抗关键词猜测的授权可搜索加密方案

曹素珍 郎晓丽* 刘祥震 张玉磊 王 斐
(西北师范大学计算机科学与工程学院 兰州 730070)

摘 要：大多数可搜索加密方案仅支持对单关键词集的搜索，且数据使用者不能迅速对云服务器返回的密文进行有效性判断，同时考虑到云服务器具有较强的计算能力，可能会对关键词进行猜测，且没有对数据使用者的身份进行验证。针对上述问题，该文提出一个对数据使用者身份验证的抗关键词猜测的授权多关键词可搜索加密方案。方案中数据使用者与数据属主给授权服务器进行授权，从而验证数据使用者是否为合法用户；若验证通过，则授权服务器利用授权信息协助数据使用者对云服务器返回的密文进行有效性检测；同时数据使用者利用服务器的公钥和伪关键词对关键词生成陷门搜索凭证，从而保证关键词的不可区分性。同时数据属主在加密时，利用云服务器的公钥、授权服务器的公钥以及数据使用者的公钥，可以防止合谋攻击。最后在随机预言机模型下证明了所提方案的安全性，并通过仿真实验验证，所提方案在多关键词环境下具有较好的效率。

关键词：可搜索加密；抗关键词猜测；授权验证；多关键词搜索；数据使用者身份验证
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)09-2180-07
DOI: 10.11999/JEIT181103

Delegate Searchable Encryption Scheme Resisting Keyword Guess

CAO Suzhen LANG Xiaoli LIU Xiangzhen ZHANG Yulei WANG Fei
(*College of Computer Science and Engineering, Northwest Normal University, Lanzhou* 730070, *China*)

Abstract: Most existing searchable encryption schemes only support the search for keyword sets, and the data users can not quickly identify the file keyword information returned by the server. Meanwhile, considering the server has strong computing power, it may judge keyword information from single keywords and the identity of the data consumer is not verified. In this paper, the data user and data owner are delegated server to verify whether the data ueer is a legitimate user; if legal, the delegated server can detect the validity of the return ciphertext with data user. The data user uses the server public key, keywords and pseudo-keywords to generate trapdoor, in order to ensure the indistinguishable of the keywords, a delegated multi-keyword searchable encryption scheme is designed, which is resistant to keyword guessing of data user authentication. Meanwhile, when the data owner encrypts, the public key of the cloud server, the delegated server, and the data user can be used to prevent collusion attacks. In the random oracle model the security of the proposed scheme is proved. The experiment results show that the scheme is efficient under the multi-keyword environment.

Key words: Searchable encryption; Keyword guessing attack; Delegate verification; Multi-keyword search; Data user verification

1 引言

2000年，Song等人[1]首次给出了可搜索加密，该方案实现了对密文的检索，解决了用户把数据以密文的形式存储到云服务器但用户如何从云服务器下载该密文的问题。可搜索加密方案被广泛应用到云[2]环境领域中。自此，可搜索加密成为密码学与网络安全领域的研究热门[3–6]。文献[7]提出了公钥可搜索加密方案，随后文献[8]对该方案进一步完善。文献[9]提出了密钥聚合的可搜索加密方案，文献[10]指出该方案存在离线关键字猜测攻击。

文献[11]提出了满足陷门不可区分性的公钥可搜索加密方案，该方案在陷门生成阶段利用服务器公钥进行运算，从而可以在公开信道下传输。文献[12]构造了一种陷门无法识别的可搜索加密方案，但是该方案不能抵抗关键词猜测攻击。文献[13]提出了对称可搜索加密方案，但是该方案的执行效率较低。

收稿日期：2018-11-28；改回日期：2019-03-12；网络出版：2019-03-28
*通信作者： 郎晓丽 1452420594@qq.com
基金项目：国家自然科学基金(61662071, 61662069, 61462077)；甘肃省高等学校科研项目(2017A-003, 2018A-207)
Foundation Items: The National Natural Science Foundation of China (61662071, 61662069, 61462077);The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2018A-207)

目前，已有的大部分可搜索加密方案仅支持对单关键词集的搜索，而基于授权的可搜索加密方案可以对云服务器返回的密文进行有效性检测并可以实现对多关键词的加密与检索。一旦用户将授权信息发送给授权服务器，授权服务器就可以利用授权信息自己创建陷门来执行密文有效性检测。并在数据使用者不改变密钥的前提下仅需授权一次[14]。文献[15]重新定义了基于授权的公钥可搜索加密，该方案将服务器分为授权服务器和搜索服务器，数据使用者只对授权服务器发送授权信息即可。文献[16]提出了支持多关键词搜索的公钥可搜索加密方案，该方案在不同的属性位置不会出现相同的关键词。

本文基于文献[16]提出了一个抗关键词猜测的多关键词授权可搜索加密方案，同时将文献[15]中的授权扩展为两部分，一部分为数据属主对服务器进行授权，另一部分为数据使用者对服务器进行授权，授权服务器同时收到这两部分的授权信息时对数据使用者的身份进行验证，从而保证了数据使用者的身份有效性。若数据使用者为合法用户，则授权服务器从授权信息中计算出该部分私钥，协助数据使用者对云服务器返回的密文进行有效性检测；数据使用者利用随机数、服务器的公钥、伪关键词来生成陷门搜索凭证，从而保证在公开信道下陷门信息能够抵抗关键字猜测攻击。数据属主在上传密文时利用了服务器的公钥、授权服务器的公钥以及数据使用者的公钥，一方面满足了上传密文时不需要安全信道；另一方面可以防止不诚实的数据使用者与授权服务器或者是云服务器进行合谋攻击。最后本文通过仿真实验来验证方案的效率，实验结果表明本文方案能够适用于云存储环境。

