3d_4t_{i,2})}\\
\text{右边}&=e(T_{i,2}^{-1},u^{W_i}h)\\
&=e(g^{-d_1d_2t_{i,1}-d_3d_4t_{i,2}},u^{W_i}h)\\
&=e(u^{W_i}h,g)^{-(d_1d_2t_{i,1}+d_3d_4t_{i,2})}
\end{aligned}$$

根据上述计算,若等式成立,则表示云服务器猜测的关键字 W_i 与陷门中用户欲搜索的关键字 $W_{\rho(i)}$ 相等,即用户欲搜索的关键字泄漏而算法无法抵抗关键字猜测攻击。而本文 EABSE 方案中的陷门经过改进,使得云服务器无法通过陷门中的组件相乘和双线性配对运算猜测出用户欲搜索的关键字,抵抗了陷门中的关键字猜测攻击。

定理 1 基于 DBDH 和(q-2)假设,本文 EABSE 方案在关键字攻击下是选择性不可区分的(IND-CKA 安全)。

证明:通过一系列安全游戏来证明安全性。其中安全游戏 $Game_0$ 与原始安全游戏相同,而 $Game_1$ 在陷门生成的实体方面与 $Game_0$ 不同。本文方案通过证明不存在外部敌手 $\mathcal{A}$ 可以区分安全游戏 $Game_0$ 和 $Game_1$ 来证明这一结论,并构建挑战者 $\mathcal{B}$ 来解决 DBDH 假设。

(1)敌手 $\mathcal{A}$ 将挑战关键字集 $W_0^*=\{W_{0,1}^*,W_{0,2}^*,\cdots,W_{0,m}^*\}$ 和 $W_0^*=\{W_{1,1}^*,W_{1,2}^*,\cdots,W_{1,m}^*\}$ 发送给挑战者 $\mathcal{B}$。

(2)初始化。挑战者 $\mathcal{B}$ 执行 Setup 算法,生成系统公共参数和主密钥。

(3)阶段 1。由于挑战者 $\mathcal{B}$ 拥有主密钥,因此 $\mathcal{B}$ 可以根据任意搜索策略输出陷门。如果敌手 $\mathcal{A}$ 根据 W_β^* 可满足的搜索策略生成陷门查询,则 $\mathcal{B}$ 执行 Trapgen 算法生成陷门。

(4)挑战。挑战者 $\mathcal{B}$ 基于关键字集 W_β^* 执行 Encrypt 算法,生成挑战密文 CT^*,并发送给敌手 $\mathcal{A}$。

(5)阶段 2。与阶段 1 相同。

(6)猜测。敌手 $\mathcal{A}$ 对 β 输出猜想 β'。

如果敌手 $\mathcal{A}$ 能够以不可忽略的概率区分游戏 $Game_0$ 和 $Game_1$，则挑战者在打破 DBHD 问题时具有不可忽略的概率。

令 Z 为 G 上的随机元素，定义以下游戏，并将挑战密文发送给敌手 $\mathcal{A}$。

(1) $Game_0$：挑战密文为 $(C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, \{C_{W_i}^*\}_{i=1,2,\cdots,m})$。

(2) $Game_1$：挑战密文为 $(Z, C_1^*, C_2^*, C_3^*, C_4^*, \{C_{W_i}^*\}_{i=1,2,\cdots,m})$。

定理 2 在(q－2)假设下，敌手 $\mathcal{A}$ 区分游戏 $Game_0$ 和 $Game_1$ 的多项式时间的优势可忽略。

证明：假设敌手 $\mathcal{A}$ 可以区分游戏 $Game_0$ 和 $Game_1$，则可以构建挑战者 $\mathcal{B}$ 解决(q－2)问题。

(1)敌手 $\mathcal{A}$ 将挑战关键字集 $W_0^* = \{W_{0,1}^*, W_{0,2}^*, \cdots, W_{0,m}^*\}$ 和 $W_0^* = \{W_{1,1}^*, W_{1,2}^*, \cdots, W_{1,m}^*\}$ 发送给挑战者 $\mathcal{B}$。

(2)初始化。挑战者 $\mathcal{B}$ 设置 $\alpha = xy$，并随机选择 $\gamma \in \{0, 1\}$，$a, t_1, t_2, t_3, t_4 \in Z_p$，计算生成公共参数 $PK = \{e(g,g)^{t_1 t_2 \alpha}, e(g,g)^{\beta}, g^{a}, g^{t_1}, g^{t_2}, g^{t_3}, g^{t_4}\}$。

