浙江科技学院学报，第 32 卷第 6 期，2020 年 12 月
Journal of Zhejiang University of Science and Technology
Vol. 32 No. 6, Dec. 2020

doi：10.3969/j.issn.1671-8798.2020.06.003

一种基于多服务器的安全可搜索加密方法

吴　凯[1a]，王海江[1b]，魏贵义[2]，陈　力[1a]

（1.浙江科技学院 a.机械与能源工程学院；b.信息与电子工程学院，杭州 310023；
2.浙江工商大学 计算机与信息工程学院，杭州 310018）

摘　要：为了解决在群协作中传统可搜索加密机制存在服务器叛逆的问题，提出了一种基于多服务器的安全可搜索加密方法。本方法利用多服务器的协同遍历计算，通过群组密钥协商和双线性配对的算法来提高可搜索加密的安全性。首先采用群组密钥协商协议构造出密钥，对群共享文件和关键字加密；然后通过私钥与关键字间的哈希运算产生搜索令牌；最后通过多服务器的双线性配对算法完成对加密关键字的检索，实现可搜索加密。安全性分析表明，本方法能够实现安全的可搜索加密和叛逆者追踪，同时可保证关键字与搜索令牌的安全，防止隐私数据泄露。困难性假设证明显示，基于多服务器的安全可搜索加密方法能够提高可搜索加密的安全性，具备抵御服务器叛逆风险的能力。

关键词：群协作；群组密钥协商；双线性配对；可搜索加密；叛逆者可追踪

中图分类号：TN918.1　　**文献标志码**：A　　**文章编号**：1671-8798(2020)06-0523-08

A secure searchable encryption method based on multi-server

WU Kai[1a], WANG Haijiang[1b], WEI Guiyi[2], CHEN Li[1a]

(1 a. School of Mechanical and Energy Engineering; b. School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310023, Zhejiang, China; 2. School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, Zhejiang, China)

Abstract: In group collaboration, a secure searchable encryption method based on multiple servers was proposed to solve the risk of server rebellion in the traditional searchable encryption mechanism. This method applied multi-server collaborative traversal calculations to improve the security of searchable encryption through group key agreement and bilinear pairing algorithms. Firstly, the group shared files and the keywords were encrypted to construct the key by using the group key agreement protocol. Then, the hash calculation of the private key and the keywords was used to generate a search token. Finally, the multi-server bilinear pairing algorithm was employed to complete retrieval of the encrypted keywords and achieve secure searchable encryption. Security analysis shows that this method can achieve secure searchable encryption and trace traitors, ensure the security and privacy of keywords and search tokens, and prevent privacy data from disclosing. The results show that the secure searchable encryption method based on multi-server can improve the security of searchable encryption and has the

收稿日期：2020-06-08

基金项目：浙江省自然科学基金项目(LQ20F020010)

通信作者：王海江(1987—　)，男，河南省新乡人，讲师，博士，主要从事信息安全和密码学研究。E-mail：wanghaijiangyes@163.com。

ability to resist the risk of server rebellion.

Keywords: group collaboration; group key agreement; bilinear pairing; searchable encryption; traitor traceability

随着网络中群体协作工作活动的增多,如多人协作、云存储共享、远程会议等,用户对云存储数据的安全性和可靠性有了更高的要求。由于公有云中的加密文件具有机密性和完整性,服务器无法直接为用户检索到指定文件,因此数据的可用性大大降低。为解决这一难题,通常采用可搜索加密(searchable encryption,SE)[1]方法,即数据拥有者将文件及关键字进行加密后上传至云服务器中,当数据使用者需要获取包含某一关键字的文件时,可通过数据拥有者提供的搜索密钥生成令牌递交给服务器进行搜索。该方法由于搜索密钥长度会随文件数量而线性增长,因此无法控制其存储成本。密钥聚合可搜索加密机制(key-aggregate searchable encryption,KASE)[2]的提出,较好地解决了搜索密钥过多的问题,但由于搜索密钥需要由数据提供者授权,因此无法适用于多用户群协作场景中。基于多用户的可搜索加密[3-5]方法和群组密钥协商[6]机制能够为多用户的分享提供支持,数据使用者仅需一个搜索密钥即可搜索多个分享者所提供的加密数据,但这两种方法的缺点是搜索令牌与关键字不具备隐秘性和可靠的安全性[7],且保密性差,易泄露,容易被他人获取和攻击。Wang 等[8]提出的一种安全的 KASE 方法能够抵御密钥提取攻击,虽然提高了密钥的安全性,但没有解决群用户间的协作共享和叛逆者可追踪的问题。而在密钥生成过程中,采用非对称群组密钥协商(asymmetric group key agreement,ASGKA)机制[8]并加入群组用户的身份信息[10-11],可实现对群组中泄露密钥的用户进行追踪,但无法实现抵御服务器的叛逆。因此,本研究针对现有的可搜索加密技术中存在的问题,采用非对称群组密钥协商协议[8]和双线性配对方法[12],构造了一种基于多服务器场景下的加密关键字搜索(multi-server searchable encryption,MSSE)技术。通过关键字与私钥融合,构造搜索令牌,保证了关键字与令牌的隐秘性,实现群用户的身份对等和服务器的可搜索加密;同时利用多服务器的构造方式,不仅能够对叛逆者进行追踪,还降低了服务器叛逆的风险;最终通过双线性迪菲-赫尔曼指数(bilinear diffie-hellman exponentiation,BDHE)假设证明了其安全性。