2　基础知识

(1) 双线性映射：G与G_T阶同为大素数q的乘法循环群。P是G的生成元：

(a) 线性：对于所有的$P\in G$, $a,b\in Z_q^*$未知，满足$e(aP,bP)=e(P,P)^{ab}$。

(b) 非退化性：存在$P\in G$，使得$e(P,P)\neq 1$，1为G_T单位元。

(c) 可计算性：对于任意的$P,Q\in G$，使得$e(P,Q)$有一个有效计算值。

(2) 计算双线性Diffie-Hellman问题(Computational Bilinear Diffie-Hellman problem, CBDH)：对于任意未知的$a,b\in Z_q^*$，给定(g,g^a,g^b)，计算$e(g,g)^{ab}$是困难的。

(3) 判定性双线性Diffie-Hellman问题(Decisional Diffie-Hellman problem, DDH)：对任意未知的$a,b,c\in Z_q^*$未知，给定(g,g^a,g^b,g^c)，判断$c=ab$是困难的。

3　基本方案

3.1　系统模型

系统主要包括数据属主、数据使用者、云服务器和授权服务器4个主体。其中，两个服务器是诚实但好奇的，既能够诚实地根据数据使用者的需求返回相对应的服务请求，也会在通信过程中尝试窃取用户的隐私。如图1所示。

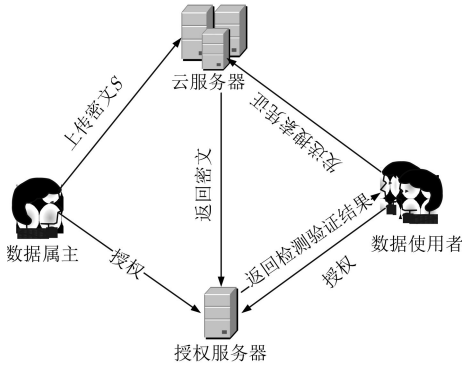

图 1 系统模型图

(1) 数据属主：数据的拥有者，将分享的密文S上传到云服务器；对授权服务器进行授权。

(2) 数据使用者：对明文关键词Ωw_j生成搜索凭证T_w，发送给云服务器进行陷门匹配验证；对授权服务器进行授权以验证云服务器返回密文的有效性。

(3) 云服务器：接收陷门信息T_w，检测密文关键词中是否含有与陷门信息相匹配的关键词S。

(4) 授权服务器：授权服务器收到授权信息时，首先对数据使用者的身份进行验证，其次协助数据使用者对云服务器返回的密文进行有效性检测。

3.2　形式化定义

本文方案由以下10个算法组成：

(1) Setup：系统管理者执行，输出公共参数cp。

(2) CSKeyGen：云服务器执行，输入公共参数cp，利用公共参数cp输出公/私钥$(\mathrm{Pk_{CS}},\mathrm{Sk_{CS}})$。

(3) DSKeyGen：授权服务器执行，输入公共参数cp，利用公共参数cp输出公/私钥$(\mathrm{Pk_{DS}},\mathrm{Sk_{DS}})$。

(4) rKeyGen：数据使用者执行，输入公共参数cp，利用公共参数cp输出公/私钥$(\mathrm{Pk}_R,\mathrm{Sk}_R)$。

(5) SCF-PEKS：数据属主执行，输入公共参数cp、数据使用者的公钥Pk_R、云服务器的公钥

$\mathrm{Pk_{CS}}$以及授权服务器的公钥$\mathrm{Pk_{DS}}$，输出对明文关键词w的密文信息S。

(6) Trapdoor：数据使用者执行，输入公共参数cp、数据使用者的私钥Sk_R、云服务器的公钥$\mathrm{Pk_{CS}}$，输出对明文关键词Ωw_j的陷门信息T_w。

(7) Verify1：云服务器执行，输入公共参数cp、云服务器的私钥$\mathrm{Sk_{CS}}$、密文S以及陷门信息T_w，检测$(\Omega w_1 = w_1), (\Omega w_2 = w_2), \cdots, (\Omega w_t = w_t)$是否相等。若相等，返回1，即返回密文$(C_0, C_1')$给授权服务器，否则返回0。

(8) Delegate：数据使用者与数据属主执行，数据使用者输入数据使用者的私钥Sk_R、授权服务器的公钥$\mathrm{Pk_{DS}}$，输出授权信息$T_* = (t_1, t_2)$给授权服务器。数据属主利用授权服务器的公钥$\mathrm{Pk_{DS}}$，输出授权服务器的授权信息$T_* = (t_3, t_4)$。

(9) Verify2$(\mathrm{cp}, S, \mathrm{Sk}_S, T_*)$：授权服务器执行，输入私钥$\mathrm{Sk_{DS}}$、授权信息$T_*$以及收到的密文$(C_0, C_1')$，首先对数据使用者的身份进行验证；验证通过后检测密文的有效性，若密文有效，则把部分密文$(C_0, \tilde{M})$发送给数据使用者。

