doi:10.11959/j.issn.1000-436x.2015307

云环境下关键词搜索加密算法研究

林鹏，江颉，陈铁明
（浙江工业大学 计算机学院，浙江 杭州 310000）

摘 要：现有方案将关键词搜索加密和属性基加密相结合，解决了云环境下访问控制问题，但是未充分考虑信道安全以及关键词猜测攻击等安全问题。针对上述问题，提出了一种指派搜索服务器的关键词搜索属性加密方案，实现了关键词搜索访问权限控制，且检索不需要安全信道，可抵抗离线/在线关键词猜测攻击。实验结果表明，方案性能方面可取得较好结果，可应用于云环境。
关键词：可搜索加密；属性基加密；关键词猜测攻击；安全信道
中图分类号：TP309.7 **文献标识码**：A

Application of keyword searchable encryption in cloud

LIN Peng, JIANG Jie, CHEN Tie-ming
(Institute of Computer, Technology of Zhejiang University, Hangzhou 310000, China)

Abstract: Recently, some schemes combined keyword searchable encryption with attribute based encryption, solved access control problem in cloud environment, but they didn't consider security problems like keyword guessing attack and security channels, so they couldn't be applied to cloud. A keyword searchable attribute based encryption scheme with a designated tester was proposed, which could be against online/offline keyword guessing attacks and without security channel. Moreover, the user was able to encrypt data by setting a fine-gained access control policy. The efficiency of the scheme is analyzed it can be applied to cloud.
Key words: searchable encryption; attribute based encryption; keyword guessing attack; secure channel

1 引言

随着云技术的快速发展，云存储服务也越来越成熟。为了节省管理维护费用，专注于业务，中小企业或者个人更倾向于将数据存放于云端，由云存储服务提供商负责存储数据。用户将数据上传到云端后，便失去了数据的完全控制权，倘若云存储服务提供商与其他用户合谋，或是云服务器存在漏洞，用户数据可能会泄露，数据将失去安全性。所以用户更倾向于将数据加密后上传至云端。

加密后的数据由于失去了数据结构和语义特性，云端服务器通常无法向用户提供明文的搜索服务。若用户需要搜索数据，最简单的做法是先将所有加密数据下载到本地，然后逐一解密再进行搜索。这种方案虽然简单，但未充分利用云端的计算能力，并且对用户主机的带宽和 CPU 有一定要求，搜索效率过低。

关键词搜索加密[1]是一种特殊的加密技术。该技术能够实现合法用户搜索关键词密文,并且保证攻击者无法通过关键词密文或者搜索凭证获得用户查询的关键词信息。现有方案将关键词加密搜索方案和属性基加密方案相结合，解决了多用户环境下访问控制问题，但是未充分考虑信道安全以及关键词猜测攻击等安全问题，不适合部署于应用环境。针对上述安全问题，本文提出一种指派搜索服务器的关键词属性加密方案。一方面，实现关键词密文访问权限控制；另一方面，关键词密文及搜索凭证可抵抗离线在线关键词猜测攻击，上传时不需

收稿日期：2015-10-26
基金项目：国家自然科学基金资助项目（61103044）；浙江省科技厅计划基金资助项目（2013C01121）
Foundation Items: The National Natural Science Foundation of China (61103044); Zhejiang Provincial Science and Technology Project (2013C01121)

要安全信道。本文通过实验验证方案效率可行性。实验结果表明，该方案在性能方面可取得较好结果，可应用于云环境。

2 相关工作

Boneh[1]等首次提出非对称关键词可搜索加密概念，即PEKS(public key encryption with keyword search)概念，并基于IBE，构造了具体的BDOP-PEKS方案。但是BDOP-PEKS方案仅仅保证了PEKS密文的安全性，保证用户无法从PEKS密文获得关于关键词的任何信息。Baek等[2]指出，BDOP-PEKS方案要求用户和搜索服务器之间建立安全信道，否则，外部恶意攻击者能够通过公开信道截获和篡改陷门和查询结果。另外，某些恶意服务器也可以存储已查询的陷门与搜索结果，以预测未来的查询结果。因此Baek等[2]提出不需要建立安全信道的可搜索加密方案SCF-PEKS。

