计算机科学
COMPUTER SCIENCE

云环境下基于属性策略隐藏的细粒度高效可搜索加密方案

周艺华, 李美奇, 扈新宇, 杨宇光

引用本文

周艺华, 李美奇, 扈新宇, 杨宇光.云环境下基于属性策略隐藏的细粒度高效可搜索加密方案[J]. 计算机科学, 2023, 50(7): 339-346.

ZHOU Yihua, LI Meiqi, HU Xinyu, YANG Yuguang. Fine Grained and Efficient Searchable Encryption Scheme Based on Attribute Policy Hiding inCloud Environment [J]. Computer Science, 2023, 50(7): 339-346.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220500238

云环境下基于属性策略隐藏的细粒度高效可搜索加密方案

周艺华　李美奇　扈新宇　杨宇光
北京工业大学信息学部　北京 100124
可信计算北京市重点实验室　北京 100124
(zhouyh@bjut.edu.cn)

摘　要　基于属性的加密为存储在云中的外包数据提供了灵活且细粒度的访问控制。传统的基于属性的密文策略加密方案(CP-ABE)的访问策略常以明文形式出现,极易暴露用户的隐私敏感信息。另外,由于属性的加入,在加解密以及搜索阶段的相关计算和存储开销与属性数量呈线性关系,而且策略隐藏也会增加后续的计算开销。这些都难以满足云环境下具有隐私保护的安全高效可搜索加密的实际需求。针对上述问题,提出了一种同时支持策略隐藏与密文长度恒定的可搜索加密方案。该方案基于多值通配符与门策略,实现了密文长度恒定,并且具有固定的加解密和搜索开销,减少了用户的计算开销和云端对密文的存储开销。将访问策略中的属性通过加密完全隐藏,在搜索时使用布隆过滤器判断用户是否拥有访问策略中的相关属性,保护了用户隐私,也提高了计算效率。所提方案在 q-BDHE 假设下满足 IND-CPA 安全。安全性分析与实验结果表明了所提方案的安全性、高效性和可行性,其是一个高效的关键词搜索方案,在云环境与物联网中具有较好的应用前景。

关键词:属性基加密;策略隐藏;密文恒定;关键词搜索;云环境
中图法分类号　TP309

Fine Grained and Efficient Searchable Encryption Scheme Based on Attribute Policy Hiding in Cloud Environment

ZHOU Yihua, LI Meiqi, HU Xinyu and YANG Yuguang
Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

Abstract　Attribute based encryption provides flexible and fine-grained access control for outsourced data stored in the cloud. The traditional attribute based ciphertext policy encryption scheme(CP-ABE), whose access policy often appears in the form of plaintext, is very easy to expose users' sensitive privacy information. In addition, due to the addition of attributes, the related calculation and storage costs in the encryption, decryption and search stages are linear with the number of attributes, and policy hiding will also increase the subsequent calculation costs. These are difficult to meet the actual needs of secure and efficient searchable encryption with privacy protection in cloud environment. To solve the above problems, a searchable encryption scheme supporting both policy hiding and constant ciphertext length is proposed. Based on the multi-valued wildcard and gate strategy, the scheme realizes the constant length of the ciphertext, and has a fixed encryption, decryption and search overhead, reducing users' computing overhead and the storage overhead of the ciphertext in the cloud. The attributes in the access policy are completely hidden by encryption, and the bloom filter is used to judge whether the user has the relevant attributes in the access policy during the search, which not only protects users' privacy, but also improves the computing efficiency. The scheme meets the IND-CPA safety under the assumption of q-BDHE. Security analysis and experimental results show that the scheme is safe, efficient and feasible. It is an efficient keyword search scheme, and has a good application prospect in cloud environment and Internet of Things.

Keywords　Attribute based encryption, Policy hiding, Constant ciphertext, Keyword search, Cloud environment

1　引言

随着云计算和物联网的出现和发展,云辅助外包技术变得越来越普遍。特别是对于计算和存储能力有限的设备,用户往往需要将其数据存储到云端。然而,这样会增加用户隐私被泄露的可能。因此,用户在上传数据前需要对其进行

到稿日期:2022-05-25　返修日期:2022-10-10
基金项目:国家自然科学基金(62071015)
This work was supported by the National Natural Science Foundation of China(62071015).
通信作者:李美奇(limeiqi@emails.bjut.edu.cn)

加密，并加入一些访问控制策略来保护隐私。2005 年，Sahai 等[1]首次将属性应用到加密方案中，提出了细粒度的基于属性的加密(Attribute-based Encryption，ABE)方案。数据拥有者可以将加密数据的访问控制策略制定为基于属性的布尔公式，只有满足属性的用户才可解密出相关明文。受 ABE 的启发，Sun 等[2]提出了 ABE 的关键词可搜索方案。

目前，在 ABE 方案[3-7]中，基于密文策略的属性基加密(Ciphertext policy ABE，P-ABE)方案更适合外包存储且可搜索的云环境，数据的访问策略是由数据拥有者控制的。它既保护了用户的数据隐私，也支持细粒度的访问控制。Waters 等[8]的方案允许数据拥有者根据系统属性的任何访问公式来指定访问策略。Liu 等[9]的 CP-ABE 方案使用了代理重加密技术，可以直接在密文上进行访问策略的转换，并且减小了用户端的计算开销。Shao 等[10]的 CP-ABE 方案使用索引树和编辑距离实现了模糊搜索，即使搜索关键词不是完全正确的，也可以实现搜索匹配；并使用解密外包减小用户开销。为了实现解密操作，大多数方案[8-12]的访问策略都是公开嵌在密文上的，这容易被得到密文的人或服务器推测得到密文和用户的相关隐私信息，若被居心叵测的攻击者所利用，用户的人身财产安全则会受到威胁。