(10) Decrypt：数据使用者执行，利用自己的私钥对收到的部分密文$(C_0, \tilde{M})$进行解密。

4 方案设计

4.1 方案构造

(1) Setup：输入安全参数λ，选择G和G_T阶为$q > 2^\lambda$大素数的循环群，选择双线性映射$e: G \times G \to G_T$，其中g为群G的生成元，选择$g_1 \in G$和3个散列函数$H, H_1: \{0,1\}^* \to G$, $H_2: G_T \to G$。公开系统参数$\mathrm{cp} = \{G, G_T, e, q, g, g_1, H, H_1, H_2\}$。

(2) CSKeyGen：输入公共参数cp，云服务器随机选择$\alpha_1 \in \mathrm{Z}_q^*$，私钥为$\mathrm{Sk_{CS}} = \alpha_1$。公钥为$\mathrm{Pk_{CS}}=g^{\alpha_1}$。

(3) DSKeyGen：输入公共参数cp，授权服务器随机选择$\alpha_2 \in Z_q^*$，私钥为$\mathrm{Sk_{DS}} = \alpha_2$。公钥为$\mathrm{Pk_{DS}}= (\mathrm{Pk_{DS,1}}, \mathrm{Pk_{DS,2}}) = (g^{\alpha_2}, g_1^{\alpha_2})$。

(4) rKeyGen：输入公共参数cp，数据使用者随机选择$\beta, \chi \in Z_q^*$，私钥为$\mathrm{Sk}_R = \beta\chi$。公钥为$\mathrm{Pk}_R= g^{\beta\chi}$。

(5) SCF-PEKS：输入公共参数cp，数据使用者的公钥Pk_R，云服务器的公钥$\mathrm{Pk_{CS}}$，授权服务器的公钥$\mathrm{Pk_{DS}}$、明文关键词w，输出$w_i (1 \le i \le m)$的密文信息S。数据属主随机选择$k_i \in Z_q^*$，计算$C_0 = g^{k_i}$，$C_1 = H_1(w_i)(\mathrm{Pk}_R)^{k_i}(\mathrm{Pk_{CS}})^{k_i}(\mathrm{Pk_{DS},2})^{k_i} = H_1(w_i) g^{\beta\chi k_i} g^{\alpha_1 k_i} g_1^{\alpha_2 k_i}$。将关键词密文$S = \{C_0, C_1\}$上传至云服务器。

(6) Trapdoor：数据使用者的私钥Sk_R、云服务器的公钥$\mathrm{Pk_{CS}}$、明文关键词$\Omega w_j (1 \le j \le t)$，数据使用者随机选择$\tilde{a} \in \{0,1\}^*$, $r' \in Z_q^*$，计算$T_1 = g_1^{r'}$，$T_2 = \Big[\mathrm{Pk_{CS}}(H_1(\Omega w_1) + H_1(\Omega w_2) + \cdots + H_1(\Omega w_t))^{\beta^{-1}} + H_1(\tilde{a})^{\beta^{-1}}\Big] \oplus H_2\left(e\left(\mathrm{Pk}_R^{\mathrm{Sk}_R}, \mathrm{Pk_{CS}}^{r'}\right)\right)$, $T_3 = H_1(\tilde{a})^{\beta^{-1}}$。将$T_w = (T_1, T_2, T_3)$给云服务器。

(7) Verify1：由云服务器执行，云服务器首先计算$T_2' = T_2 \oplus H_2\left(e\left(\mathrm{Pk}_R^{\mathrm{Sk_{CS}}}, T_1^{\mathrm{Sk_{CS}}}\right)\right)$, $T_3' = T_2' - T_3$，检查$\dfrac{e(C_0, T_3')}{e(C_0, g)^{\mathrm{Sk_{CS}}}} = e\left(g^{k_i}, H_1(\Omega w_j)^{\beta^{-1}}\right)$是否相等，若相等输出1，即返回密文$(C_0, C_1')$给授权服务器，其中$C_1' = C_1 / C_0^{\mathrm{Sk_{CS}}}$；否则，输出0。

(8) Delegate：由数据使用者与数据属主分别对授权服务器进行授权。

(a) 数据使用者授权：输入私钥Sk_R、授权服务器的公钥$\mathrm{Pk_{DS}}$，数据使用者随机选择$r' \in Z_q^*$，计算$t_1 = \beta g^{\alpha_2 \cdot r'}$, $t_2 = g^{r'}$，将$T_* = (t_1, t_2)$给授权服务器。授权服务器利用自己私钥$\mathrm{Sk_{DS}}$，得到$\beta = t_1 / t_2^{\alpha_2}$。

(b) 数据属主授权：输入授权服务器的公钥$\mathrm{Pk_{DS}}$，数据属主随机选择$k_i \in Z_q^*$，计算$t_3 = g_1^{\alpha_2 k_i}$, $t_4 = g_1^{k_i}$，输出授权信息$T_* = (t_3, t_4)$给授权服务器。

(9) Verify2：由授权服务器执行，输入私钥$\mathrm{Sk_{DS}}$、授权信息T_*，当Verify1阶段返回密文C_1'时，首先计算$e(t_3, t_2) = e\left(\beta^{-1} t_1, t_4\right)$，若相等，则说明数据使用者是合法用户，计算$\tilde{M} = \dfrac{C_1'}{t_4^{\mathrm{Sk_{DS}}}}$，将$(C_0, \tilde{M})$返回给数据使用者；否则说明数据使用者是不合法的用户。