1 预备知识

1.1 双线性映射

双线性映射定义[12]为:假定 G_1、G_2 是两个阶为素数 l 的乘法循环群,$u\in G_1$,$v\in G_2$,且 u、v 分别是 G_1 和 G_2 的生成元。若有双线性配对映射 $e:G_1\times G_2\rightarrow G_3$,则 e 需要满足以下条件:

1)双线性,对于 $\forall u$、$v\in G$,a、$b\in Z_p$(Z_p 表示所有素数),都有 $e(u^a,v^b)=e(u,v)^{ab}=e(u^b,v^a)$ 成立;

2)非退化性,即 $e(u,v)\neq 1$ 成立;

3)可计算性,存在某一算法,在有效时间内计算出 $G_1\times G_2$。

通常情况下,如果 $G_1=G_2=G$,则认为配对线性映射 $e(\cdot,\cdot)$ 是对称的,即 $e(u,v)=e(v,u)$。这是因为对一个生成元 $g\in G$ 而言,存在整数 p、$q\in Z_p$,满足 $u=g^p$,$v=g^q$。因此 $e(u,v)=e(g^p,g^q)=e(g,g)^{pq}=e(g^q,g^p)=e(v,u)$。

1.2 复杂性假设

本研究提出的多服务器下的关键字可搜索方法的安全性验证,是基于判定性 l 阶 BDHE 来证明的,其描述如下:

假设存在一个算法 $\mathcal{B}$,G 是阶为素数 l 的双线性群,$e:G\times G\rightarrow G_3$,$g$ 和 h 是 G 的两个独立生成元,记 $\boldsymbol{y}_{g,\alpha,l}=(g_1,g_2,\cdots,g_l,g_{l+2},\cdots,g_{2l})\in G^{2l-1}$,其中 $g_i=g^{\alpha^i}$,α 为未知数。

$$|P_r[\mathcal{B}(g,h,\boldsymbol{y}_{g,\alpha,l},e(g_{l+1},h))=0]-P_r[\mathcal{B}(g,h,\boldsymbol{y}_{g,\alpha,l},Z)=0]|\geqslant\varepsilon。\tag{1}$$

式(1)中:P_r 为概率函数;Z 为 G_3 中任意一个元素;ε 为一定值。

若式(1)成立,则算法 $\mathcal{B}$ 有 ε 的优势来解决判定性 l-BDHE 假设,算法 $\mathcal{B}$ 的输出值为 $b\in\{0,1\}$。若

不存在一个算法，在多项式时间内以至少 ε 的优势解决 l-BDHE 假设，则认为 l-BDHE 假设成立。

1.3　基于聚合签名的广播机制

基于聚合签名的广播方法(aggregatable signature-based broadcast，ASBB)[8]，既是一种广播方法也是一种认证签名的方法。ASBB 利用了解密密钥与签名的二重性和基于认证方式的加密方法，其过程包含了 6 个多项式时间算法，即系统参数生成、密钥生成、签名、认证、加密和解密算法，算法描述如下：

1)初始化 $\pi \leftarrow \lambda$，输入安全参数 λ，输出公共参数 π；

2)密钥生成 $(k_{\text{pub}}, k_{\text{sig}}) \leftarrow \pi$，输入公共参数 π，输出公钥和私钥对 $(k_{\text{pub}}, k_{\text{sig}})$；

3)签名 $\sigma \leftarrow (k_{\text{pub}}, k_{\text{sig}}, s)$，输入密钥对 $(k_{\text{pub}}, k_{\text{sig}})$ 和字串 s，输出签名消息 $\sigma(s)$；

4)验证签名 $(0,1) \leftarrow (k_{\text{pub}}, \sigma)$，输入公钥 k_{pub} 和签名消息 $\sigma(s)$，输出 0 或 1，签名认证成功时，输出 1，并保留签名信息 $\sigma(s)$，否则退出；

5)加密 $C_m \leftarrow (k_{\text{pub}}, m)$，输入公钥 k_{pub} 和需要加密明文 m，输出加密后的密文 C_m；

6)解密 $m \leftarrow (k_{\text{pub}}, \sigma, C_m)$，输入公钥 k_{pub}，有效的签名串 $\sigma(s)$ 和密文 C_m，解密输出明文 m。