针对策略隐藏问题，为了实现访问策略的隐藏，同时让用户知道解密涉及的属性；2008 年，Nishide 等[13]提出了基于属性的部分隐藏策略加密的概念，并提出了两种隐藏 CP-ABE 策略的方案；Lai 等[14]构造了一种完全安全的内积加密来隐藏访问策略，但仅隐藏了访问策略中的属性值的方案[13-17]并不是很安全，属性名在某种程度上也会泄露用户的隐私信息；Arkin 等[18]构造了一种基于线性秘密访问结构的选择性策略隐藏方案，并不是隐藏所有的属性，而是自定义选择一些容易暴露用户隐私的敏感属性进行隐藏；Zhang 等[19]通过隐藏向量加密来实现访问策略的完全隐藏，但在后续的用户解密阶段，增加了用户的计算开销。本文在用户解密阶段使用哈希计算来确定数据拥有者的访问策略，减小了计算开销。

针对密文长度问题，由于基于属性的访问策略的引入，在 ABE 方案[8-19]中，密文长度和密钥长度随着策略中涉及的属性数量的增加而而增加。大量的密文和密钥使得系统的计算开销和通信开销很大。同时，在解密阶段，大量的配对运算会产生巨大的计算成本。遗憾的是，这种大量的计算需要用户拥有强大的计算能力，对资源受限的用户或设备很不友好。Gan 等[20]将基于属性的部分策略隐藏加密方案应用于车载雾计算，满足自适应性安全，但是也存在方案的密文长度过大而不适合资源受限的设备的问题。文献[21]提出了一种基于门限结构的密文恒定方案，并可将其扩展到较高表达能力的加权门限策略上，该方案满足在标准模型下的选择明文攻击。Guan 等[22]提出了基于物联网系统的恒定密文长度方案，满足自适应安全。Wei 等[23]提出了一种基于层次属性的定长密文访问控制方案，在加密和解密算法中的计算成本较低。上述密文长度恒定的方案均是基于密文进行加解密，并没有对密文的关键词搜索问题进行研究。

针对上述的策略隐私泄露与密文的计算存储开销太大的问题，本文提出了一种同时支持策略隐藏和密文长度恒定的可搜索加密方案。本文的贡献如下：

(1)隐藏的访问策略。所提方案基于多值通配符与门策略，将属性名和属性值同时嵌入到密文中，实现访问策略的完全隐藏；在搜索和解密过程中，通过布隆过滤器判断用户是否拥有访问策略中的属性，使用哈希计算来减小用户的额外计算开销。

(2)恒定的密文长度。在加密阶段得到的密文长度是固定的，不会随访问策略中的属性数量的增加而增加，并且在搜索和解密阶段使用的双线性配对次数也是恒定的，有效降低了用户端的计算开销和云端的密文存储与搜索开销。

(3)细粒度且高效快速的关键词搜索。采用多值通配符与门策略，以丰富用户访问策略的表达；在关键词搜索阶段仅需两次双线性配对即可得到搜索结果。

2 预备知识

2.1 双线性映射

假设群 G 与群 G_T 是阶为素数 p 的循环群，g 是群 G 的生成元，存在双线性映射 $e:G\times G\rightarrow G_T$，并满足以下性质。

(1)双线性。对于任意的 $x,y\in G,a,b\in Z_p$，存在 $e(x^a,y^b)=e(x^b,y^a)=e(x,y)^{ab}$。

(2)非退化性。存在 $x,y\in G$，使 $e(x,y)\neq 1$。

(3)可计算性。对于所有的 $x,y\in G$，存在有效的算法来计算 $e(x,y)$。

2.2 与门访问结构

本文采用了一种支持多值属性和通配符的“AND”门访问策略[24]。假设全局属性集为 $U=\{att_1,att_2,\cdots,att_n\}$，总共有 n 个属性；每个属性 att_i 能够拥有多个属性值 $V_i=\{v_{i,1},v_{i,2},\cdots,v_{i,m_i}\}$，$m_i=|V_i|$；访问策略 $W=\{w_1,w_2,\cdots,w_n\}$，其中 $w_i\in\{V_i,*\}$，“$*$”表示用户可以拥有属性 att_i，也可以没有；V_i 表示用户拥有的属性的具体值。下标索引集 I_W 为访问策略 W 中非“$*$”的属性下标的集合，$I_w=\{i\mid 1\leqslant i\leqslant n,w_i\neq *\}$；用户属性列表为 $S=\{s_1,s_2,\cdots,s_n\},s_i\in\{V_i\}$。在进行访问策略匹配时，若 $i\in I_W$ 且 $s_i=w_i$，则说明用户属性集 S 满足访问策略 W。

2.3 布隆过滤器

布隆过滤器(Bloom Filter，BF)是由 Bloom[25]于 1970 年提出的，用于快速测试并判定一个元素是否是某个集合的成员，是一种基于哈希映射的快速查找算法。

BF 由一个长 m 的位数组和 k 个随机独立的哈希函数组成，通过哈希映射将元素映射到位数组中。哈希函数定义为：$h:\{0,1\}^*\rightarrow[1,m],1\leqslant i\leqslant k$。初始化时，所有位数组均为 0；插入时，对该元素进行哈希，得到 k 个位置，将位数组中的这几个位置置为 1，若为 1 则不变；查找时，对查找元素进行哈希得到 k 个位置，比对位数组中这几个位置是否全为 1，若全为 1，则说明该元素可能在 BF 中，否则该元素一定不在 BF 中。

BF 在一定程度上会出现哈希冲突，导致误判的情况。这时需要在 BF 的位数组长度以及哈希个数与误判率之间找到一个平衡点。根据可以接受的误判率和需要判断的元素个数，选择适当的 m 值和 k 值。图 1 给出了集合$\{a,b\}$的 BF