(10) Decrypt：由数据使用者执行，当数据使用者从授权服务器那里得到加密的消息$(C_0, \tilde{M})$，利用私钥Sk_R进行解密得到关键词信息$H_1(w_i) = \dfrac{\tilde{M}}{C_0^{\mathrm{Sk}_R}}$。

4.2 方案的正确性

$$\begin{aligned} T_2' &= T_2 \oplus H_2\left(e\left(\mathrm{PK}_R^{\mathrm{Sk_{CS}}}, T_1^{\mathrm{Sk_{CS}}}\right)\right) \\ &= T_2 \oplus H_2\left(e\left(g^{\beta\chi \cdot \alpha_1}, g^{r'\alpha_1}\right)\right) \\ &= \mathrm{Pk_{CS}}(H_1(\Omega w_1) + H_1(\Omega w_2) + \cdots \\ &\quad + H_1(\Omega w_t))^{\beta^{-1}} + H_1(\tilde{a})^{\beta^{-1}} \end{aligned} \tag{1}$$

$$\begin{aligned} T_3' &= T_2' - T_3 = \mathrm{Pk_{CS}}(H_1(\Omega w_1) + H_1(\Omega w_2) \\ &\quad + \cdots + H_1(\Omega w_t))^{\beta^{-1}} + H_1(\tilde{a})^{\beta^{-1}} - H_1(\tilde{a})^{\beta^{-1}} \\ &= \mathrm{Pk_{CS}}(H_1(\Omega w_1) + H_1(\Omega w_2) + \cdots \\ &\quad + H_1(\Omega w_t))^{\beta^{-1}} \end{aligned} \tag{2}$$

$$\frac{e(C_0, T_3')}{e(C_0, g)^{\mathrm{Sk_{CS}}}} = \frac{e\left(g^{k_i}, \mathrm{Pk_{CS}}(H_1(\Omega w_1)+H_1(\Omega w_2)+\cdots+H_1(\Omega w_t))^{\beta^{-1}}\right)}{e(g^{k_i}, g)^{\alpha_1}}$$
$$= \frac{e\left(g^{k_i}, g^{\alpha_1}\right) e\left(g^{k_i}, (H_1(\Omega w_1)+H_1(\Omega w_2)+\cdots+H_1(\Omega w_t))^{\beta^{-1}}\right)}{e(g^{k_i}, g)^{\alpha_1}} = e\left(g^{k_i}, H_1(\Omega w_j)^{\beta^{-1}}\right) \tag{3}$$

$$C_1' = \frac{C_1}{C_0^{\mathrm{Sk_{CS}}}} = \frac{H_1(w_i) g^{\beta\chi k_i} g^{\alpha_1 k_i} {g_1}^{\alpha_2 k_i}}{g^{k_i\alpha_1}}$$
$$= H_1(w_i) g^{\beta\chi k_i} {g_1}^{\alpha_2 k_i} \tag{4}$$

$$\tilde{M} = \frac{C_1'}{t_4^{\mathrm{Sk_{DS}}}} = \frac{H_1(w_i) g^{\beta\chi k_i} {g_1}^{\alpha_2 k_i}}{{g_1}^{k_i\alpha_2}}$$
$$= H_1(w_i) g^{\beta\chi k_i} \tag{5}$$

$$\frac{\tilde{M}}{C_0^{\mathrm{Sk}_{R,1}\mathrm{Sk}_{R,2}}} = \frac{H_1(w_i) g^{\beta\chi k_i}}{g^{k_i\beta\chi}} = H_1(w_i) \tag{6}$$

5　安全性分析

5.1 抗合谋攻击

若数据使用者为不诚实的用户，与授权服务器或者云服务器进行合谋也无法恢复出消息。本文方案加密算法中数据属主是利用云服务器的公钥、授权服务器的公钥与数据使用者的公钥进行加密。因此，数据使用者与授权服务器进行合谋也无法恢复出消息；与云服务器进行合谋也无法恢复出消息。云服务器与授权服务器合谋也无法恢复出消息。

5.2 密文不可区分性

定理 1　假设问题DDH困难，随机预言模型下的敌手A_{I}, A_{II}与A_{III}对该方案在适应性选择明文攻击下密文不可区分性的证明是安全的。

该定理的证明需要以下3个引理来证明。

引理 1　随机预言模型下A_{I}能以不可忽略优势ε攻破本文方案，其中，A_{I}为恶意的云服务器。则挑战者C就能以不可忽略的概率$\varepsilon' \geq \left(1-\frac{q_T}{n}\right)\frac{1}{n}\frac{\varepsilon}{2}$解决DDH问题，其中，$q_T$为Trapdoor询问的执行次数，$n$为数据用户的数量。

证明　挑战者C输入DDH问题的实例(g, g^a, g^b, g^c)，目标是计算$c=ab$。

(1) 初始化：挑战者C运行Setup算法，公开系统参数cp; A_{I}运行算法CSKeyGen，生成公私钥$\mathrm{Pk_{CS}} = g^{\alpha_1}$, $\mathrm{Sk_{CS}} = \alpha_1$。

(2) KeyGen询问：C运行算法rKeyGen，生成数据接收者R的公钥，C随机选择$\beta, \chi \in \mathrm{Z}_q^*$，设置$\mathrm{Pk}_R = {g_1}^{\beta\chi}$，把公钥$\mathrm{Pk}_R$给$A_{\mathrm{I}}$。若询问关于目标接收者$R^*$的身份时，设置公钥为$\mathrm{Pk}_R^* = g^a$；同时$C$运行算法DSKeyGen，生成授权服务器的公钥，$C$计算$\mathrm{Pk}_{\mathrm{DS},1} = g^{\alpha_2}$, $\mathrm{Pk}_{\mathrm{DS},2} = g^b$，把公钥$\mathrm{Pk_{DS}}$给$A_{\mathrm{I}}$。