Byun等[3]指出SCF-PEKS无法抵御离线关键词猜测攻击。在关键词搜索的应用中，用户总是使用常用搜索关键词，关键词空间熵值过低，攻击者仅需截获用户生成的搜索凭证，即可进行破解。Rhee等[4]提出了能够抵抗离线关键词猜测攻击的方案dPEKS，该方案要求用户在生成关键词密文，以及上传搜索凭证时指定搜索服务器。Hu等[5]对dPEKS进行了改进，消除了指定搜索服务器进行离线关键词猜测攻击的隐患。同样为了抵御离线关键词猜测攻击，Tang等[6]提出的方案中加入了关键词注册过程，Xu等[7]提出将搜索关键词模糊化，降低关键词加密搜索方案的一致性从而提高安全性，但是上述方案牺牲了一定性能。因此设计出能抗离线关键词猜测攻击且高效的可搜索加密方案依然是未来的研究方向[8]。

Jeong等[9]提出了在线关键词猜测攻击的概念(online keyword guessing attack)。攻击者为每个可能的关键词生成密文并上传至服务器，并记录关键词和密文的对应关系，若用户向搜索服务器发起搜索请求，攻击者可根据服务器返回的文件列表，从记录的表项中推断出用户的搜索词。Chen等[10]提出SPEKS方案用于抵御在线关键词猜测攻击。该方案需要半可信服务器，即该服务器不对用户进行在线关键词猜测攻击。当服务器返回搜索结果给用户时，首先进行加密计算，用户再在本地解密恢复出搜索结果，从而保证攻击者即使截获返回结果也无法获得检索结果信息。

上述的方案都是以关键词可搜索加密的安全性作为切入点。若将关键词可搜索加密方案部署到云环境，则不得不考虑多用户情况。Hwang等[11]实现了第一个多用户关键词加密方案，但是该方案要求加密前首先确定具体的用户列表，而在云环境中，加密方可能无法确定具体的用户，但是能够对数据制定访问权限。最近提出的大部分方案采用属性基加密技术实现多用户访问控制。结合属性基加密技术，当用户对密文进行加密时，加密的对象不是单个用户，而是一个群体[12]。现有的属性基加密方案大部分是在CP-ABE[13]和KP-ABE[14]基础上进行扩展。文献[15~17]基于KP-ABE方案将访问策略设置在搜索凭证上，由于在关键词可搜索加密方案中，搜索凭证中的策略信息需要保密，所以该类方案需要构造合数阶群来实现策略隐藏，虽然安全性满足要求，但是性能较低，并且每次搜索都需要向授权机构申请搜索凭证，所以目前还不适合部署到现实应用中。CP-ABE方案[13]被目前大部分方案[18~22]所参考，这类方案将访问控制设置在密文上。该类方案为关键词密文设置搜索访问控制权限，仅当用户属性满足访问策略时，才能够进行关键词搜索。李双等[17]、Wang等[18]和Li等[19]提出的方案需要授权机构参与搜索凭证生成，无法像传统PEKS方案一样，支持用户自行生成搜索凭证。在云环境应用中，可能有大量用户进行频繁的搜索，可能会对授权机构造成过重的负担，并且在请求搜索凭证时用户需要与授权机构建立安全信道，还会造成额外开销。Liu等[20]、Zheng等[21]为可搜索加密方案提供了结果验证算法，但是都无法抵御关键词猜测攻击。上述基于属性基的可搜索加密方案都无法抵御在线关键词猜测攻击。

针对上述问题，本文提出了一种可指派搜索服务器的属性基关键词加密搜索方案。在本方案中，用户可选择相对可信的搜索服务器，该搜索服务器不会进行在线关键词猜测攻击。在本方案所有交互过程中，用户只有在接收搜索服务器公钥和用户私钥时需要安全信道。对于非安全信道中传输的数据，即使恶意用户截获了这些信息，也无法通过在线离线关键词猜测攻击，恢复出任何信息。并且，本文的方案支持灵活的多用户访问权限控制，支持用户自行生成搜索凭证，适合应用于云环境。