示意图,其中 $m=12$,$k=3$。

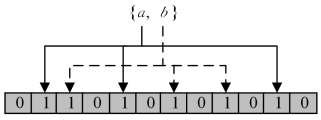

图 1 布隆过滤器

Fig. 1 Bloom filter

2.4 困难问题假设

决策性 q-BDHE 假设[26]如下。设随机元素 $T\in G_T$,给定 $\vec{y}_{g,a,q}=(g_1,g_2,\cdots,g_q,g_{q+2},\cdots,g_{2q})$,其中 $g_i=g^{a^i}$,$\alpha\in Z_p^*$,如果一个输出为 $\mu\in\{0,1\}$的算法 A 能以优势 ε 解决判定性 q-BDHE 问题,则式(1)成立:

$$|\Pr[A(g,h,\vec{y}_{g,a,q},e(g_{q+1},h))=0]-\Pr[A(g,h,\vec{y}_{g,a,q},T)=0]|\geqslant\varepsilon \tag{1}$$

若在多项式时间内,攻击者无法以不可忽略的优势区分 $(g,h,\vec{y}_{g,a,q},e(g_{q+1},h))$和$(g,h,\vec{y}_{g,a,q},T)$,则表明 G_1 和 G_T 上的决策性 q-BDHE 问题是困难的。

2.5 符号说明

系统方案中所涉及的一些符号和对应的说明如表 1 所列。

表 1 符号说明

Table 1 Symbol description

符号	说明
λ	安全参数
G,G_T	阶为素数 p 的乘法循环群
Z_P	一个有限域,其中 P 是一个大的素整数
g	群 G 的生成元
PK	系统的公共参数
MSK	系统的主密钥
H_0,H_1,H_2	抗合谋的哈希函数
U,n	系统的属性集合,n 为属性个数
V_i,m_i	属性 att_i 的属性值集合,m_i 为属性值个数
$h_1,h_2,\cdots,h_k$	BF 的 k 个随机独立的哈希函数
S	用户的属性集合
W	拥有者的访问策略集合
I_W	访问策略 W 对应的下标集合
Q,Q'	文件索引关键字集合和用户查询关键字集合
SK	用户的私钥
M	文件的明文
C	文件的对应密文
I	文件的索引密文
BF_W	文件的访问策略 W 对应的布隆过滤器
T	用户的搜索陷门

3 系统与安全模型的定义

3.1 系统模型

本系统主要包括 4 个实体,分别是数据拥有者(Data Owner,DO)、数据使用者(Data User,DU)、云服务提供商(Cloud Server Provider,CSP)、属性授权中心(Attribute Authorization,AA)。系统的模型及其流程如图 2 所示。

(1)属性授权中心,即一个完全可信的实体,负责生成系统的主密钥、公共参数和用户私钥。此外,还负责为用户的属性分发属性密钥。

(2)数据拥有者,即加密数据的拥有者。数据拥有者设置文档的访问策略并对其进行隐藏,对关键字加密,生成关键字索引,与加密后的密文一并上传到云服务器。

(3)数据使用者,即需要从云端搜索下载数据的用户。每一个用户都拥有 AA 授权的与其属性集相关的私钥。使用私钥生成带有关键字及属性的搜索陷门,将其发送给云服务器。搜索成功时,会收到 CSP 返回的搜索结果,使用私钥进行解密会得到相应的明文。

(4)云服务提供商,提供云端存储及计算服务的服务提供商。存储服务:云服务器负责存储 DO 发送的密文及索引数据。计算服务:当收到 DU 发送的陷门时,会进行搜索服务,检查用户属性值是否满足 DO 的访问策略,查询关键字是否与密文数据的关键词索引相匹配,若两者均满足,则云端会将搜索到的密文数据返回给用户。

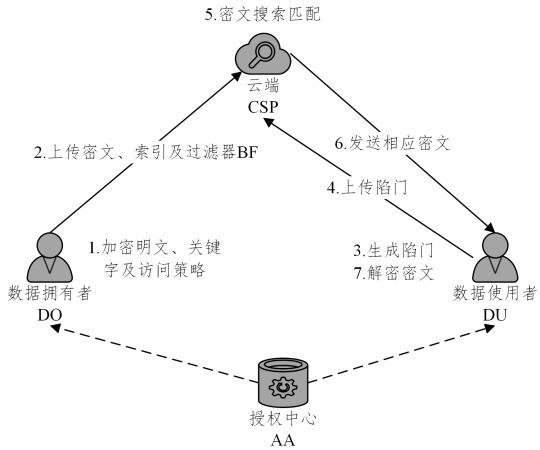

图 2 系统框架图

Fig. 2 System frame diagram

3.2 算法的形式化定义

本文方案由以下 6 种算法组成,具体如下。

(1)$SetUp(1^\lambda)\rightarrow(PK,MSK)$:该算法由 AA 执行,输入为安全参数 λ,输出为系统的公钥 PK 和主密钥 MSK。

(2)$KeyGen(PP,MSK,S)\rightarrow SK$:该算法由 AA 执行,输入为公开参数 PP、主密钥 MSK、用户属性集 S,输出为用户私钥 SK。

(3)$Encrypt(PP,M,W,Q)\rightarrow CT$:该算法由 DO 执行,输入为公开参数 PP、明文文件 M、文件访问策略 W、文件关键字 Q,输出为密文文件 CT(包括密文 C、索引密文 I、访问策略的布隆过滤器 BF_W)。

(4)$Trapdoor(PP,SK,Q')\rightarrow T$:该算法由 DU 执行,输入为公开参数 PP、私钥 SK、查询关键字 Q',输出为陷门 T。

(5)$Search(PP,CT,T)\rightarrow(CT/\perp)$:该算法由 CSP 执行,输入为公开参数 PP、密文文件 CT、陷门 T,若用户满足访问策略并且关键字匹配成功,则输出为密文 CT,否则返回 $\perp$。

(6)$Decrypt(PP,SK,CT)\rightarrow M$:该算法由 DU 执行,输入为公开参数 PP、私钥 SK、密文文件 CT,输出为明文文件 M。

3.3 安全模型

本文方案考虑了选择明文攻击下的不可区分性(Indistinguishability Under Chosen-plaintext Attack,IND-CPA)。它基于攻击者 A 和挑战者 B 之间的博弈,其安全模型的定义如下。