(3) H_1询问：C维护H_1^1列表，元组为$(w_i, \tilde{a}_i, c_i, h_i, h_a)$，初始为空。$A_{\mathrm{I}}$对$w_i \in \{0,1\}^*$进行询问时，$C$首先查$H_1^1$表，若表中存在，$C$就把相应的$h_i$给$A_{\mathrm{I}}$；否则，$C$随机选择$c_i \in \{0,1\}$，若$c_i = 0$, C随机选择$e_i \in Z_q^*$，计算$H_1(w_i) = g^{xe_i}$。若A_{I}对$H_1(\tilde{a})$询问时，C首先查H_1^1表，若表中存在，C就把相应的h_a给A_{I}；否则，C随机数选择$h_a \in G$给A_{I}；并增加该元组到表H_1^1中。

(4) H_2询问：C维护列表$H_2 = \{t, v\}$，当A_{I}询问$t \in G_T$时，C首先检查H_2列表，若询问已存在列表中，就返回相应的值；否则C随机选择$v \in G$，计算$H_2(t) = v$，保存该元组到表H_2中并返回给A_{I}。

(5) Delegate询问：A_{I}请求接收者R的陷门授权时，C随机选择$r_1 \in Z_q^*$，计算$t_1 = \beta g^{\alpha r_1}$, $t_2 = {g_1}^{r_1}$, $t_3 = {g_1}^{\alpha_2 k_i}$, $t_4 = {g_1}^{k_i}$，输出授权信息$T_* = (t_1, t_2, t_3, t_4)$给$A_{\mathrm{I}}$；否则，$C$中止。

(6) Trapdoor询问：当A_{I}询问关键字w的陷门T_w时，C首先检查列表H_1^1，若列表存在该元组，C就返回相应的值；若$c_i = 0$, C终止；否则，C随机地选择$r' \in Z_q^*$和$\tilde{a} \in \{0,1\}^*$，计算$T_1 = g^{r'}$, $T_2 = \left[\mathrm{Pk_{CS}}(H_1(\Omega w_1)^{\beta^{-1}}+H_1(\Omega w_2)^{\beta^{-1}}+\cdots+H_1(\Omega w_t)^{\beta^{-1}}\right]$和$T_3 = H_1(\tilde{a})^{\beta^{-1}}$。最后$C$将$(T_1, T_2, T_3)$发送给$A_{\mathrm{I}}$。

(7) Challenge: A_{I}选择关键词w_0和w_1，设置$H_1(w_0) = h_0$, $H_1(w_1) = h_1$，其中$h_0, h_1 \in G$。若$R = R^*$，则C随机选择$b \in \{0,1\}$并输出密文$S_b = \{{C_0}^b, {C_1}^b\} = \{g^c, H_1(w_i) C_u\}$；若$R \neq R^*$，则$C$终止。

(8) Trapdoor询问：A_{I}继续进行陷门询问，但不允许将w_0, w_1进行Trapdoor询问。

(9) Guess: A_{I}输出猜测值$b' \in \{0,1\}$，若$b' = b$，则A_{I}能以不可忽略的优势区分密文S^*，即$C_u = g^{abc}$，对于C来说，他无法解决DDH困难问题；否则，返回0。　　证毕

引理 2　在随机预言机模型下A_{II}能以不可忽略优势ε攻破本文方案，其中，A_{II}为恶意数据使用者。则挑战者C以不可忽略的概率$\varepsilon' \geq \left(1-\frac{q_T}{n}\right)\cdot\left(1-\frac{q_{H1}}{n}\right)\frac{1}{n}\frac{\varepsilon}{2}$解决DDH问题的实例，其中$q_{H_1}$, q_T分别为H_1询问次数、Trapdoor询问的执行次数，n为数据用户的数量。

证明 挑战者C输入DDH问题的实例(g, g^a, g^b, g^c)，目标是计算$c=ab$。

(1) 初始化：挑战者C运行Setup算法，公开系统参数cp; A_{II}运行算法rKeyGen生成数据使用者的公钥，随机选择$\beta, \chi \in \mathrm{Z}_q^*$，计算$A_{\text{II}}$公钥$\mathrm{Pk}_R=g^{\beta\chi}$，私钥为$\mathrm{Pk}_R=(\beta,\chi)$。

(2) KeyGen询问：当C收到对云服务器的公钥询问时，C运行算法CSKeyGen，计算公钥$\mathrm{Pk}_{\mathrm{CS}}=g^a$给敌手$A_{\text{II}}$。当收到对授权服务器的公钥询问时，$C$运行算法DSKeyGen，计算$\mathrm{Pk}_{\mathrm{DS},1}=g^{\alpha_2}$, $\mathrm{Pk}_{\mathrm{DS},2}=g^b$，将$\mathrm{Pk}_{\mathrm{DS}}=(\mathrm{Pk}_{\mathrm{DS},1}, \mathrm{Pk}_{\mathrm{DS},2})$给$A_{\text{II}}$。