(3)阶段 1 和阶段 2。挑战者 $\mathcal{B}$ 基于搜索策略 $(N, \pi, \{\pi(i)\})$ 生成陷门，且 W_0^* 和 W_1^* 无法满足该搜索策略。挑战者随机选择 $z_2, \cdots, z_{k_o}, r_1, r_2 \in Z_p$，令向量 $\boldsymbol{v} = (\alpha, z_2, \cdots, z_{k_o})$，对于 $i = 1, 2, \cdots, l_o$，计算 $\sigma_i = N_i \cdot v_i$，输出陷门 $T = \{K, \{\hat{K}_{i1}, \hat{K}_{i2}, \hat{K}_{i3}, \hat{K}_{i4}\}_{i=1,2,\cdots,l_o}\}$ 如下：

$$K = g^{r_1 t_1 t_2 + r_2 t_3 t_4}$$

$$\hat{K}_{i1} = g^{t_2 \sigma_i} H_2(W_{\beta,m}^*)^{-r_1 t_2}$$

$$\hat{K}_{i2} = g^{t_1 \sigma_i} H_2(W_{\beta,m}^*)^{-r_1 t_1}$$

$$\hat{K}_{i3} = H_2(W_{\beta,m}^*)^{-r_2 t_4}$$

$$\hat{K}_{i4} = H_2(W_{\beta,m}^*)^{-r_2 t_3}$$

(4)挑战。挑战者 $\mathcal{B}$ 生成挑战密文，随机选择 $s, s_1, s_2 \in Z_p$，输出挑战密文 $C_W^* = \{C_0^*, C_1^*, C_2^*, C_3^*, C_4^*, \{C_{W_i}^*\}_{i=1,2,\cdots,m}\}$ 如下：

$$C_0^* = Z$$

$$C_1^* = g^{t_1(s-s_1)}$$

$$C_2^* = g^{t_2 s_1}$$

$$C_3^* = g^{t_3(s-s_2)}$$

$$C_2^* = g^{t_4 s_2}$$

$$C_{W_m}^* = H_2(W_{\beta,m}^*)^{-s}$$

(5)阶段 2。与阶段 1 相同。

(6)猜测。敌手 $\mathcal{A}$ 输出猜想 β'。如果 $Z = e(g,g)^{t_1 t_2 \alpha s}$，则敌手的游戏模拟与原始游戏相同；如果 Z 随机选取，则敌手 $\mathcal{A}$ 的优势可以忽略。因此，如果敌手 $\mathcal{A}$ 以不可忽略的概率区分游戏 $Game_0$ 和 $Game_1$，则挑战者 $\mathcal{B}$ 打破(q－2)假设具有不可忽略的概率。

7 性能分析和实验仿真

7.1 功能分析

从功能性方面对比本文方案 EABSE 与目前支持“AND”“OR”关键字搜索策略的多关键字可搜索加密方案[13-15]如表 1 所列。首先，与文献[13-14]相比，本文方案与文献[15]中的方案基于素数阶群，素数阶群上的元素长度较文献[13-14]中的复合阶群长，在计算成本和存储开销方面有显著的优势。而本文方案和文献[15]相比，攻击者无法通过双线性对运算从陷门中猜测出关键字值，而文献[15]无法抵抗云服务器的关键字值猜测攻击。由于云服务器只是一个半信任的实体，该方案存在关键字泄漏问题。另外文献[13-14]中，关键字的数量在初始化阶段限定，且公共参数的大小与关键字数量呈线性关系；而本文方案与文献[15]支持无界关键字搜索，公共参数的大小与关键字数量无关，关键字数量不受限制，更适用于实际场景。

表 1 本文方案与文献[13-15]中方案的功能性比较

Table 1 Comparison with schemes in literature [13-15] on functionality

Scheme	Bilinear Group	Keywords disclosure	Unbounded keywords
Lai 等[13]	Composite	Yes	No
Lv 等[14]	Composite	No	No
Cui 等[15]	Prime	Yes to CSP	Yes
EABSE	Prime	No	Yes

7.2 理论分析

本文方案 EABSE 与文献[13-15]方案中的存储和计算开销的对比结果如表 2 和表 3 所列。文献[13-14]是基于复合阶群构造的，文献[15]和本文方案是基于素数阶群构造的。素数阶群在参数大小和计算效率上有明显的优势。