(1)初始化:挑战者 B 选择安全参数 λ 并运行 $Setup()$ 算法,以生成系统主密钥 MSK 和公共参数 PP。B 将 PP 发送给攻击者 A,自己保存主密钥 MSK。

(2)阶段 1:A 根据自己的属性集 S 向 B 进行私钥问询。

(3)挑战:A 发送两条等长的消息 M_0 和 M_1 以及一个访问结构 W^* 给 B,W^* 不能被查询属性集 S 中任何属性满足。B 通过抛硬币随机选择一个数 $\beta\in\{0,1\}$,并在 W^* 下加密 M_β,将结果密文 CT 发送给 A。

(4)阶段 2:重复阶段 1 的工作,A 继续向 B 进行私钥问询,并且限制这些属性都不满足访问结构 W^*。

(5)猜测:A 输出一个对 M_β 的猜测结果 $\beta'\in\{0,1\}$。如果 $\beta'=\beta$,则说明攻击者 A 成功了,而 A 的优势被定义为:

$$Adv_{A,\text{CP-ABE}}^{\text{CPA}}=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right| \tag{2}$$

4 本文方案

4.1 系统初始化

(1)输入安全参数 λ,设 G 和 G_T 是阶为素数 p 的乘法循环群,g 是群 G 的生成元,$e:G\times G\rightarrow G_T$ 是一个双线性映射。假设系统的属性集合为 $U=\{att_1,att_2,\cdots,att_i,\cdots att_n\}$,属性 att_i 的可能取值集合为 $V_i=\{v_{i,1},v_{i,2},\cdots,v_{i,j},\cdots,v_{i,m_i}\}$,其中 $1\leqslant i\leqslant n$,$1\leqslant j\leqslant m_i$。$H_0$,$H_1$ 和 H_2 是 3 个抵制合谋的哈希函数,即 $H_0:Z_p^*\times\{0,1\}^{\log_2 n}\times\{0,1\}^{\log_2 m}\rightarrow Z_P^*$,$H_1:Z_P^*\rightarrow G$,$H_2:Z_P^*\times\{0,1\}^{\log_2^2}\leftarrow Z_P^*$,其中 $m=\max_{i=1}^{n} m_i$。设 L_{BF} 为 BF 的位数组大小,并生成 k 个随机独立的哈希函数 $h_1,h_2,\cdots,h_k$,将每个元素映射到位数组中。

(2)AA 随机选取 $\alpha,\beta\in Z_P^*$,对于每一属性值,都有 $X_{i,j}=g^{-H_0(\alpha\|i\|j)}$ 和 $Y_{i,j}=e(g,g)^{H_0(\beta\|i\|j)}$,其中 i 对应属性名的下标,j 对应 i 的属性值下标,$1\leqslant i\leqslant n$,$1\leqslant j\leqslant m$,输出系统公开参数 PP 和主密钥 MSK。

$$PP=\{G,G_T,e,g,(X_{i,j},Y_{i,j}),1\leqslant i\leqslant n,1\leqslant j\leqslant m\} \tag{3}$$

$$MSK=\{\alpha,\beta\} \tag{4}$$

4.2 用户密钥生成

当 AA 收到 DU 的属性集 $S=\{s_1,s_2,\cdots,s_i,\cdots,s_n\}$,$s_i\in\{V_i\}$ 时,为 DU 生成相关私钥。

AA 为用户随机选择 $sk,a\in Z_P^*$,计算 $\theta_{i,1}=g^{H_0(\beta\|i\|j)}H_1(sk)^{H_0(\alpha\|i\|j)}$,$\theta_{i,2}=g^{-H_0(\alpha\|i\|j)\cdot a}$,$k=g^a$,生成用户的私钥 SK,通过安全信道发送给用户。

$$SK=\{k,(\theta_{i,1},\theta_{i,2}),1\leqslant i\leqslant n\} \tag{5}$$

4.3 数据加密

(1)DO 对文件的访问策略 W 进行加密。

1)对需要上传的文件 M 设置相应的访问策略 $W=\{w_1,w_2,\cdots,w_i,\cdots,w_n\}$,$w_i\in\{V_i,*\}$,"$*$"代表用户对此属性值不在意。访问策略 W 对应的下标集合为 $I_W=\{i\mid 1\leqslant i\leqslant n,w_i\neq *\}$。

2)对访问策略的下标集合 I_W 中的值进行哈希加密:$H_2(i),i\in I_W$。将得到的一系列哈希值 $H_2(i)$ 经过 k 个 BF 的哈希函数 $h_1,h_2,\cdots,h_k$ 映射到 BF 数组中,将对应位置置为 1,得到访问策略对应的位数组 BF_W。

(2)DO 对文件 M 进行加密。

1)根据 I_W 中涉及的属性和对应的属性值下标,计算 $X_W=\prod_{i\in I_W}X_{i,j}$,$Y_W=\prod_{i\in I_W}Y_{i,j}$;

2)随机选择 $s\in Z_P^*$,计算 $C_1=M\cdot Y_W{}^s$,$C_2=g^s$,$C_3=X_W{}^s$,生成密文 C。

$$C=\{C_1,C_2,C_3\} \tag{6}$$

(3)DO 对文件关键字集 Q 进行加密。文件的关键字集为 $Q=\{q_1,q_2,\cdots,q_l\}$,计算 $I^2=g^s$,对 Q 中的每个关键字 q_k 进行如下加密,即 $\{I_{1,k}=H_1(q_k)^s,1<k<l\}$,最后生成索引文件 I。

$$I=\{I_{1,k},I_2\},1<k<l \tag{7}$$

最后,生成密文文件 CT,将其发送给云服务器存储。

$$CT=\{C,I,BF_W\} \tag{8}$$

4.4 陷门生成

用户的查询关键字集为 $Q'=\{q_1',q_2',\cdots,q_{l'}'\}$。

(1)DU 根据私钥对属性加密。

1)对拥有的属性下标 i 进行哈希:$H_2(i)$,$1\leqslant i\leqslant n$。

2)随机选择 $t\in Z_P^*$,计算 $T_{i,1}=\theta_{i,2}^t$,$T_2=g^t$,$T_3=k^t=g^{a\cdot t}$。