3　预备知识

3.1　双线性映射及复杂性假设

定义 1　双线性映射[23]。

G_0 和 G_1 为素数 p 阶的乘法循环群。g 为 G_0 的生成元。双线性映射 $e: G_0 \times G_0 \to G_1$ 需要满足以下特性。

1) 双线性：对于 $\forall u, v \in Z_p$，$\forall a, b \in G_0$，满足 $e(a^u, b^v) = e(a,b)^{uv}$。

2) 非退化性：$e(g,g) \neq 1$。

3) 可计算性：对于 $\forall a, b \in G_0$，能够在多项式时间内计算 $e(a,b)$。

定义 2　DBDH 难题[23]。

G 为素数阶 p 的群，g 为 G 中的生成元。随机选择 $a,b,c \in Z_p$，$z \in Z_p$。DBDH 难题即为已知 g^a、g^b、g^c，在多项式时间内，无法区分 $e(g,g)^{abc}$ 与 $e(g,g)^z$。

定义 3　CDH 难题[24]。

G 为素数阶 p 的群，g 为 G 中的生成元。随机选择 $a,b \in Z_p$。CDH 难题即为已知 g^a、g^b，在多项式时间内，无法计算 g^{ab}。

3.2　访问结构

本文方案使用 CP-ABE[13]方案定义的访问树来表示访问结构。访问树能够灵活高效地应用于访问权限控制，定义如下。

令 T 表示访问树，T 中的每一非叶子节点代表一个门限值，若节点 x 有 num_x 个子节点，并且其门限值为 k_x，则 $0 < k_x \leqslant num_x$。当 $k_x = 1$ 时，该节点表示或门。若 $k_x = num_x$，则表示与门。T 中每一叶子节点表示属性，并且叶子节点对应的 $k_x = 1$。

当检查用户权限是否满足访问树 T 时，令 R 为 T 树的根节点。令 T_x 为以节点 x 为根节点的子树，如果属性集 S 能够满足 T_x 表示的策略，则记 $T_x(S) = 1$。利用如下递归算法计算 $T_x(S)$。

若 x 是非叶子节点，则对 x 的子节点 x' 计算 $T_{x'}(S)$，仅当满足 $T_{x'}(S) = 1$ 的子节点的数量大于等于 k_x 时，令 $T_x(S) = 1$，否则为 NULL。若节点为叶子节点，仅当该节点对应的属性 $attr(x) \in S$，令 $T_x(S) = 1$，否则为 NULL。

3.3　系统模型

本文提出的方案有以下 5 类角色：授权机构、云存储服务器、搜索服务器、数据属主、数据用户，如图 1 所示。

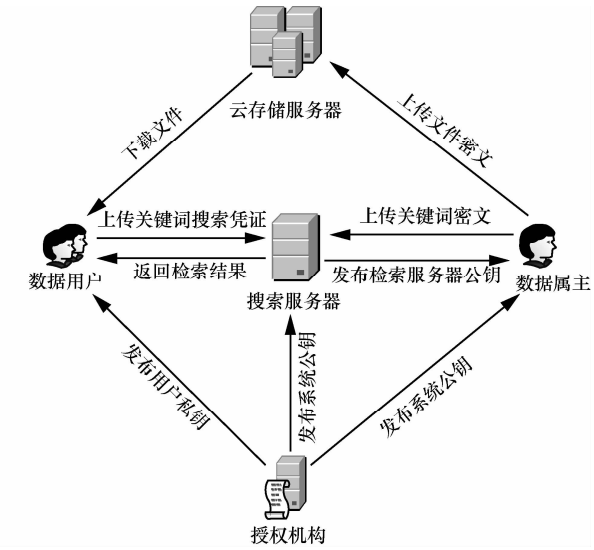

图 1　系统模型

云存储服务器负责存储加密文件。

授权机构负责生成、发布系统公钥以及向用户发布用户私钥。

数据属主是数据的拥有者。当数据属主需要上传数据时，对文件可以采用任意加密技术进行加密，然后利用本文提出方案加密关键词，并将加密关键词上传至指定的搜索服务器。

搜索服务器负责密文搜索。搜索服务器中保存关键词加密信息，能够利用数据用户上传的搜索凭证对密文进行搜索。仅当用户权限满足加密关键词搜索权限控制，且搜索关键词和文件关键词相符合，搜索服务器才返回正确信息。