2　模型定义

2.1　方案模型

本研究提出的基于多服务的可搜索加密方法 MSSE 由 8 个多项式时间算法构成。

1)初始化系统参数：输入安全参数 λ，输出公共参数 K_{parm}；

2)群组密钥协商：利用群协商算法，生成用户身份索引 I_{id} 作为输入，输出广播消息 $(R_i, A_i, \{\sigma_{i,j}\})$；

3)群组公钥生成：将用户广播消息作为输入，输出群组公共密钥 (R, A)；

4)用户私钥生成：群组中每个用户 i 输入公钥 (R, A)，输出用户私钥 k_{sig}，并验证其私钥的正确性；

5)关键字加密：输入公钥 (R, A) 及关键字 w，输出 $I_w = <C_1, C_2, C_3>$；

6)访问令牌生成：输入用户 k_{sig} 和所查找关键字 w，输出搜索令牌 T_r；

7)服务器匹配令牌：主服务器和辅助服务器分别计算用户提交的令牌消息 T_r 和参数信息，并遍历服务器所有文件的关键字；

8)返回结果：主服务器计算验证 T_r 与系统中存储的加密关键字是否匹配，并返回给用户 $\{0,1\}$，0 表示未找到包含该令牌关键字的文件，1 表示找到包含该令牌关键字的文件。

2.2　安全模型

本研究为 MSSE 方法定义了一个安全模型，在这个模型中首先要保证加密关键字 I_w 的设计是安全的，即当 I_w 上传到服务器后，任何用户无论何种情况下均无法获知关键字 w 的明文信息。设定攻击者 B 能够以 B_{adv} 的优势获得关键字 w 的搜索令牌 T_w，且攻击者 B 在没有获取到令牌前无法区分出 I_{w0} 和 I_{w1}。下面将通过挑战者 C 和攻击者 B 之间的游戏规则，来定义 MSSE 方法的安全性。挑战者 C 表示利用 MSSE 方法所建立的系统，攻击者 B 表示对该系统进行的攻击行为。

1)初始化：挑战者 C 通过 P_{airgen} 函数算法生成公共参数 K_{parm}；

2)训练：当 B 询问用户 U_i 信息时，C 使用群组密钥协商协议算法，输出公共参数和群组公钥，并交给 B。攻击者 B 可向挑战者 C 索要任意用户 U_i 的搜索令牌 I_w；

3)挑战：攻击者 B 向挑战者 C 发送两个准备挑战的关键字 w_0 和 w_1。设定攻击者 B 在挑战前未向 C 索要过关于 w_0 和 w_1 的令牌 T_{w1} 和 T_{w2}。挑战者 C 随机选择一个关键字 w_b，加密得到 $I^*_{w_b}$ 后交给 B，其中 $b \in \{0,1\}$；

4)再训练：攻击者 B 仍然可以继续向 C 索要组中任意用户任意关键字的令牌 T_w，但此时的关键字 $w \neq \{w_0, w_1\}$；

5)输出：攻击者 B 输出 $b' \in \{0,1\}$，作为对 C 输出结果的猜想。如果 $b = b'$，则攻击者 B 将以 $B_{\text{adv}} = \left| P_r[b=b'] - \frac{1}{2} \right|$ 的优势赢得了这场游戏。

3 具体方案

3.1 基本思想

在群协作活动中，用户需要将自己的数据共享给同组的其他用户，同时要求数据内容不会直接暴露给无关的第三者，因此通常采用可搜索加密(SE)方法。如图1所示，用户将共享文件及关键字进行可搜索加密后上传至服务器中，其他用户通过关键字令牌向云服务器请求相应文件。一般情况下，用户通过令牌算法将个人私钥与关键字进行运算生成令牌后递交云服务器，由服务器对令牌和存储的加密关键字进行匹配。如果令牌生成算法采用静态方法来实现，那么将面临着用户在搜索相同关键字时，每次所生成的搜索令牌也均相同，这对恶意攻击者而言，一旦获取解密密钥，即可破解任意加密文件。

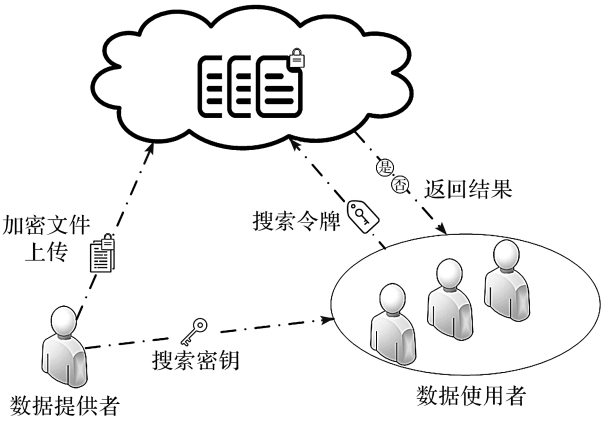

图1 可搜索加密示意图

Fig. 1 Schematic diagram of searchable encryption

因此，令牌构造必须采用随机动态生成算法。本研究提出的MSSE方法，其基本思想如下。

首先，考虑到所构造的密钥必须方便群用户间加解密数据，因此采用ASGKA协议构建出群组协商密钥即共享密钥(R,A)，便于用户使用共享密钥对原始文件进行加密，同时群组中每个用户U_i都可计算出此共享密钥对应的解密密钥k_{sig_i}，用于解密出云服务器中的加密文件。