(2)DU 对查询关键字集加密。对 Q' 中的每个关键字 q_k' 做如下加密:$\{T_{4,k}=H_1(q_k')^t,1<k<l'\}$;

最后,生成陷门文件 T,并将其发送给云服务器。

$$T=\{T_2,T_3,\{T_{4,k},1<k<l\},\{H_2(i),T_{i,1},1\leqslant i\leqslant n\}\} \tag{9}$$

4.5 搜索

CSP 收到 DU 发来的陷门 T,为 DU 进行密文搜索并返回相关结果。

(1)CSP 检验 DU 是否拥有 DO 访问策略中的属性。CSP 将 DU 陷门中的 $H_2(i)$ 值经过哈希映射,得到其在位数组 BF_W 中的对应位置,看对应位置上的值是否为 1,如果为 1,则说明 DU 的该属性在 DO 的访问策略中,最终得到 DU 符合访问策略的属性集,继续下一步搜索,以确定属性值和关键字是否匹配;若不匹配则终止搜索,返回 $\perp$。

(2)CSP 根据式(10),进一步检验 DU 的属性、属性值和关键字是否与 DO 的访问策略和索引相匹配。

$$\frac{e(T_1,I_2)}{e(T_3,C_3)}=e(I_1,T_2) \tag{10}$$

其中,$T_1=\prod_{i\in I_W}T_{i,1}\cdot T_4=g^{-\sum_{i\in I_W}H_0(\alpha\|i\|j)\cdot a\cdot t}\cdot H_1(q')^t$。若式(10)成立,则搜索成功,返回该密文的 CT 给 DU,否则搜索失败,返回 $\perp$。

4.6 用户解密

DU 收到 CSP 返回的 CT,根据 CT 中的 BF_W 和自己的属性相关值 $H_2(i)$,判断符合 DO 的访问策略的属性,对符合访问策略的属性进行计算,$\theta=\prod_{i\in I_W}\theta_{i,1}=g^{\sum_{i\in I_W}H_0(\beta\|i\|j)}\cdot H_1(sk)^{\sum_{i\in I_W}H_0(\alpha\|i\|j)}$,根据式(11)计算得到明文 M。

$$M=\frac{C_1}{e(\theta_1,C_2)e(H_1(sk),C_3)} \tag{11}$$

4.7 方案的正确性

(1)在搜索阶段,当 DU 拥有 DO 访问策略中的相关属性时,通过式(12)对 DU 的属性、属性值和关键字进行匹配确认。

(2)在解密阶段,当 DU 根据 BF_W 确定自己的符合 DO 的访问策略的属性后,通过式(13)进行解密,并再次确认属性值与访问策略的匹配性。

5 安全性分析

本文方案满足 q-BDHE 假设下的 IND-CPA 安全,基于 3.3 节中的安全模型进行证明。

$$\begin{aligned}M&=\frac{C_1}{e(\theta_1,C_2)\cdot e(H_1(sk),C_3)}\\&=\frac{M\cdot\prod_{i\in I_W}e(g,g)^{H_0(\alpha\|i\|j)\cdot s}}{e(g^{\sum_{i\in I_W}H_0(\beta\|i\|j)}\cdot H_1(sk)^{\sum_{i\in I_W}H_0(\alpha\|i\|j)},g^s)\cdot e(H_1(sk),\prod_{i\in I_W}g^{-H_0(\alpha\|i\|j)\cdot s})}\\&=\frac{M\cdot e(g,g)^{s\cdot H_0(\beta\|i\|j)}}{e(g,g)^{s\cdot H_0(\beta\|i\|j)}\cdot e(H_1(sk),g)^{s\cdot\sum_{i\in I_W}H_0(\alpha\|i\|j)}\cdot(H_1(sk),g)^{-s\cdot\sum_{i\in I_W}H_0(\alpha\|i\|j)}}\\&=M\end{aligned}\tag{13}$$

定理 1 若决策性 q-BDHE 假设在群 G_1 和 G_T 中成立,则没有多项式攻击者 A 能够以不可忽略的优势选择性地攻破本文方案。

(1)初始化:挑战者 B 选择安全参数 λ 并运行 Setup(λ)算法。B 随机选取 $\alpha,\beta\in Z_P^*$,对于系统的每个属性,计算相应的 $X_{i,j}=g^{-H_0(\alpha\|i\|j)}$ 和 $Y_{i,j}=e(g,g)^{H_0(\beta\|i\|j)}$。产生系统公共参数 $PP=\{G,G_T,e,g,(X_{i,j},Y_{i,j}),1\leqslant i\leqslant n,1\leqslant j\leqslant m_i\}$ 并将其发送给 A,自己保留主密钥 $MSK=\{\alpha,\beta\}$。

(2)阶段 1:A 根据自己的属性集 S 向 B 进行私钥问询。

B 首先随机选择 $sk,a\in Z_P^*$,再计算 $\theta_{i,1}=g^{H_0(\beta\|i\|j)}H_1(sk)^{H_0(\alpha\|i\|j)}$,$\theta_{i,2}=g^{-H_0(\alpha\|i\|j)\cdot a}$,$k=g^a$,并将其发送给 A。

(3)挑战:A 发送两条等长的消息 M_0 和 M_1 以及一个访问结构 $W^*=\bigwedge_{i\in I_w}w_i$ 给 B,W^* 不能被查询属性集 S 中任何属性满足。