数据用户是搜索服务的请求方。数据用户发起搜索请求时，首先在本地生成关键词搜索凭证，然后将该凭证上传至指定的搜索服务器。由搜索服务器负责搜索。

4　方案设计

本文方案由 Setup、ServerKeyGen、UserKeyGen、dPEKS、Trap、Test、TEncrypt、TDecrypt 等 8 个算法组成，分别负责系统建立，搜索服务器密钥生成，用户私钥生成，关键词加密，搜索凭证生成，关键词搜索，搜索结果加密，搜索结果解密。各算法具体细节如下。

1) $\text{Setup}(\mu) \to (GP, PK, MK)$

Setup 算法由授权机构执行。在 Setup 阶段，授权机构首先根据安全参数 μ，生成全局参数 GP，

如式(1)所示。该算法生成加密需要的双线性对、对应的乘法循环群 G， G_T 和生成元 g 以及散列函数 $H_1:\{0,1\}^{\log w}\to G$， $H_2:\{0,1\}^{\log w}\to G$，其中 H_1 用于计算属性在 G 上的映射， H_2 用于计算关键词在 G 上的映射。

然后授权机构随机选取 $\alpha,\beta\in Z_p$，生成系统私钥 MK，并作为秘密保存，如式(2)所示。最后根据生成的私钥 MK，生成系统公钥 PK，如式(3)所示。

$$GP=(e,g,G,G_T,H_1,H_2) \tag{1}$$

$$\alpha,\beta\in Z_p,\ MK=(\alpha,\beta) \tag{2}$$

$$PK=(g^{\alpha},g^{\beta}) \tag{3}$$

2) ServerKeyGen$(PK)\to(SSK,SPK)$

ServerKeyGen 算法由搜索服务器执行。搜索服务器随机选取 $x\in Z_p$，生成服务器私钥 SSK，如式(4)所示。搜索服务器将该私钥作为秘密保存。最后生成搜索服务器公钥 SPK，如式(5)所示。

$$x\in Z_p,SSK=(x) \tag{4}$$

$$SPK=\left(g^{x},g^{\frac{\beta}{x}}\right) \tag{5}$$

3) UserKeyGen$(MK,S)\to(USK)$

UserKeyGen 算法由授权机构执行，授权机构根据用户属性集合 S 和系统私钥 MK，生成用户私钥 USK。该算法首先随机选取 $r\in Z_p$，并为属性集 S 中的每个属性 j 随机选取 $r_j\in Z_p$，最终生成用户私钥，如式(6)所示。

$$r\in Z_p,\forall j\in S,r_j\in Z_p$$

$$USK=(K=g^{\alpha\beta+r},\forall j\in S:D_j=g^{r}H_1(attr_j)^{r_j},D_j^{'}=g^{r_j}) \tag{6}$$

4) dPEKS$(PK,SPK,W,T)\to CT$

dPEKS 算法由数据属主执行。数据属主首先选取文件数据对应的关键词 W，然后为关键词密文设置搜索权限，并生成访问树 T，选择搜索服务器公钥 $g^{\frac{\beta}{x}}$，最后利用该算法生成关键词密文 CT 并上传。

该算法根据访问树 T，为 T 中每个节点 x 选择多项式 q_x，多项式 q_x 按如下方式生成。从 T 根节点 R 开始，使用递归算法自上而下运行。对于每个节点 x，令多项式 q_x 的项数 d_x 比该节点表示的阈值 k_x 小 1，即 $d_x=k_x-1$。首先为根节点 R 随机选取 $s\in Z_p$，并且令 $q_R(0)=s$，然后随机选择其他项的系数。对于其他节点 x，定义函数 $parent(x)$，$index(x)$，前者表示节点 x 的父节点，后者表示 x 节点在父节点中的位置，令 $q_x(0)=q_{parent(x)}(index(x))$，并为 q_x 其他项随机选择系数。根据上述算法，最终为 T 中所有节点生成 C_v， $C_v^{'}$。