(3) H_1询问：C维护H_1^1列表，元组为$(w_i, \tilde{a}_i, c_i, h_i, h_a)$，初始为空。当$A_{\text{II}}$对$w_i \in \{0,1\}^*$进行询问时，$C$首先查表$H_1^1$，若表中存在，$C$就把相应的$h_i$给$A_{\text{II}}$；否则，$C$随机选择$c_i \in \{0,1\}$，若$c_i=0$, C随机选择$e_i \in Z_q^*$计算$h_i=g^{e_i}$；若A_{II}对$H_1(\tilde{a})$询问时，C首先查H_1^1表，若表中存在，C就把相应的h_a给A_{II}，否则，随机数选择$h_a \in G$给A_{II}；并增加该元组到表H_1^1中。

(4) H_2询问，Delegate询问：同引理1。

(5) Challenge: A_{II}选择关键词w_0和w_1，设置$H_1(w_0)=h_0$, $H_1(w_1)=h_1$，其中$h_0, h_1 \in G$，C首先查表H_1^1，若$c_i=0$时，C终止；否则计算并输出密文$S_b=\{{C_0}^b, {C_1}^b\}=\{g^c, g^{e_i}C_u\}$，其中，$g^b$与$C_u$均来自困难问题的一个实例，只有当$C_u=g^{abc}$时，挑战密文的分布才和本文方案的密文分布相同。

(6) Guess: A_{II}输出猜测值$b' \in \{0,1\}$，若$b'=b$，即$C_u=g^{abc}$，对C来说，他无法解决DDH问题。否则，返回0。 证毕

引理 3 在随机预言机模型下A_{III}能以不可忽略优势ε攻破本文方案，其中，A_{III}为恶意授权服务器。则挑战者C能以不可忽略的概率$\varepsilon' \geq \left(1-\frac{q_T}{n}\right)\cdot\left(1-\frac{q_{H1}}{n}\right)\frac{1}{n}\frac{\varepsilon}{2}$解决DDH问题的实例，其中$q_{H_1}$, q_T分别为H_1询问次数、Trapdoor询问的执行次数，n为数据用户的数量。

证明 挑战者C输入DDH问题的实例(g, g^a, g^b, g^c)，目标是计算$c=ab$。

(1) 初始化：挑战者C运行Setup算法，公开系统参数cp; A_{III}运行算法DSKeyGen生成公私钥，随机选择$\alpha_1 \in Z_q^*$，计算公钥为$\mathrm{Pk}_{\mathrm{DS},1}=g^{\alpha_2}$, $\mathrm{Pk}_{\mathrm{DS},2}={g_1}^{\alpha_2}$，私钥为$\mathrm{Sk}_R=(\beta,\chi)$。

(2) KeyGen询问：当C收到对云服务器的公钥询问时，C执行算法CSKeyGen计算公钥$\mathrm{Pk}_{\mathrm{CS}}=g^a$给敌手$A_{\text{III}}$；当收到对数据使用者的公钥询问时，$C$执行算法rKeyGen，计算$\mathrm{Pk}_R=g^b$给$A_{\text{III}}$。

(3) H_1询问：与引理2中的H_1询问方式相同。

(4) H_2询问，Delegate询问：同引理1。

(5) Challenge: A_{III}选择关键词w_0和w_1，设置$H_1(w_0)=h_0$, $H_1(w_1)=h_1$，其中$h_0, h_1 \in G$，C首先查表H_1^1，若$c_i=0$时，C终止；否则计算并输出密文$S_b=\{{C_0}^b, {C_1}^b\}=\{g^c, g^{e_i}C_u\}$，其中，$g^b$与$C_u$均来自困难问题的一个实例，只有当$C_u=g^{abc}$时，挑战密文的分布才和本文方案的密文分布相同。

(6) Guess: A_{III}输出猜测值$b' \in \{0,1\}$，若$b'=b$，则A_{III}能以不可忽略的优势区分密文S^*，即$C_u=g^{abc}$，对于C来说，他无法解决DDH困难问题；否则，返回0。 证毕

5.3 陷门不可区分性

定理 2 假设CBDH问题是困难的，该方案在适应性选择消息下的陷门是不可区分性的。

引理 4 在随机预言机模型下A_{IV}能以不可忽略优势ε攻破本文方案，其中，A_{IV}为恶意的云服务器，则挑战者C就能以不可忽略的概率解决CBDH问题的一个实例。

证明 挑战者C输入CBDH问题的实例(g, g^a, g^b)，目标是计算$e(g,g)^{ab}$。

(1) 初始化：挑战者C公开系统参数cp; A_{IV}运行算法CSKeyGen，随机选择$\alpha_1 \in Z_q^*$。计算公钥$\mathrm{Pk}_{\mathrm{CS}}=g^{a\alpha_1}$。

(2) KeyGen询问：C运行算法rKeyGen，生成数据接收者R的公钥，C随机选择$\beta, \chi \in Z_q^*$，设置$\mathrm{Pk}_R=g^b$，把公钥Pk_R给A_{IV}。同时C运行算法DS-KeyGen，生成授权服务器的公钥，计算$\mathrm{Pk}_{\mathrm{DS},1}=g^{a\alpha_2}$, $\mathrm{Pk}_{\mathrm{DS},2}={g_1}^{\alpha_2}$，把公钥$\mathrm{Pk}_{\mathrm{DS}}$给$A_{\text{IV}}$。