B 通过抛硬币随机选择一个数 $\beta\in\{0,1\}$,并在 W^* 下加密 M_β。计算符合 W^* 的 $X_W=\prod_{i\in I_W}X_{i,j}$,$Y_W=\prod_{i\in I_W}Y_{i,j}$,随机选择 $s\in Z_P^*$,计算 $C_1=M\cdot Y_W{}^s$,$C_2=g^s$,$C_3=X_W{}^s$,生成密文 $C=\{C_1,C_2,C_3\}$。将结果密文 C 交给 A。

(4)阶段 2:重复阶段 1 的工作,A 继续向 B 进行私钥问询,并且限制这些属性都不满足访问结构 W^*。

(5)猜测:A 输出一个对 M_β 的猜测结果 $\beta'\in\{0,1\}$。

如果 $\beta'=\beta$,则挑战者 B 输出 $\mu=0$ 来猜测 $T=e(g_{q+1},h)$;否则输出 $\mu=1$,表示它认为 T 是 G_T 中的随机群元素。

当 $\mu=0$ 时,即 $T=e(g_{q+1},h)$。此时 $C=\{C_1,C_2,C_3\}$ 为可用密文,为 B 提供的有效仿真。A 的优势至少为 ε,因此有式(14)。

$$\Pr[\beta'=\beta|\mu=0]=\varepsilon+\frac{1}{2}\tag{14}$$

当 $\mu=1$ 时,说明 T 是 G_T 中的一个随机元素。A 从中不能得到任何关于 β 的信息。因此,我们有式(15):

$$\Pr[\beta'\neq\beta|\mu=1]=\Pr[\beta'=\beta|\mu=1]=\frac{1}{2}\tag{15}$$

最后,可以得到式(16):

$$\begin{aligned}Adv_A&=\frac{1}{2}\cdot\Pr[\beta'=\beta]-\frac{1}{2}\\&=\frac{1}{2}\cdot\left(\varepsilon+\frac{1}{2}+\frac{1}{2}\right)-\frac{1}{2}\\&=\frac{\varepsilon}{2}\end{aligned}\tag{16}$$

即,在多项式时间内,若攻击者 A 能以不可忽略的优势 $1/2+\varepsilon$ 攻破本文方案,则挑战者 B 可以以优势 $\varepsilon/2$ 攻破 q-BDHE 问题。

6 性能分析和实验仿真

6.1 功能特性比较

表 2 列出了本文方案与文献[27-30]在访问策略、安全假设、定长密文、策略隐藏和可搜索加密这几方面的对比。为了实现细粒度的访问控制,所有的方案都采用了 ABE 技术。从比较结果中可以看出,文献[28-29]的访问策略更加灵活,但方案只支持关键词搜索;本文方案的访问策略较文献[27,30]更为灵活,访问策略支持多值和通配符,方案在支持定长密文和策略隐藏的基础上同时支持关键词搜索。

表 2 功能对比

Table 2 Function comparison

文献	访问策略	安全假设	定长密文	策略隐藏	可搜索加密
[27]	AND_m	l-BDHE	×	√	√
[28]	$LSSS$	—	×	×	√
[29]	访问树	BDHE	×	×	√
[30]	$AND+,-$	BDHE	√	×	×
本文	AND_m^*	q-BDHE	√	√	√

6.2 理论分析

表 3 和表 4 列出了本文方案与文献[27-30]的方案在加密开销、搜索开销、陷门开销、解密开销以及密钥和密文存储方面的对比结果。其中,T_e 为群上的幂运算,T_p 为双线性对运算,$|G|$ 和 $|GT|$ 分别表示群 G 和 GT 上的元素长度,S 为用户属性集的长度,W 为关键字集的长度。从表中可以看出,文献[30]的方案与本文方案的加解密运算与密文存储开销较小,能有效减少用户与云端的通信和存储开销,但文献[30]的

方案没有关键词搜索功能；文献[28]的方案的密钥长度较小，但它的密文长度是随属性数量变化的，而本文方案的密文长度不随属性数量的变化而变化，且密钥长度在量级上与文献[28]的方案一致。

表 3 计算开销对比

Table 3 Computing overhead comparison

方案	加密开销	搜索开销	陷门开销	解密开销
文献[27]的方案	$(4S+2W+1)T_e$	$(2S+W)T_e+(2S+W)T_p$	$(2S+W)T_e$	—
文献[28]的方案	$(3S+2)T_e$	$S\cdot T_e+(S+2)T_p$	—	$1\ T_e$
文献[29]的方案	$(4S+W+1)T_e$	$(2S+2W+1)T_p$	$(2S+W+3)T_e$	$2S\cdot T_e+S\cdot T_p$
文献[30]的方案	$4T_e$	—	—	$2\ T_e+2\ T_p$
本文方案	$(W+4)T_e$	$(2W+1)T_p$	$(S+W+2)T_e$	$2\ T_p$

表 4 存储开销对比

Table 4 Storage overhead comparison

方案	密钥长度	密文长度
文献[27]的方案	$(2S+1)\lvert G\rvert$	$\lvert GT\rvert+(4S+2W)\lvert G_1\rvert$
文献[28]的方案	$(S+2)\lvert G\rvert$	$(2S+1)\lvert G\rvert+\lvert GT\rvert$
文献[29]的方案	$(2S+2)\lvert G\rvert$	$(2S+W+1)\lvert G\rvert+S\cdot\lvert GT\rvert$
文献[30]的方案	$(2S+2)\lvert G\rvert$	$3\lvert G\rvert+\lvert GT\rvert$
本文方案	$(2S+2)\lvert G\rvert$	$(W+3)\lvert G\rvert+\lvert GT\rvert$

6.3 实验分析

本实验模拟环境的操作系统为 64 bit Ubuntu 21.20，处理器为 Intel(R) Core(TM) i5-7200U CPU @2.50GHz，计算机内存为 4GB，使用 python 的 pypbc 库进行双线性计算及编程，采用 A 类超奇异曲线 $E(F_q):y^2=x^3+x$，阶为 p 的椭圆曲线群 G 和 GT 是 $E(F_q)$ 的子群，其中参数 p 和 q 分别为 160 bit 和 512 bit。