表 2 各方案存储、通信开销的比较

Table 2 Comparison of each scheme on storage costs

Scheme	Lai 等[13]	Lv 等[14]	Cui 等[15]	EABKS
$\lvert PK\rvert$	$(n+5)\lvert G\rvert + \lvert G_T\rvert$	$(n+4)\lvert G\rvert + \lvert G_T\rvert$	$9\lvert G\rvert + \lvert G_T\rvert$	$5\lvert G\rvert + 2\lvert G_T\rvert$
$\lvert MSK\rvert$	$(n+4)\lvert Z_P\rvert$	$(n+2)\lvert Z_P\rvert$	$5\lvert Z_P\rvert$	$6\lvert Z_P\rvert$
$\lvert CT\rvert$	$(w+1)\lvert G\rvert + \lvert G_T\rvert$	$(w+1)\lvert G\rvert + \lvert G_T\rvert$	$(5w+1)\lvert G\rvert + \lvert G_T\rvert$	$(w+4)\lvert G\rvert + \lvert G_T\rvert$
$\lvert TD\rvert$	$2l\lvert G\rvert$	$3l\lvert G\rvert$	$(6l+2)\lvert G\rvert$	$(4l+1)\lvert G\rvert$

表 3 各方案计算开销的比较

Table 3 Comparison of each scheme on computation costs

Scheme	Lai 等[13]	Lv 等[14]	Cui 等[15]	EABKS
Encrypt	$(2w+2)E$	$(w+2)E+P$	$(7w+2)E$	$(w+5)E$
Trapgen	$4lE$	$4lE$	$(16l+2)E$	$(6l+1)E$
Search	$\chi E + 2\chi P$	$\chi E + 2\chi P$	$(\chi+1)E + (6\chi+1)P$	$\chi E + 5\chi P$

令 $\lvert G\rvert, \lvert G_T\rvert, \lvert Z_P\rvert$ 分别表示 G, G_T, Z_P 中元素的长度，l 表示陷门中搜索策略关键字的数量，w 表示关键字密文中关键字的数量，n 表示文献[13-14]系统初始化时设置的最大关键字数量。表 2 比较了 4 种方案公开参数大小($\lvert PK\rvert$)、主密钥大小($\lvert MSK\rvert$)、密文大小($\lvert CT\rvert$)以及陷门大小($\lvert TD\rvert$)。数据的加密应包括数据文件的加密和关键字的加密，但由于文献[13-15]都忽略了数据文件的加密，为了便于对比方案性能，在表 2 和表 3 的性能比较中，本文方案也不进行数据文件的加密，只考虑关键字的加密。与文献[13-14]相比，本文方案与文献[15]在公开参数和主密钥方面的存储开销较小，在密文和陷门通信的开销方面较大，这是由于本文方案和文献[15]支持无界关键字大小，而文献[13-14]只支持固定关键字大小。另外本文方案在存储和通信开销方面均小于文献[15]。

对于计算开销的比较，为了方便起见，本文主要考虑了耗时的指数运算和双线对运算，令 E 表示群的指数运算时间，P 表示双线性配对计算时间，χ 为满足陷门中搜索策略 (N,π) 的一系列最小关键字子集 $I_o=\{I_1,\cdots,I_\chi\}$ 中关键字的个数。表 3 列出了 4 种方案的 Encrypt 算法、Trapgen 算法和 Search 算法的计算开销。从表 3 可以看出，本文方案在加密、陷门生成和搜索匹配阶段的计算开销均优于文献[15]。

7.3 实验分析

由于文献[13-14]是基于复合阶群构造的，因此本节实验仅将本文方案与基于素数阶群的文献[15]进行比较。为了便于比较，实验数据与文献[15]相同，每个关键字都包含一个通用名称和对应的关键字值，例如关键字名“Illness”“Position”“Affiliation”对应的关键字值分别为“Diabetes”“Doctor”“City”。为了表达方便，关键字值用整数值代替，例如关键字“Illness=6”表示“Illness=Diabetes”。通过这种方式，实验首先生成了一个包含 50 个关键字的关键字集，然后用该关键字集加密生成 80000 个关键字密文。对于陷门的生成，与文献[15]相同，从关键字集中随机选取 2～10 个关键字来生成随机的搜索策略（在实际应用中，一个搜索查询中的关键字数目通常不超过 10 个）。最后，实验对包含 10 个关键字的陷门执行搜索算法，检索出满足陷门中搜索策略的密文，将其部分解密并把部分解密密文输出给用户。

实验的代码实现是基于 CP-ABE 工具包和 Java 配对的密码学（Java Pairing-Based Cryptography，JPBC）库[35-36]，实验程序均采用 Java 语言编写，并在 IntelliJIDEA 下运行，微机环境为 Windows 操作系统 Intel(R) Core(TM) i5-8200U CPU2.4GHz 和 8.00GB 内存。实验利用 JPBC 中提出的基于椭圆曲线 $y^2=x^3+x$ 构造的 512 位椭圆曲线群。G 和 G_T 中元素的大小是 128 字节。