(3) H_1询问，H_2询问，Delegate询问：同引理1中的H_1询问方式相同。

(4) Challenge：A_{IV}选择关键词w_0和w_1，设置$H_1(w_0)=h_0$, $H_1(w_1)=h_1$，其中$h_0, h_1 \in G$, C首先检查列表H_1^1，并随机选择$\tilde{a} \in \{0,1\}^*$, $r' \in Z_q^*$，计算$T_1^*=g^b$ ， $T_2^*=\left[g^{a\alpha_1}(H_1\left(\Omega w_1\right)^{\beta^{-1}}+H_1(\Omega w_2)^{\beta^{-1}}+\cdots+H_1(\Omega w_t)^{\beta^{-1}}\right)+H_1(\tilde{a})^{\beta^{-1}}\right]\oplus H_2\left(e\left(g^a, g^{b\alpha_1}\right)\right)$ 和$T_3^*=H_1(\tilde{a})^{\frac{1}{\beta}}$ 。将$T_w^*=(T_1^*, T_2*, T_3^*)$ 给A_{IV}。

(5) Guess: A_{IV}输出猜测值$b' \in \{0,1\}$，若$b'=b$，则A_{IV}成功解决CBDH问题。其中$e\left(g^a, g^{b\alpha_1}\right)=e(g,g)^{ab\alpha_1}$。

5.4 抗关键词猜测攻击

Rhee等人在文献[11]对关键词猜测攻击和陷门

不可区分性的关系给出：如果方案能满足陷门不可区分性则一定能满足关键词猜测攻击。

6　性能分析

本文方案和文献[6,12,15,16]在关键词抗暴力猜测、授权、双服务器以及是否满足公开信道等方面进行分析对比，比较结果如表1所示。与文献[6,12,15,16]相比，本方案能够抵抗关键词暴力猜测攻击，本方案利用随机比特串$\tilde{a}\in\{0,1\}^*$与随机数，使云服务器在执行算法Test1时无法区分出要搜索的关键词。即使接收者离线，服务器也无法进行猜测/伪造关键词。与文献[12,15,16]相比，本文方案是双服务器模式，其中云服务器执行算法Test1，授权服务器执行算法Test2，即对密文进行有效性检测。

通过理论数值分析，将本文方案和文献[15]与文献[16]在计算开销上进行比较。P表示为双线性对运算，E表示为指数运算，M表示为点乘运算。如表2所示，由于文献[15]是对单关键词进行加密，所以加密时间与陷门生成时间均为确定常数。在加密时间上，与文献[16]相比，本文方案不会随着关键词的增多而呈现线性增长，本文方案为确定性常数。在陷门生成时间上，本文方案即使增加了服务器的公钥，满足了在公开信道下的传输，但在计算时间上并没有增加额外的开销。在测试上，本文方案与文献[15]计算开销多一个点乘运算，但是，本文方案可以在一定程度上防止数据使用者为恶意用户的情况而得到全部的密文。

表 1　各方案功能比较

	文献[6]	文献[12]	文献[15]	文献[16]	本文方案
抗暴力猜测	×	×	×	×	√
授权	×	×	√	×	√
双服务器	√	×	√	×	√
多关键词	√	×	×	√	√
是否满足公开信道	√	×	×	×	√

表 2　计算效率对比

方案	加密	陷门生成	测试1	测试2
文献[15]	$2E$+$2M$	$2E$+$2M$	$4E$+$4P$	E+M+$2P$
文献[16]	$(n$+$2)M$+nP	$(n$+$1)M$	$(n$+$1)M$+P	×
本文方案	$4E$+$(n$+$3)M$	$6E$+M+P	$4E$+$4P$	E+$2M$+$2P$

实验环境为戴尔AW笔记本(I7-4700CPU频率3.10 GHz, 16 GB内存和Ubuntu Linux操作系统)。调用PBC库，对关键词数量分别取1000, 3000, 5000, 9000, 10000时加密时间如图2所示。当对关键词生成陷门时取关键词为1, 5, 10, 15, 20时陷门生成时间如图3所示。

通过图2发现，本文方案的加密时间明显低于文献[16]。通过图3可知，本文方案的陷门生成算法时间与关键词个数无关，但是文献[16]的陷门生成时间却与关键词的数量呈线性关系。

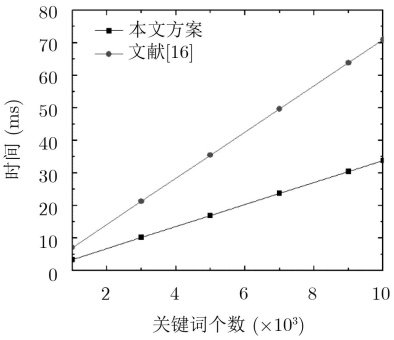

图 2 加密时间

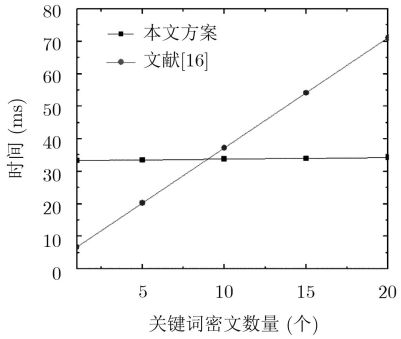

图 3 陷门生成时间

7　结束语

本文设计了一个抵抗关键字猜测攻击的多关键词授权可搜索加密方案，若数据使用者为合法用户，则协助数据使用者对云服务器返回的密文进行有效性检测；同时保证了云服务器与授权服务器的合谋攻击，也保证了数据接收者与授权服务器的合谋攻击。即使数据使用者为恶意的用户也无法通过授权服务器获得密文。并在随机预言模型下证明了方案满足密文不可区分和关键词不可区分，抗关键字猜测攻击。仿真实验结果表明，本文方案具有较好的

实现性能。但是，数据使用者把收到的密文解密后发给其他不合法的用户问题是下一步考虑的重点。

参 考 文 献

[1] SONG D X, WAGNER D, and PERRIG A. Practical techniques for searches on encrypted data[C]. Proceedings of 2000 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2000: 44–55. doi: 10.110SECPRI.2000.848445.