实验对比了 5 种方案在查询关键词的数量固定不变时，加密阶段、搜索阶段、陷门生成、解密阶段的计算开销和密文长度的存储开销与属性数量的变化关系。如图 3 和图 4 所示，文献[27-29]的方案的密文计算和存储开销会随属性数量的增加呈线型增长关系，而文献[30]的方案与本文方案采用了密文恒定技术，密文的计算和存储开销是一个定值，且均小于文献[27-29]的方案。如图 5 所示，在陷门生成过程中，虽然本文方案的计算开销不是一个定值，但随属性数量的变化程度比文献[27,29]的方案小。如图 6 所示，在搜索过程中，本文的计算量也是一个定值，不随属性数量的变化而变化。如图 7 所示，在解密阶段，文献[29]的方案的解密时间随属性数量的增加呈线性增加；本文方案与文献[28,30]的方案的解密时间均为定值，其中文献[28]的方案的部分解密数据由云端计算，因此解密时间最短，但文献[28]的方案的访问策略与搜索关键词是明文上传的，易暴露隐私信息；本文方案在解密时，采用加密时的密文定长方法，因此解密时间不随属性数量的增加而增加，是一个很小的定值。

另外，实验还对比了 5 种方案在属性数量固定不变时，密文生成阶段、陷门生成阶段的计算开销与关键词数量的变化关系。如图 8 所示，在密文生成阶段，本文的计算量虽然不是一个定值，但其随关键词的变化量还是较小。文献[30]的方案的加密时间最短且为一个定值，因为文献[30]并没有关键词搜索，所以其加密时间最短。如图 9 所示，在陷门生成阶段，本文的计算量小于文献[27,29]的方案。因此，本文在计算和存储开销上优于其他方案。

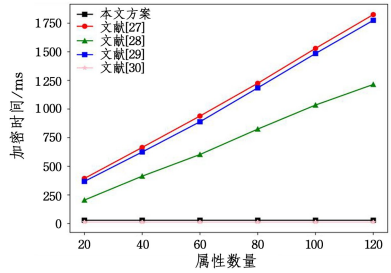

图 3 密文生成的开销对比图

Fig. 3 Cost comparison of ciphertext generation

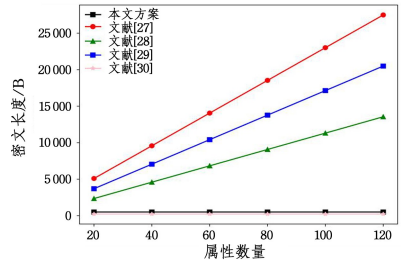

图 4 密文存储的开销对比图

Fig. 4 Cost comparison of ciphertext storage

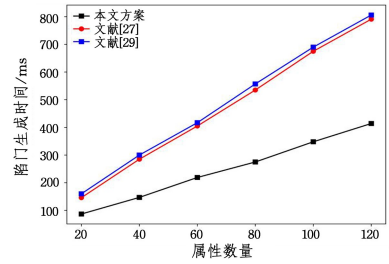

图 5 陷门阶段的计算量对比图

Fig. 5 Comparison of calculation amount in trap-gate stage

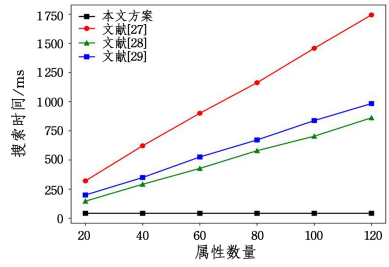

图 6 搜索阶段的计算量对比图

Fig. 6 Comparison of calculation amount in search stage

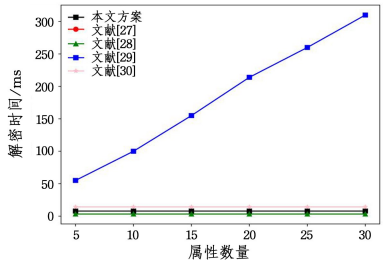

图 7 解密阶段的计算量对比图

Fig. 7 Comparison of calculation amount in decryption stage

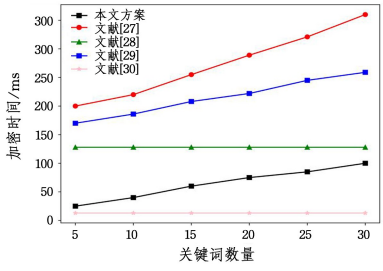

图 8 加密时间与关键词的对比图

Fig. 8 Comparison of encryption time and keywords

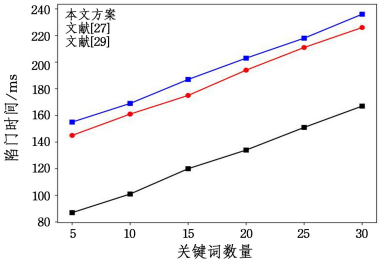

图 9 陷门生成时间与关键词的对比图

Fig. 9 Comparison of trap-gate generation time and keywords

结束语 本文提出了一种高效的策略隐藏且密文恒定的可搜索加密方案。针对基于属性的加密方案中密文长度随属性数量的增加线性增长的问题，实现了密文长度恒定，减小了相关的计算和存储开销。通过访问策略的完全隐藏，加强了用户的隐私保护。用户在搜索时需保证搜索关键词一致且属性符合访问策略，才可以检索到相关密文，进一步保证了数据使用的安全性。安全性证明通过将方案规约到 q-BDHE 困难问题上，实现方案的 IND-CPA 安全。最后的性能分析与实验仿真表明，本文方案是一个多功能且高效的密文搜索方案。之后，可对方案的安全性和访问策略的表达性进行进一步的研究与提高。

参 考 文 献

[1] SAHIA A, WATERS B R. Fuzzy Identity-Based Encryption [C]// Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin/Heidelberg: Springer, 2005: 457-473.

[2] SUN W, YU S, LOU W, et al. Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud[C]// IEEE INFOCOM 2014. IEEE, 2014: 226-234.