实验对比了两个方案的 3 个主要算法（陷门生成、关键字加密以及关键字搜索算法）的计算开销，结果如图 2－图 4 所示。根据实验结果可以看出，两个算法的计算开销都与关键字数量呈线性关系，而本文方案 3 个算法的计算开销均低于文献[15]。

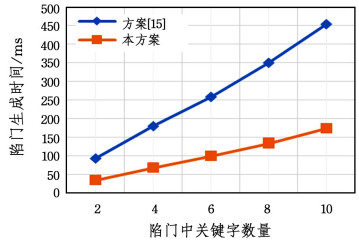

图 2 陷门生成的计算开销比较

Fig. 2 Comparison of trapdoor generation costs

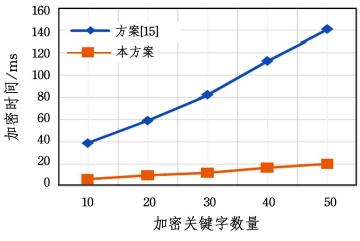

图 3 关键字加密的计算开销比较

Fig. 3 Comparison of encryption computation costs

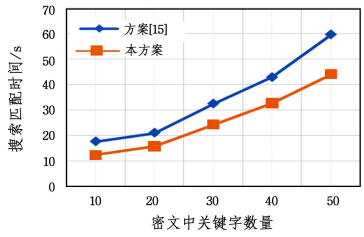

图 4 关键字搜索的计算开销比较

Fig. 4 Comparison of computation search costs

结束语 本文提出了一种针对云环境下可支持任意表达的基于属性可搜索加密方案。该方案通过在陷门中嵌入搜索策略，实现了更加细粒度的搜索；同时将关键字拆分为关键字名和关键字值，关键字值通过“线性拆分”技术隐藏在密文中，而关键字名随密文公开，在提高匹配搜索效率的同时保证了方案的安全性。本文通过理论和实验验证了该方案的可行性。此外，为满足实际应用的需要以及解决云环境下的安全问题，我们需要考虑利用区块链技术设计更安全、更高效的可搜索方案，因此在未来的工作中，将对区块链上的基于属性可搜索加密方案进行研究。

参 考 文 献

[1] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]// Proceedings of 2000 IEEE Symposium on Security and Privacy. Berkeley, CA: IEEE, 2000: 44-55.

[2] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[C]// Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2004: 506-522.

[3] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption. Improved definitions and efficient constructions[C]// Proceedings of the 2006 ACM Computer and Communication Security. New York: ACM, 2006: 79-88.

[4] LI J, SHI Y, ZHANG Y. Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage[J]. International Journal of Communication Systems, 2017, 30(1): 2933-2947.

[5] MIAO Y, MA J, LIU X, et al. Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing[J]. IEEE Transactions on Services Computing, 2017, 17(99): 1427-1441.

[6] SWAMINATHAN A, MAO Y, SU G M, et al. Confidentiality-preserving rank-ordered search[C]// Proceedings of the 2007 ACM Workshop Storage Security and Survivability. Alexandria, VA: ACM, 2007: 7-12.

[7] WANG C, CAO N, REN K, et al. Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data[J]. IEEE Transactions on Parallel & Distributed Systems, 2011, 23(8): 1467-1479.

[8] ZERR S, OLMEDILLA D, NEJDL W, et al. Zerber+R: Top-k retrieval from a confidential index[C]// Proceedings of International Conference on Extending Database Technology. 2009: 439-449.

[9] DAN B, WATERS B. Conjunctive, subset, and range queries on encrypted data[C]// Proceedings of 4th Theory of Cryptography Conference. Berlin, Springer, 2007: 535-554.

[10] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure func-

tional encryption:Attribute-based encryption and (hierarchical) inner product encryption[C]// Proceedings of Annual International Conference on Theory and Applications of Cryptographic Technology. Berlin,Springer,2010:62-91.

[11] MIAO Y,MA J,LIU X,et al. Practical Attribute-Based Multi-Keyword Search Scheme in Mobile Crowdsourcing[J]. IEEE Internet of Things Journal,2018,5(4):3008-3018.

[12] MIAO Y,MA J,LIU X,et al. VCKSM: Verifiable conjunctive keyword search over mobile e-health cloud in shared multi-owner settings[J]. Pervasive and Mobile Computing,2017,40:205-219.

[13] LAI J,ZHOU X,DENG R H,et al. Expressive search on encrypted data[C]// ACM Sigsac Symposium on Information. ACM,2013:243-251.