其次，由于云服务器存储的内容为加密文件，所以服务器在没有解密密钥的情况下无法为用户检索出其所需文件，即包含用户关键字的文件，因此云服务器的可用性大为降低。为解决这一问题，本研究采用可搜索加密方式提取文件中关键字作为索引，进行加密设计。用户使用个人私钥k_{sig_i}，与一个随机数s和关键字w进行运算，得到一个搜索令牌T_{r}，递交给服务器进行检索，服务器将接收到的令牌T_{r}和所存储文件中的加密关键字I_w进行遍历匹配运算，并告知用户检索结果。由于关键字长度可能不一，明文不能暴露，因此在构造T_{r}前，需要对关键字w进行哈希运算$H(w)$，以保证关键字的隐私。该方式使得服务器可以在未知用户检索内容和所存储信息内容的情况下，实现可搜索加密内容，极大地提高了数据的可操作性。

通常情况下，如果群组中有用户泄露个人私钥，恶意攻击者将通过该私钥解密出加密文件，导致信息泄露。由于本研究采用非对称群组密钥协商，在设计群组公钥和私钥时，群组中每个用户都有唯一身份索引ID，一旦由用户泄露自己的私钥，群组中其他用户可通过该私钥反推出用户ID，锁定泄密者身份。同时，考虑到服务器可能产生叛逆，获取到用户私钥，云服务器中加密文件会暴露无遗，因此在多服务器上采用可搜索加密方法在很大程度上解决了服务器的叛逆性问题。

最后，基于此我们提出了多服务器下的安全可搜索加密方法。该方法实现了群组中叛逆者可追踪，同时可抵御单服务器的叛逆性问题，具有更高的安全性和可靠性。本研究所提出的MSSE方法是基于双服务器的安全搜索协作，即主服务器和辅助服务器共同完成加密搜索任务。其中主服务器用于存放用户存储的加密文件及文件关键字信息，具备计算匹配用户搜索令牌的功能；辅助服务器用于存放文件关键字索引，协助主服务器计算关键字的匹配参数。

3.2 方案描述

MSSE协议采用了双线性群的思想，首先构造群配对生成函数P_{airgen}，输入安全参数1^{λ}，输出元组$\gamma=(p,g_0,G_0,G_1,e_0,H)$，其中$G_0$、$G_1$同是阶为素数$p$的循环群，$g_0$是$G_0$的生成元，映射$e_0:G_0\times G_0\to G_1$，$H$表示对明文的哈希运算。MSSE实现的具体流程如下。

1)生成系统参数$K_{\mathrm{parm}}\leftarrow(1^{\lambda})$：向群配对生成函数$P_{\mathrm{airgen}}$输入安全一个参数$1^{\lambda}$，即$P_{\mathrm{pair}}(1^{\lambda})$，生成一个双线性元组$\gamma=(p,G_0,G_1,e_0)$。随机选择$x'\in G_0$，并且$\boldsymbol{X}=(x_1,x_2,\cdots,x_k)$，$x_i\in G_0$，$k$为一固定值。系统

公开参数设置为：$K_{\text{parm}}=(\gamma,g_0,x',\boldsymbol{X})$。

2）群组密钥协商$(R_i,A_i,\{\sigma_{i,j}\})\leftarrow(\boldsymbol{I}_{\text{id}_1},\boldsymbol{I}_{\text{id}_2},\cdots,\boldsymbol{I}_{\text{id}_n})$：记群组中 n 个参与者，分别为 $U_1,U_2,\cdots,U_n$，令 $\boldsymbol{I}_{\text{id}_1},\boldsymbol{I}_{\text{id}_2},\cdots,\boldsymbol{I}_{\text{id}_n}$ 表示每个用户的身份信息，其中 $\boldsymbol{I}_{\text{id}_i}=(s_1^i,s_2^i,\cdots,s_k^i)$，$i=1,\cdots,n$。群组中每个用户 U_i 分别独立选择随机数 a_i、$r_i\in Z_p$，计算并广播 $R_i=g_0^{-r_i}$，$A_i=e_0(g_0,g_0)^{a_i}$；计算用户特征标识，即 $f(\boldsymbol{I}_{\text{id}_j})=x'\prod_{l=1}^{k}x_l^{s_l^j}$，$j=1,2,\cdots,n$；计算每个用户身份 $\boldsymbol{I}_{\text{id}_j}$ 信息的签名，即 $\sigma_{i,j}=g_0^{a_i}\cdot f^{r_i}(\boldsymbol{I}_{\text{id}_j})$，$j=1,2,\cdots,n$；每个用户广播信息$(R_i,A_i,\{\sigma_{i,j}\}_{j=1,2,\cdots,n,j\neq i})$如以下矩阵所示：