[3] CHENG S J, ZHANG C H, PAN S Q. Design of cloud storage data access control scheme based on cp-abe algorithm [J]. Information Network Security, 2016(2): 1-6.

[4] HAN D, PAN N, LI K C. A Traceable and Revocable Ciphertext-policy Attribute-based Encryption Scheme Based on Privacy Protection[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 316-327.

[5] ZHANG Y, DENG R, XU S, et al. Attribute-Based Encryption for Cloud Computing Access Control: A Survey[J]. ACM Computing Surveys, 2020, 53(4): 1-41.

[6] JITENDRA K S, NARANDER K. Secure Data Validation and Transmission in Cloud and IoT Through BanLogic and KP-ABE [J]. International Journal of Sensors, Wireless Communications and Control, 2022, 12(1): 79-87.

[7] SANGEETHA M, VIJAVAKARTHIK P. To provide a secured access control using combined hybrid key-ciphertext attribute based encryption (KC-ABE) [C] // IEEE International Conference on Intelligent Techniques in Control. IEEE, 2017: 1-4.

[8] WATERS B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization[C]// International Workshop on Public Key Cryptography. Berlin/Heidelberg: Springer, 2008: 53-70.

[9] LIU S, GUO Y Z. Multi authorization center CP-ABE proxy re-encryption scheme in cloud computing [J]. Journal of Network and Information Security, 2022, 8(3): 176-188.

[10] SHAO F J, ZHENG R J. An Efficient Fuzzy Searchable Encryption Scheme based Attribute for Medical Data[J]. International Core Journal of Engineering, 2022, 8(7): 118-126.

[11] XIE M, RUAN Y, HONG H, et al. A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices[J]. Future Generation Computer Systems, 2021, 121(5): 114-122.

[12] VARRI U S, PASUPULETI S K, KADAMBARI K V. CP-ABSEL: Ciphertext-policy attribute-based searchable encryption from lattice in cloud storage[J]. Peer-to-Peer Networking and Applications, 2021, 14(3): 1290-1302.

[13] NISHIDE T, YONEYAMA K, OHTA K. Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures[C]// International Conference on Applied Cryptography and Network Security. Berlin/Heidelberg: Springer, 2008: 111-129.

[14] LAI J, DENG, LI R H. Fully Secure Cipertext-Policy Hiding CP-ABE[C]// Information Security Practice and Experience. Berlin/Heidelberg: Springer, 2011: 24-39.

[15] QIU S, LIU J, SHI Y, et al. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack[J]. Science China (Information Sciences), 2016, 60(5): 1-12.

[16] ZHANG L, HU G, MU Y, et al. Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System[J]. IEEE Access, 2019, 7(3): 33202-33213.

[17] MENG F, CHENG L, WANG M. Ciphertext-policy attribute-

based encryption with hidden sensitive policy from keyword search techniques in smart city[J]. EURASIP Journal on Wireless Communications and Networking, 2021, 2021(1): 20.

[18] ARKIN G, HELIL N. Ciphertext-Policy Attribute Based Encryption with Selectively-Hidden Access Policy [J]. Computing and Informatics, 2021, 40(5): 1136-1159.

[19] ZHANG Z, ZHANG J, YUAN Y, et al. An Expressive Fully Policy-Hidden Ciphertext Policy Attribute-Based Encryption Scheme with Credible Verification Based on Blockchain [J]. IEEE Internet of Things Journal, 2022, 9(11): 8681-8692.

[20] GAN T, LIAO Y, LIANG Y, et al. Partial policy hiding attribute-based encryption in vehicular fog computing[J]. Soft Computing, 2021, 25(6): 10543-10559.

[21] HERRANZJ , LAGUILLAUMIE F, CARLA R. Constant Size Ciphertexts in Threshold Attribute-Based Encryption[C]// International Conference on Practice & Theory in Public Key Cryptography. Berlin/Heidelberg: Springer, 2010: 19-34.

[22] GUAN Z, YANG W, ZHU L, et al. Achieving adaptively secure data access control with privacy protection for lightweight IoT devices[J]. Science China Information Sciences, 2021, 64(6): 1-14.

[23] WEI T, GENG Y, YANG X, et al. Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing [J]. IEEE Transactions on Cloud Computing, 2017, 5(4): 617-627.

[24] ZHAO Z Y, ZHU Z Q, WANG J H, et al Attribute based encryption scheme with revocable attributes and constant ciphertext length[J]. Acta Electronica Sinica, 2018, 46(10): 2391-239.

[25] BLOOM B H. Space/time trade-offs in hash coding with allowable errors[J]. Communications of the ACM, 1970, 13(7): 422-426.

[26] GE A, RUI Z, CHENG C, et al. Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts[C]// Australasian Conference on Information Security & Privacy. Berlin/Heidelberg: Springer, 2012: 336-349.

[27] ZHANG K, LI Y P, LU L F. Privacy-Preserving Attribute-Based Keyword Search with Traceability and Revocation for Cloud-Assisted IoT[J/OL]. Security and Communication Networks, 2021, 2021, 9929663. https://www.xueshufan.com/publication/3171431550.

[28] CHEN R, LI Z. Blockchain-Based Mechanism for Electronic Healthy Records Sharing Using Fine-grained Authorization [C]// 2021 7th International Conference on Computer and Communications(ICCC). 2021: 1557-1564.

[29] MIAO Y, MA J, LIU X, et al. Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing[J]. IEEE Transactions on Services Computing, 2020, 13(6): 985-998.

[30] LI Q, XIA B, HUANG H, et al. TRAC: Traceable and Revocable Access Control Scheme for mHealth in 5G-Enabled IIoT[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3437-3448.

ZHOU Yihua, born in 1969, Ph.D, associate professor. His main research interests include network and information security.

LI Meiqi, born in 1998, postgraduate. Her main research interests include information security and privacy protection.

(责任编辑:喻藜)