随机选择 $k\in Z_p$，生成 W_1， W_2， H，如式(7)所示。

$$CT=(W_1=g^{s},W_2=g^{\frac{\beta k}{x}},H=g^{\alpha s}H_2(W)^{k},$$
$$\forall v\in T,C_v=g^{q_v(0)},C_v^{'}=H_1(attr(v))^{q_v(0)}) \tag{7}$$

5) Trap$(W,USK,SPK,PK)\to(TR,t)$

Trap 算法由数据用户执行。根据数据用户需要搜索的关键词 W，随机选取 $t,y\in Z_p$，选择搜索服务器公钥 g^{x}，生成搜索凭证 TR，如式(8)所示，并且数据用户将 t 作为秘密保存。

$$TR=(T_0=g^{\beta t},T_1=K^{t}=g^{(\alpha\beta+r)t},T_2=H_2(W)^{t}g^{y},T_3=g^{xy},$$
$$\forall j\in \mathrm{S},E_j=D_j^{t}=g^{tr}H_1(attr_j)^{r_jt},E_j^{'}=D_j^{'t}=g^{r_jt}) \tag{8}$$

6) Test$(CT,TR)\to b$

Test 算法由搜索服务器执行。搜索服务器根据用户在 trapdoor 阶段生成的搜索凭证 TR 与数据属主在 dPEKS 阶段生成的关键词密文 CT 来计算关键词是否相等。

该算法首先计算搜索凭证 TR 中的用户属性是否满足密文 CT 中定义的访问结构。令函数 $DecryptNode(x)$ 为权限计算函数，该函数通过如下递归方式执行。

若节点 x 为叶子节点，令 $i=attr(x)$ 为节点 x 对应的属性。若 $i\in S$，则

$$DecryptNode(x)=\frac{e(E_j,C_v)}{e(E_j^{'},C_v^{'})}=e(g,g)^{trq_v(0)} \tag{9}$$

否则，令 $DecryptNode(x)=\mathrm{NULL}$。

若节点 x 为非叶子节点，则对节点 x 的子节点 z 计算 $F_z=DecryptNode(z)$。令 S_x 为满足 $F_z\neq\mathrm{NULL}$ 的 k_x 个子节点集合，若找不到这样的集合 S_x，则 $DecryptNode(x)=\mathrm{NULL}$，否则按式(10)计算，其中， $\Delta_{i,S_x^{'}}$ 为拉格朗日系数[13]。

$$F_x=\prod_{z\in S_x}F_z^{\Delta_{i,S_x^{'}}(0)}=\prod_{z\in S_x}e(g,g)^{trq_x(i)\Delta_{i,S_x^{'}}(0)}=e(g,g)^{trq_x(0)} \tag{10}$$

利用拉格朗日插值定理[13]，可得

$$V=DecryptNode(R)=e(g,g)^{trs} \tag{11}$$

随后，搜索服务器利用私钥 SSK，计算如式(12)。

$$T_2^{'} = \frac{T_2^{x}}{T_3} = H_2(W)^{tx} \tag{12}$$

搜索服务器利用双线性算法根据式(13)、式(14)和式(15)分别计算 X， Y， Z。最后根据式(16)得出返回值 b， $b \in \{0,1\}$。

$$X = e(H, T_0) \tag{13}$$

$$Y = e(W_1, T_1) \tag{14}$$

$$Z = e(W_2, T_2^{'}) \tag{15}$$

$$\frac{Y}{V} = \frac{X}{Z} \tag{16}$$

7) $\text{TEncrypt}(T_0, M) \to (\tilde{M}, L)$

TEncrypt 算法由搜索服务器执行。M 是搜索服务器搜索完数据之后生成的元素，且 $M \in G$。TEncrypt 是为了防止恶意用户截获返回结果并进行在线关键词猜测攻击。搜索服务器随机选取 $n \in Z_p$，生成密文，如式(17)所示。

$$n \in Z_p, \tilde{M} = MT_0^{n}, L = g^{\beta n} \tag{17}$$

8) $\text{TDecrypt}(t, \tilde{M}, L) \to M$

TDecrypt 算法由数据用户执行。当数据用户获得搜索服务器返回的搜索结果加密信息 $\tilde{M}$，利用 Trap 算法阶段生成的随机数秘密 t，进行解密计算，如式(18)所示。