$$\begin{bmatrix} & & U_1 & U_2 & \cdots & U_n & \text{公钥} \\ U_1 & \prec & \varnothing & \sigma_{1,2} & \cdots & \sigma_{1,n} & (R_1,A_1) \\ U_2 & \prec & \sigma_{2,1} & \varnothing & \cdots & \sigma_{2,n} & (R_2,A_2) \\ \vdots & \prec & \vdots & \vdots & \ddots & \vdots & \vdots \\ U_n & \prec & \sigma_{n,1} & \sigma_{n,2} & \cdots & \varnothing & (R_n,A_n) \\ & & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\ \text{系统生成参数} & & \sigma'_1 & \sigma'_2 & \cdots & \sigma'_n & (R,A) \end{bmatrix}。$$

3）群组公钥生成$(R,A)\leftarrow(R_i,A_i)$：为生成群用户的公钥，每个用户 U_i 应该先确认其 n 个信息-签名对是否有效，即验证下列等式是否成立，

$$e_0(\sigma_{j,i},g_0)\cdot e_0(R_j,f(\boldsymbol{I}_{\text{id}_i}))=A_j。$$

如果所有的信息-签名对均是有效的，则计算公钥(R,A)，

$$R=\prod_{j=1}^{n}R_j=g_0^{\sum_{i=1}^{n}(-r_j)},A=\prod_{j=1}^{n}A_j=e_0(g_0,g_0)^{\sum_{j=1}^{n}a_j}。$$

4）用户私钥生成 $k_{\text{sig}_i}\leftarrow(R,A,f(\boldsymbol{I}_{\text{id}_i}))$：通过既定的广播信息 $\sigma_{j,i}$，每个用户 U_i 计算个人私钥 k_{sig_i}，

$$k_{\text{sig}_i}=\prod_{j=1}^{n}\sigma_{j,i}=\prod_{j=1}^{n}g_0^{a_j}\cdot f^{r_j}(\boldsymbol{I}_{\text{id}_i})=g_0^{a}\cdot f^{r}(\boldsymbol{I}_{\text{id}_i})。$$

同时验证该私钥是否满足

$$e_0(k_{\text{sig}_i},g_0)\cdot e_0(R,f(\boldsymbol{I}_{\text{id}_i}))=A。\tag{2}$$

若式(2)成立，则接受该私钥 k_{sig_i} 作为搜索密钥和解密密钥；

5）关键字加密 $I_w\leftarrow(k_{\text{sig}_i},w,t,H)$：数据提供者随机选择 $t\in Z_{\text{p}}$，对关键字 w 进行哈希运算 $H(w)$，并加密为 I_w，

$$I_w=<C_1=g_0^t,C_2=R^{tH(w)},C_3=A^{tH(w)}>。$$

6）访问令牌生成 $T_{\text{r}}\leftarrow(w,k_{\text{sig}_i},s)$：数据使用者 U_i 随机选择 $s\in Z_{\text{p}}$，使用自己的私钥 k_{sig_i} 生成关键字 w 的搜索令牌 $T_{\text{r}}=(k_{\text{sig}_i})^{H(w)s}$，并将随机数分为 $s=s_{\text{main}}+s_{\text{aid}}$，得到 $T_{\text{r,main}}=(T_{\text{r}},s_{\text{main}},f(\boldsymbol{I}_{\text{id}_i}))$，$T_{\text{r,aid}}=s_{\text{aid}}$，将两个参数分别递交给主服务器和辅助服务器。

7）服务器匹配令牌$(C_2^s,C_3^s)\leftarrow(s_{\text{main}},s_{\text{aid}})$：辅助服务器接收到 $T_{\text{r,aid}}$ 后，遍历计算文件关键字 $C_2^{s_{\text{aid}}}$ 和 $C_3^{s_{\text{aid}}}$，并将结果传递给主服务器。主服务器计算：

$$C_2^{s_{\text{main}}}C_2^{s_{\text{aid}}}=C_2^s;$$

$$C_3^{s_{\text{main}}}C_3^{s_{\text{aid}}}=C_3^s。$$

8）返回结果$(0,1)\leftarrow(I_w,T_{\text{r}})$：主服务器判别下列等式是否成立，

$$e_0(T_{\text{r}},C_1)\cdot e_0(f(\boldsymbol{I}_{\text{id}_i}),C_2^s)=C_3^s。\tag{3}$$