[14] LV Z,HONG C,ZHANG M,et al. Expressive and Secure Searchable Encryption in the Public Key Setting[J]. 2014:364-376.

[15] CUI H,WAN Z,DENG R,et al. Efficient and Expressive Keyword Search Over Encrypted Data in the Cloud[J]. IEEE Transactions on Dependable & Secure Computing,2018,15(3):409-422.

[16] HAO J,LIU J,WANG H,et al. Efficient Attribute-based Access Control with Authorized Search in Cloud Storage[J]. IEEE Access,2019,7:182772-182783.

[17] SHEN C,LU Y,LI J. Expressive Public-Key Encryption with Keyword Search:Generic Construction from KP-ABE and an Efficient Scheme over Prime-Order Groups[J]. IEEE Access,2020,8:93-103.

[18] SAHAI A,WATERS B. Fuzzy Identity-Based Encryption[M]. Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer,2005:457-473.

[19] DAN B,FRANKLIN M. Identity-Based Encryption from the Weil Pairing[M]. Society for Industrial and Applied Mathematics,2003:235-252.

[20] GOYAL V,PANDEY O,SAHAI A,et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proceedings of ACM Conference on Computer and Communications Security. ACM,2006:89-98.

[21] PARK D J,KIM K,LEE P J. Public Key Encryption with Conjunctive Field Keyword Search[C]// Proceedings of Information Security Applications,5th International Workshop,WISA 2004. Jeju Island,Korea,2004:73-86.

[22] HAN F,QIN J,ZHAO H,et al. A general transformation from KP-ABE to searchable encryption[J]. Future Generation Computer Systems,2014,30(Jan.):107-115.

[23] ABDALLA M,BELLARE M,CATALANO D,et al. Searchable Encryption Revisited: Consistency Properties,Relation to Anonymous IBE,and Extensions[C]// Annual International Cryptology Conference. Berlin:Springer,2005:205-222.

[24] KAUSHIK K,VARADHARAJAN V,NALLUSAMY R. Multi-user Attribute-based Searchable Encryption[C]// IEEE International Conference on Mobile Data Management. IEEE,2013:200-205.

[25] XIONG A P,GAN Q X,et al. A searchable encryption of CP-ABE scheme in cloud storage[C]// Proceedings of the 10th International Computer Conference on Wavelet Active Media Technology (ICCWAMTIP'13). USA:IEEE,2013:345-349.

[26] HE H,ZHANG J,LI P,et al. A lightweight secure conjunctive keyword search scheme in hybrid cloud[J]. Future Generation Computer Systems,2019,93:727-736.

[27] WANG S P,JIA S S,ZHANG Y L,et al. Verifiable and Multi-Keyword Searchable Attribute-Based Encryption Scheme for Cloud Storage[J]. IEEE Access,2019,7:50136-50147.

[28] SUN J,REN L,WANG S,et al. Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage[J]. IEEE Access,2019,7:66655-66667.

[29] LIU X,LU T,HE X,et al. Verifiable Attribute-Based Keyword Search Over Encrypted Cloud Data Supporting Data Deduplication[J]. IEEE Access,2020,8(99):52062-52074.

[30] LIU X,YANG X. Verifiable Multi-keyword Search Encryption Scheme with Anonymous Key Generation for Medical Internet of Things[J]. IEEE Internet of Things Journal(Early Access),2021,8:1-13.

[31] BAEK J,SAFAVI-NAINI R,SUSILO W. Public Key Encryption with Keyword Search Revisited[C]// Proceedings of the International Conference on Computational Science and Its Applications,Part I. Berlin:Springer,2008:1249-1259.

[32] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Haifa:Israel Institute of Technology,1996.

[33] ROUSELAKIS Y,WATERS B. New Constructions and Proof Methods for Large Universe Attribute-Based Encryption[C]// ACM Sigsac Conference on Computer & Communications Security. ACM,2013:463-473.

[34] BOYEN X,WATERS B. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles)[C]// Proceedings of the 26th Annual International Conference on Advances in Cryptology. Berlin:Springer,2006:290-307.

[35] SHOUP V. A proposal for an iso standard for public key encryption (version 2.1)[OL]. http://eprint.iacr.org/2001/112.

[36] CARO A D,IOVINO V. jPBC:Java pairing based cryptography[C]// 2011 IEEE Symposium on Computers and Communications (ISCC). Kerkyra,2011:850-855.

GAO Shi-yao, born in 1996, postgraduate. His main research interests include information security and modern cryptography.

CHEN Yan-li, born in 1969, Ph.D, professor. Her main research interests include network security and computer architecture.

(责任编辑:喻藜)