$$M = \frac{\tilde{M}}{L^{t}} \tag{18}$$

5　实验结果与分析

5.1　正确性分析

该节对 Test 算法正确性进行分析。检索服务器将搜索凭证 TR 和关键词密文 CT 进行匹配计算。首先根据式(13)，得出中间结果 X，如式(19)所示。其次，根据式(14)，得出中间结果 Y，如式(20)所示。最后根据式(15)，得出中间结果 Z，如式(22)所示。

$$X = e(H, T_0) = e(g,g)^{\alpha\beta st} e(H_2(W, g)^{\beta kt}) \tag{19}$$

$$Y = e(W_1, T_1) = e(g,g)^{\alpha\beta ts + rts} \tag{20}$$

$$V = DecryptNode(CT, SK, R) = e(g,g)^{rts} \tag{21}$$

$$Z = e(W_2, T_2^{'}) = e(H_2(W), g)^{\beta kt} \tag{22}$$

最终结合式(16)，得出最终计算结果，如式(23)所示，由此可证方案是正确的。

$$\left(\frac{Y}{V}\right) = \left(\frac{X}{Z}\right) = e(g,g)^{\alpha\beta st} \tag{23}$$

5.2　安全性分析

访问控制：本方案采用了基于密文策略的属性基加密技术，数据属主可以灵活地指定访问控制策略，仅当用户满足访问控制策略时才有解密的能力。若用户不满足访问控制策略，则无法恢复出关键词密文秘密，也就无法判断密文是否包含相应关键词。

抗共谋：抗共谋要求拥有不同属性的用户即使将各自的私钥和对方的私钥组合在一起，也无法解密相应的密文，在可搜索加密方案中，要求即使用户合谋，也无法搜索无权限的关键词密文。本方案中，用户私钥 r 是随机选取的，每个用户的 r 各不相同，能够恢复秘密值 $e(g,g)^{rts}$ 各不相同。故而本方案具有抗共谋性质。

关键词密文机密性：若攻击者想要破解 H，用户在已知系统公钥，服务器公钥的情况下，由于 k 为 W_2 的指数，攻击者无法解决离散对数困难问题，故只能利用双线性映射技术对关键词进行猜解。攻击者不得不对 H 与 g^{β} 进行双线性运算。得到 $e(g,g)^{\alpha\beta s} e(g, H_2(W))^{\beta t}$，根据 DBDH 困难问题，对于攻击者来说，无法区分 $e(g,g)^{z} e(g, H_2(W))^{\beta t}$，所以，关键词密文是安全的。

搜索凭证安全性：安全的加密搜索方案要求搜索凭证能够抵抗离线关键词猜测攻击。由于本文方案要求用户上传搜索凭证前，需要首先指定安全搜索服务器，关键词相关的项由随机选取的 g^{y} 保护，根据离散对数困难问题，攻击者只能利用双线性对 T_2 和 g^{x} 进行计算，但是，生成的 $e(g, H_2(W))^{tx}$ 同样需要用户解决 DBDH 问题。故而搜索凭证能够抵御离线关键词猜测攻击。

用户私钥安全性：本方案支持用户根据自己的私钥自行生成搜索凭证，所以需要保证搜索凭证无法被其他恶意用户二次利用。由于用户在上传搜索凭证时，利用随机数对 K，以及 E_j 和 $E_j^{'}$ 进行指数运算，只能与 T_2 一起计算，所以即使攻击者截获上传的搜索凭证，也不能用于生成其他搜索凭证。

信道安全性：因为用户在加密关键词和加密搜索凭证时都指定了搜索服务器，使用了搜索服务器的公钥，即使恶意用户同时截获了加密关键词密文与搜索凭证，没有搜索服务器私钥也无法执行 *TEST*

算法。

服务器返回结果安全性：首先，T_0 不可伪造，若第三方截获 T_0 并修改，则服务器无法正常进行 Test 算法；其次，即使攻击者截获了 $\tilde{M}$，由于攻击者不知道秘密值 t，只能通过解决 CDH 问题来破解密文，所以服务器返回结果是安全的。