若式(3)成立，则表示搜索到加密关键字，并返回结果 1；否则，表示未查询到该加密关键字，返回结果 0。

3.3　正确性证明

根据 MSSE 的方案描述，服务器在最终判别令牌 T_{r} 与存储的加密关键字 I_w 是否匹配需通过验证式(4)是否成立。

$$e_0(T_r,C_1)\cdot e_0(f(\boldsymbol{I}_{id_i}),C_2^s)=C_3^s。\tag{4}$$

证明：

$$e_0(T_r,C_1)\cdot e_0(f(\boldsymbol{I}_{id_i}),C_2^s)=e_0((k_{sig_i})^{H(w)s},g_0^t)\cdot e_0(f(\boldsymbol{I}_{id_i}),R^{tH(w)})^s=$$

$$e_0(g_0^a\cdot f^r(\boldsymbol{I}_{id_i}),g_0)^{tH(w)s}\cdot e_0(f(\boldsymbol{I}_{id_i}),g_0^{-rtH(w)})^s=$$

$$e_0(g_0^a,g_0)^{tH(w)s}\cdot e_0(f^r(\boldsymbol{I}_{id_i}),g_0)^{tH(w)s}\cdot e_0(f(\boldsymbol{I}_{id_i}),g_0)^{-rtH(w)s}=e_0(g_0,g_0)^{atH(w)s}=A^{tH(w)s}=C_3^s。$$

结果显示服务器能够依据用户提供的检索令牌，匹配出服务器中对应的加密关键字，即验证了 MSSE 算法能够实现可搜索加密方法。

3.4 叛逆者追踪

本研究可实现叛逆者追踪，如果群组中有参与者将个人私钥 k_{sig} 透露给攻击者，那么群中任何其他用户 U_j 均可通过计算式(5)来找出泄密者，

$$e_0(k_{sig},g_0)\cdot e_0(R_i,f(\boldsymbol{I}_{id_j}))=A_i。\tag{5}$$

因此，通过遍历群组 $\boldsymbol{I}_{id}$，如果存在 $\boldsymbol{I}_{id_i}$ 使式(5)成立，则群组中泄密者即为该用户。

3.5 安全性证明

定理 假设 n-BDHE 问题是难以解决的，则上述多服务器的可搜索加密方法是安全的。

假设 攻击者 B 在 τ 时间内以 ε 的优势攻破多服务器加密关键字搜索机制，那么就存在一个挑战者 C 可以在 $\tau'=\tau+O(n^2\tau_{exp})$ 时间内，以 ε 相同大小的优势解决判定性 n-BDHE 问题。

证明：创建一个参数为 $(g,h,g_1,\cdots,g_n,g_{n+2},g_{2n},Z)$ 的 MSSE 系统，作为挑战者 C 对 n-BDHE 问题的挑战。C 的目标是通过扮演攻击者 B 来攻击 n-BDHE 假设，这场安全策略游戏过程如下：

1)挑战者 C 随机选择一个向量 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_k)$，$y_i\in Z_p$，令 $g_0=g$，$x'=g_n$，$\boldsymbol{X}=(x_1,x_2,\cdots,x_k)$，$x_i=(g^{y_i})$，其中 $i\in\{1,2,\cdots,k\}$。输入系统安全参数 λ，调用 $P_{airgen}(1^\lambda)$ 函数，生成公开参数 $K_{parm}=(p,G,G_T,e_0,x',\boldsymbol{X})$，并将参数交给攻击者 B；

2)挑战者 C 计算群组公钥，令

$$v_j=\sum_{l=1}^{k}y_l s_l^j,$$

计算

$$f(\boldsymbol{I}_{id_j})=x'\cdot\prod_{l=1}^{k}x_l^{s_l^j}=g_n\cdot\prod_{l=1}^{k}g^{y_l s_l^j}=g_n\cdot g_{l=1}^{\sum_{l=1}^{k}y_l s_l^j}=g_n g^{v_j}。$$

挑战者 C 随机选择 $i^*\in\{1,2,\cdots,n\}$，$a_i,r_i\in Z_p^*$，令 $\boldsymbol{S}_i^*=(1,\cdots,i^*-1,i^*+1,\cdots,n)$。计算

$$R_{i^*}=g^{-r_{i^*}}\cdot\left(\prod_{k\in S_{i^*}}g_{n+1-k}\right);$$

$$\sigma_{i^*,j}=g^{a_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\right)\cdot R_{i^*}^{-v_j}。$$