[2] LIU Zheli, WENG Jian, LI Jin, *et al*. Cloud-based electronic health record system supporting fuzzy keyword search[J]. *Soft Computing*, 2016, 20(8): 3243–3255. doi: 10.1007/s00500-015-1699-0.

[3] 王尚平, 刘利军, 张亚玲. 一个高效的基于连接关键词的可搜索加密方案[J]. 电子与信息学报, 2013, 35(9): 2266–2271. doi: 10.3724/SP.J.1146.2012.01036.
WANG Shangping, LIU Lijun, and ZHANG Yaling. An efficient conjunctive keyword searchable encryption scheme[J]. *Journal of Electronics & Information Technology*, 2013, 35(9): 2266–2271. doi: 10.3724/SP.J.1146.2012.01036.

[4] 黄海平, 杜建澎, 戴华, 等. 一种基于云存储的多服务器多关键词可搜索加密方案[J]. 电子与信息学报, 2017, 39(2): 389–396. doi: 10.11999/JEIT160338.
HUANG Haiping, DU Jianpeng, DAI Hua, *et al*. Multi-sever multi-keyword searchable encryption scheme based on cloud storage[J]. *Journal of Electronics & Information Technology*, 2017, 39(2): 389–396. doi: 10.11999/JEIT160338.

[5] 刘振华, 周佩琳, 段淑红. 支持关键词搜索的属性代理重加密方案[J]. 电子与信息学报, 2018, 40(3): 683–689. doi: 10.11999/JEIT170448.
LIU Zhenhua, ZHOU Peilin, and DUAN Shuhong. Attribute-based proxy re-encryption scheme with keyword search[J]. *Journal of Electronics & Information Technology*, 2018, 40(3): 683–689. doi: 10.11999/JEIT170448.

[6] TARIQ H and AGARWAL P. Secure keyword search using dual encryption in cloud computing[J]. *International Journal of Information Technology*, 2018(7): 1–10. doi: 10.1007/s41870-018-0091-6.

[7] CHEN Rongmao, MU Yi, YANG Guomin, *et al*. Dual-server public-key encryption with keyword search for secure cloud storage[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(4): 789–798. doi: 10.1109/TIFS.2015.2510822.

[8] MIAO Yinbin, MA Jianfeng, LIU Ximeng, *et al*. VKSE-MO: Verifiable keyword search over encrypted data in multi-owner settings[J]. *Science China Information Sciences*, 2017, 60(12): 122105. doi: 10.1007/s11432-016-0540-x.

[9] CUI Baojiang, LIU Zheli, and WANG Lingyu. Key-Aggregate Searchable Encryption (KASE) for group data sharing via cloud storage[J]. *IEEE Transactions on Computers*, 2016, 65(8): 2374–2385. doi: 10.1109/TC.2015.2389959.

[10] ZHOU Rang, ZHANG Xiaosong, DU Xiaojiang, *et al*. File-centric multi-key aggregate keyword searchable encryption for industrial internet of things[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(8): 3648–3658. doi: 10.1109/TII.2018.2794442.

[11] 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. doi: 10.1016/j.jss.2009.11.726.

[12] 赵洋, 包文意, 熊虎, 等. 云计算里一种陷门无法识别的公钥搜索加密方案[J]. 信息网络安全, 2016(1): 1–5. doi: 10.3969/j.issn.1671-1122.2016.01.001.
ZHAO Yang, BAO Wenyi, XIONG Hu, *et al*. A scheme of public encryption keyword search with indistinguishable trapdoor[J]. *Netinfo Security*, 2016(1): 1–5. doi: 10.3969/j.issn.1671-1122.2016.01.001.

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

[14] IBRAIMI L, NIKOVA S, HARTEL P, *et al*. Public-key encryption with delegated search[C]. The 9th International Conference on Applied Cryptography and Network Security, Nerja, Spain, 2011: 532–549. doi: 10.1007/978-3-642-21554-4_31.

[15] TANG Qiang, MA Hua, and CHEN Xiaofeng. Extend the concept of public key encryption with delegated search[J]. *The Computer Journal*, 2015, 58(4): 724–734. doi: 10.1093/comjnl/bxt102.

[16] WANG Wei, XU Peng, LI Hui, *et al*. Secure hybrid-indexed search for high efficiency over keyword searchable ciphertexts[J]. *Future Generation Computer Systems*, 2016, 55: 353–361. doi: 10.1016/j.future.2014.07.008.

曹素珍：女，1976年生，副教授，研究方向为公钥密码学和软件安全.

郎晓丽：女，1993年生，硕士生，研究方向为密码学与信息安全.

刘祥震：男，1991年生，硕士生，研究方向为密码学与信息安全.

张玉磊：男，1979年生，硕士生，博士，副教授，研究方向为密码学与信息安全.

王 斐：女，1992年生，硕士生，研究方向为密码学与信息安全.