5.3 功能分析

本文将提出的方案和近几年提出的 PEKS 方案进行比较，并说明本方案的优势。表 1 主要从是否需要安全信道、能否抵抗离线关键词猜测攻击、能否抵抗在线关键词猜测攻击、是否支持权限控制、是否不依赖授权机构生成搜索凭证 5 个方面进行比较。

表 1 方案功能对比

方案	不需要安全信道	抵抗离线关键词猜测攻击	抵抗在线关键词猜测攻击	权限控制	不需要授权机构生成搜索凭证
SCF-PEKS[3]	是	否	否	否	是
dPEKS[4]	是	是	否	否	是
SPEKS[10]	是	是	是	否	是
ATT-PEKS[18]	否	否	否	是	是
VABKS[21]	否	否	否	是	是
ABEKS[15]	否	是	否	是	否
本方案	是	是	是	是	是

结合表 1 的功能分析，本方案无需安全信道，可抵抗在线离线关键词猜测攻击，支持多用户访问控制，支持搜索凭证自生成，更适合云环境下应用。

5.4 性能分析

本方案通过实验分析执行效率。实验设备为 Intel Core i5，2.60 GHz，操作系统为 Windows 7, 64 位。基于斯坦福大学的 JPBC2.0 开源库[25]。方案选取 JPBC 中 A 类型椭圆曲线。该曲线构建于 512 位有限域的超奇异曲线 $y^2=x^3+x$，提供了 160 位阶椭圆曲线群。

根据实验结果分析，基于类型 A 的双线性对计算时间为 32 ms，G_0 群上的指数计算时间为 30 ms，G_1 群上的指数计算时间为 20 ms。

实验主要对数据属主的加密算法、数据用户的搜索凭证生成算法以及服务器的搜索算法的时间代价进行分析。图 2 展示了典型算法执行效率，其中横轴为属性个数，纵轴为算法执行时间。

实验结果表明，各个算法和属性数量大致成正比关系，在现实应用中，即使面对海量用户，检索时间仅跟属性数量有关，所以适用于多用户云环境，并且，在实际应用中，加密和搜索时，一般不会设置超过 10 个以上的属性策略，所以本方案耗费的时间在可接受范围。

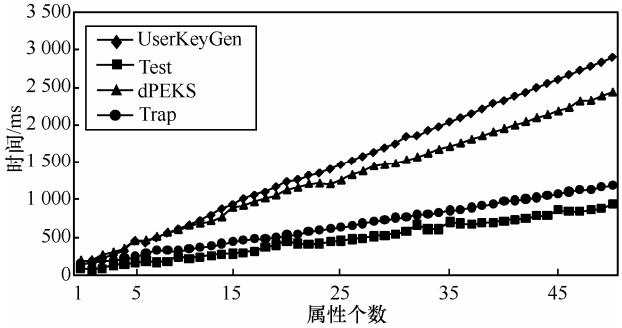

图 2 实验结果

6 结束语

本文主要是针对关键词可搜索加密方案的权限控制，无安全信道和关键词猜测攻击方面进行分析，提出了适合应用于云环境的关键词可搜索加密方案。在下一步研究中，将以属性基方案中常见的问题作为切入点，比如从用户撤销、多授权机构、用户匿名、可验证性、访问结构几个方面继续研究，使该方案最终能成熟地应用于云环境中。

参考文献：

[1] BONEH D, DI CRESCENZO G, OSTROVSKY R, *et al*. Public key encryption with keyword search[A]. Advances in Cryptology-Eurocrypt 2004[C]. Springer Berlin Heidelberg, 2004.506-522.

[2] ABDALLA M, BELLARE M, CATALANO D, *et al*. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions[A]. Advances in Cryptology–CRYPTO 2005[C]. Springer Berlin Heidelberg, 2005.205-222.

[3] BYUN J W, RHEE H S, PARK H A, *et al*. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[A]. Secure Data Management[C]. Springer Berlin Heidelberg, 2006.75-83.

[4] RHEE H S, PARK J H, SUSILO W, *et al*. Trapdoor security in a searchable public-key encryption scheme with a designated tester[J]. Journal of Systems and Software, 2010, 83(5): 763-771.