于是有

$$e_0(\sigma_{i^*,j},g)\cdot e_0(R_{i^*},f(\boldsymbol{I}_{id_j}))=$$

$$e_0(g^{a_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\right)\cdot R_{i^*}^{-v_j},g)\cdot e_0(R_{i^*},g_n\cdot g^{v_j})=$$

$$e_0(g^{a_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\right),g)\cdot e_0(R_{i^*},g_n)=$$

$$e_0(g^{a_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\right),g)\cdot e_0(g^{-r_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}g_{n+1-k}^{-1}\right),g_n)=$$

$$e_0(g^{a_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}^{k\neq n}g_{n+1-k+n}^{-1}\right),g)\cdot e_0(g^{-r_{i^*}}\cdot g^{r_{i^*}}\left(\prod_{k\in S_{i^*}}g_{n+1-k+n}^{-1}\right),g)=$$

$$e_0(g^{a_{i^*}},g)\cdot e_0(g_{n+1},g)=e_0(g,g)^{a_{i^*}}\cdot e_0(g,g)^{\alpha^{n+1}}\triangleq A_{i^*}。$$

对 $i\neq i^*$，计算

$$R_i = g^{-r_i} g_{n+1-i}^{-1};$$

$$\sigma_{i,j} = g^{a_i} g_n^{r_i} g_{n+1-k+n} R_i^{-v_j} (j \neq i)。$$

于是,就可以得到

$$e_0(\sigma_{i,j}, g) \cdot e_0(R_i, f(\boldsymbol{I}_{\mathrm{id}_j})) = e_0(g^{a_i} \cdot g_n^{r_i} \cdot g_{n+1-i+n} \cdot R_i^{-v_j}, g) \cdot e_0(R_i, g_n \cdot g^{v_j}) =$$

$$e_0(g^{a_i} \cdot g_n^{r_i} \cdot g_{n+1-i+n}, g) \cdot e_0(R_i, g_n) = e_0(g^{a_i} \cdot g_n^{r_i} \cdot g_{n+1-i+n}, g) \cdot e_0(g^{-r_i} \cdot g_{n+1-i}^{-1}, g_n) =$$

$$e_0(g^{a_i} \cdot g_n^{r_i} \cdot g_{n+1-i+n}, g) \cdot e_0(g_n^{-r_i} \cdot g_{n+1-i+n}^{-1}, g) = e_0(g, g)^{a_i} \overset{\Delta}{=} A_i。$$

因此,对于所有 $j \neq i (i \in \{1, 2, \cdots, n\})$,以下等式成立:

$$e_0(\sigma_{j,i}, g) \cdot e_0(R_j, f(\boldsymbol{I}_{\mathrm{id}_j})) = A_j。$$

3)挑战者 C 计算出群组公钥(R, A),并交给攻击者 B,令

$$a = \sum_{k=1}^{n} a_k, r = \sum_{k=1}^{n} r_k。$$

那么

$$R = \prod_{k=1}^{n} R_k = R_{i^*} \cdot \prod_{k \in S_i^*} R_i = g^{-r_{i^*}} \cdot \prod_{k \in S_i^*} g^{-r_i} = g^{-\sum_{k=1}^{n} r_k} = g^{-r};$$

$$A = \prod_{k=1}^{n} A_k = A_{i^*} \cdot \prod_{k \in S_i^*} A_i = e_0(g, g)^{(a^{n+1} + \sum_{k=1}^{n} a_k)} = e_0(g, g)^{(a^{n+1} + a)}。$$

4)攻击者 B 可以尝试性地向挑战者 C 索要任何用户 U_i 所生成关键字 w 的令牌,即挑战者 C 可计算出

$$T_{\mathrm{r}} = (k_{\mathrm{sig}_i})^{H(w)s}。$$

5)攻击者 B 生成一对准备挑战的密文$\{w_1, w_2\}$,挑战者 C 随机生成 $b \in \{0, 1\}$,并计算出 w_b 加密后的信息 $I_{w_b}^*$,

$$I_{w_b}^* = <C_1^* = h, C_2^* = h^{rH(w_b)}, C_3^* = (Z \cdot e_0(g, h)^a)^{H(w_b)}>。$$

6)攻击者 B 输出对具体值 b 的猜测 b',如果挑战者 C 判别出 $b' = b$,则 $Z = e_0(g_{n+1}, h)$。令 $h = g^t$,如果 $Z = e_0(g_{n+1}, h)$成立,则有

$$C_1^* = h = g^t;$$

$$C_2^* = h^{rH(w_b)} = (g^t)^{rH(w_b)} = (g^r)^{tH(w_b)} = R^{tH(w_b)};$$

$$C_3^* = (Z \cdot e(g, h)^a)^{H(w_b)} = (e_0(g_{n+1}, h) \cdot e_0(g, h)^a)^{H(w_b)} =$$

$$(e_0(g^{a^{n+1}}, g^t) \cdot e_0(g, g^t)^a)^{H(w_b)} = (A^t)^{H(w_b)} = A^{tH(w_b)}。$$

由于 a_i, r_i 在 Z_p^* 上是均匀分布的,故攻击者无法区别出上述模拟过程与真实过程的差异,即两者是相同的,所以挑战者 C 能够以和攻击者 B 相同的优势来解决 n-BDHE 假设。故本方法是安全的。

3.6　性能分析

从时间复杂性方面来分析本研究提出的 MSSE 方法,其主要计算成本在广播消息$(R_i, A_i, \{\sigma_{i,j}\}_{j=\{1,2,\cdots,n\}, j \neq i})$的生成和运算。计算 $\sigma_{i,j}$需要 $O(n^2)$个双线性群 G 中的指数计算,而计算 R_i、A_i 分别需要 $O(n)$个 G 中的指数计算。假设 G 中的一个指数计算的时间复杂性为 $\tau_{\exp}$,那么 MSSE 方法的时间复杂性为 $\tau' = \tau + O(n^2 \tau_{\exp})$,式中 τ 为系统原有的时间复杂性。同时,对现有的可搜索加密方法与本方法进行性能比较,结果见表 1。

表 1　MSSE 方法与现有可搜索加密方法的功能对比

Table 1　Functional comparison between MSSE and existing searchable encryption approaches

方法	可搜索加密关键字	多用户分享	叛逆可追踪	可抵御服务叛逆
文献[2]	√	×	×	×
文献[3]	√	√	×	×
文献[10]	√	×	×	×
文献[5]	√	√	√	×
本方法	√	√	√	√

注:√表示可实现该功能;×表示无法实现该功能。

4 结 语

本研究基于ASGKA协议提出了一个多服务器的安全可搜索加密方法MSSE,并验证了其正确性和安全性。选用双服务器的加密令牌匹配设计,提高了信息存储的安全性和加密搜索的安全性,解决了在单一的云存储服务器中由于服务器的叛变问题所导致云加密信息被攻击者破解的难题。关键字 w 的哈希运算加密和令牌的随机数构造,使得关键字和令牌也具备了安全性,无法被攻击者解密。因此,MSSE在服务器的叛变问题上具有较高的安全性,攻击者无法直接读取到用户请求的数据内容及明文信息;同时,还可以对群组中密钥泄露者追踪,锁定其身份。

参考文献:

[1] 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.

[2] CUI B J, LIU Z L, WANG L Y. Key-aggregate searchable encryption(KASE) for group data sharing via cloud storage[J]. IEEE Transactions on Computers,2016,65(8):2375.

[3] LI T, LIU Z L, JIA C F, et al. Key-aggregate searchable encryption under multi-owner setting for group data sharing in the cloud[J]. International Journal of Web and Grid Services,2018,14(1):22.

[4] PADHYA M, JINWALA D C. MULKASE: a novel approach for key-aggregate searchable encryption for multi-owner data[J]. Frontiers of Information Technology & Electronic Engineering,2019,20(12):1718.

[5] KIAYIAS A, OKSUZ O, RUSSELL A, et al. Efficient encrypted keyword search for multi-user data sharing[C]// European Symposium on Research in Computer Security. Cham: Springer,2016:173.

[6] INGEMARSSON I, TANG D, WONG C. A conference key distribution system[J]. IEEE Transactions on Information Theory,1982,28(5):714.

[7] KAMIMURA M, YANAI N, OKAMURA S, et al. Key-aggregate searchable encryption, revisited: formal foundations for cloud applications, and their implementation[J]. IEEE Access,2020,8(1):24153.

[8] WANG H J, DONG X L, Cao Z F, et al. Secure key-aggregation authorized searchable encryption[J]. Science China Information Sciences,2019,62(3):39111.

[9] WU Q H, MU Y, SU W, et al. Asymmetric group key agreement[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer,2009.

[10] 赵秀凤,徐秋亮,刘伟.叛逆者可追踪的非对称群组密钥协商协议[J].计算机科学,2011,38(9):42.

[11] 张启坤,王锐芳,谭毓安.基于身份的可认证非对称群组密钥协商协议[J].计算机研究与发展,2014,51(8):1727.

[12] 张特.基于双线性配对计算的认证算法实现[D].长春:吉林大学,2018.

[13] HAMLIN A, SHELAT A, WEISS M, et al. Multi-key searchable encryption, revisited[C]//Proceedings of IACR International Workshop Public Key Cryptography. Switzerland: Springer,2018:96.

[14] 卢震宇.常数轮群组密钥协商协议及其应用研究[D].成都:电子科技大学,2018.

[15] DENG Z J, LI K L, LI K Q, et al. A multi-user searchable encryption scheme with keyword authorization in a cloud storage[J]. Future Generation Computer Systems,2017,72:209.

[16] ZHANG L, WU Q H, QIN B, et al. Certificateless and identity-based authenticated asymmetric group key agreement[J]. International Journal of Information Security,2017,16(5):560.