[5] HU C, LIU P. A secure searchable public key encryption scheme with a designated tester against keyword guessing attacks and its extension[A]. Advances in Computer Science, Environment, Ecoinformatics, and Education[C]. Springer Berlin Heidelberg, 2011.131-136.

[6] TANG Q, CHEN L. Public-key encryption with registered keyword search[A]. Public Key Infrastructures, Services and Applications[C]. Springer Berlin Heidelberg, 2010.163-178.

[7] XU P, JIN H, WU Q, *et al*. Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack[J]. IEEE Transactions on Computers, 2013, 62(11): 2266-2277.

[8] 李经纬, 贾春福, 刘哲理, 等. 可搜索加密技术研究综述[J]. 软件

学报, 2015, 26(1): 109-128.
LI J W, JIA C F, LIU Z L, *et al*. Survey on the searchable encryption[J]. Journal of Software, 2015, 26(1): 109-128.

[9] JEONG I R, KWON J O, HONG D, *et al*. Constructing PEKS schemes secure against keyword guessing attacks is possible[J]. Computer Communications, 2009, 32(2): 394-396.

[10] CHEN Y C. SPEKs: secure server-designation public key encryption with keyword search against keyword guessing attacks[J]. The Computer Journal, 2015, 58(4): 922-933.

[11] HWANG Y H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[A]. Pairing-Based Cryptography-Pairing 2007[C]. Springer Berlin Heidelberg, 2007.2-22.

[12] 苏金树, 曹丹, 王小峰, 等. 属性基加密机制[J]. 软件学报, 2011, 22(6):1299-1315.
SU J S, CAO D, WANG X F, *et al*. Attribute-based encryption schemes[J]. Journal of Software,2011,22(6):1299-1315.

[13] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Security and Privacy, SP'07[C]. 2007. 321-334.

[14] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. ACM, 2006.89-98.

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

[16] LV Z, HONG C, ZHANG M, *et al*. Expressive and Secure Searchable Encryption in the Public Key Setting (Full Version)[R]. Cryptology ePrint Archive, Report 2014/614, 2014.

[17] LAI J, ZHOU X, DENG R H, *et al*. Expressive search on encrypted data[A]. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security[C]. ACM, 2013. 243-252.

[18] 李双, 徐茂智. 基于属性的可搜索加密方案[J]. 计算机学报, 2014, 37(5): 1017-1024.
LI S, XU M Z. Attribute based public encryption with keyword search[J]. Chinese Journal of Computers, 2014, 37(5):1017-1024.

[19] WANG C, LI W, LI Y, *et al*. A ciphertext-policy attribute-based encryption scheme supporting keyword search function[A]. Cyberspace Safety and Security[C]. 2013. 377-386.

[20] LI J, ZHANG L. Attribute-based keyword search and data access control in cloud[A]. Computational Intelligence and Security (CIS), 2014 Tenth International Conference[C]. IEEE, 2014.382-386.

[21] LIU P, WANG J, MA H, *et al*. Efficient verifiable public key encryption with keyword search based on KP-ABE[A]. Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference on[C]. IEEE, 2014.584-589.

[22] ZHENG Q, XU S, ATENIESE G. Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data[R]. Cryptology ePrint Archive, Report 2013/462, 2013.

[23] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[A]. Advances in Cryptology,CRYPTO 2001[C]. Springer Berlin Heidelberg, 2001.213-229.

[24] GOH E J, JARECKI S. A signature scheme as secure as the Diffie-Hellman problem[A]. Advances in CryptologyEUROCRYPT 2003[C]. Springer Berlin Heidelberg, 2003.401-415.

[25] DE C A, IOVINO V. JPBC: Java pairing based cryptography[A]. IEEE Symposium on Computers & Communications[C]. IEEE Computer Society, 2011.850-855.

作者简介：

林鹏（1990-），男，浙江温州人，浙江工业大学硕士生，主要研究方向为信息安全。

江颉（1972-），女，浙江平湖人，博士，浙江工业大学副教授，主要研究方向为网络信息安全、数据挖掘。

陈铁明（1978-），男，浙江诸暨人，博士，浙江工业大学副教授，主要研究方向为网络信息安全。