抗关键词猜测攻击的可搜索属性基加密方案

王 敏 周李京 秦璐璐
(河海大学计算机与信息学院 江苏 南京 211100)

摘 要 可搜索属性基加密能够让属性满足访问控制策略(或用来加密关键词的属性满足用户私钥指定的访问控制策略)的用户搜索加密文件。但是,现有的方案不能抵抗关键词猜测攻击。外部攻击者可以生成若干关键词密文上传到云服务器,侦测云服务器将这些密文返回给哪些用户,进而获取这些用户的搜索信息。因此,提出一种可以抵抗关键词猜测攻击的可搜索属性基加密方案。基于 DBDH 困难问题,该方案在选择安全模型中被证明是选择明文攻击安全的。

关键词 可搜索加密 属性基加密 关键词猜测攻击 隐私保护

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.03.050

A SEARCHABLE ATTRIBUTED-BASED ENCRYPTION SCHEME AGAINST KEYWORD GUESSING ATTACK

Wang Min Zhou Lijing Qin Lulu
(*School of Computer and Information, Hohai University, Nanjing 211100, Jiangsu, China*)

Abstract Searchable attribute-based encryption enables users whose attributes satisfy the access control strategy (or the attributes used to encrypt keywords to satisfy the access control strategy specified by the users' private keys) to search for encrypted files. However, existing schemes cannot resist keyword guessing attacks. External attackers can generate a number of keyword ciphertexts to upload to the cloud server. Then, these ciphertexts are returned to users by detecting the cloud server, and it is possible to know the search information of these users. Therefore, an searchable attribute-based encryption which can resist keyword guessing attacks is proposed. The scheme is proved to be selective plaintext attack security in the selective security model based on the DBDH difficult problem.

Keywords Searchable encryption Attributed-based encryption Keyword guessing attack Privacy protection

0 引 言

云计算允许用户将加密文件上传到云服务器,然后在需要时下载到本地。此外,上传的加密文件还可以分享给别的用户。随着上传文件的增多,用户需要对加密文件进行搜索,从而下载感兴趣的密文。带关键词搜索的公钥加密(Public key encryption with keyword search,PEKS)[1]允许用户对加密关键词进行搜索,同时不泄露搜索信息。但是,大部分 PEKS 方案[2-6]针对的是多对一环境,即多个发送者利用单个接收者的公钥生成密文。对于不同的接收者,发送者需要分别使用他们的公钥加密文件,然后接收者利用自己的私钥生成陷门来搜索密文。为了使同一份加密文件可以被多个接收者搜索,文献[7-8]提出可搜索属性基加密(Attributed-based encryption with keyword search,ABKS)。在 ABKS 中,发送者利用一个访问结构或属性集加密关键词,当且仅当用户的属性满足访问控制策略(或用来加密关键词的属性集满足用户私钥指定的访问控制策略)时,用户才可以搜索这些加密文件。但是,除了文献[9],大部分 ABKS 方案[10-17]不能抵抗关键词猜测攻击。需要指出的是,文献[9]

收稿日期:2019-03-10。国家自然科学基金项目(61772009)。**王敏**,硕士生,主研领域:可搜索属性基加密。**周李京**,硕士生。**秦璐璐**,硕士生。

需要隐藏访问控制策略,这样大大限制了方案的使用范围。关键词猜测攻击可以分为三种,分别是外部攻击者的离线关键词猜测攻击、外部攻击者的在线关键词猜测攻击和内部攻击者的离线关键词猜测攻击,具体参考文献[18 - 20]。外部攻击者可以生成若干关键词密文上传给云服务器,通过侦测云服务器将这些密文返回给哪些用户,从而获取这些用户的搜索信息。

因此,本文提出了一种可以抵抗关键词猜测攻击的可搜索属性基加密方案。方案包括四个参与方,分别是发送者、接收者、授权中心和云服务器。发送者必须先向授权中心获取发送者私钥才能生成密文。非法用户无法获取发送者私钥,也就无法生成合法密文,从而可以抵抗关键词猜测攻击。

1 预备知识

1.1 双线性对映射

设 G 和 G_T 是乘法循环群,它们的阶是素数 q,g 是群 G 的生成元,双线性对映射是 $e:G\times G\rightarrow G_T$,此双线对映射具有以下三种性质:

1) 双线性:对于任意 $g_1,g_2\in G$ 和 $a,b\in Z_q$,有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

2) 非退化性:对于任意 $g_1,g_2\in G$,有 $e(g_1,g_2)\neq 1$。

3) 可计算性:对于任意 $g_1,g_2\in G$,存在一个高效的算法计算出 $e(g_1,g_2)$。

1.2 DBDH 困难问题

设 G 和 G_T 是乘法循环群,它们的阶是素数 q,g 是群 G 的生成元,双线性对映射是 $e:G\times G\rightarrow G_T$。选取随机数 $a,b,c\in Z_q$,不存在一个概率多项式时间的敌手 $\mathcal{B}$ 能够以不可忽略的优势区分 $(g^a,g^b,g^c,e(g,g)^{abc})$ 和 $(g^a,g^b,g^c,e(g,g)^z)$。我们定义 $\mathcal{B}$ 能够区分它们的优势为:$\mathcal{Adv}_{\mathcal{B}}^{DBDH}(1^\delta)=|\Pr[\mathcal{B}(g^a,g^b,g^c,e(g,g)^{abc})=1]-Pr[\mathcal{B}(g^a,g^b,g^c,e(g,g)^z)=1]|$。

1.3 访问结构

假设 $P=\{P_1,P_2,\cdots,P_3\}$ 是一组参与方,$A\subseteq 2^P$ 是一个单调集合。如果集合 $B\in A$ 且 $B\subseteq C$,那么有 $C\in A$。对于非空集合 P,A 可作为一个访问结构。我们称属于 A 的集合是授权集合,不属于 A 的集合是非授权集合。

设 ω 和 A 分别是一个属性集合和访问结构,谓词 $\gamma(\omega,A)$ 定义如下:如果 $\omega\in A$,那么 $\gamma(\omega,A)=1$;否则,$\gamma(\omega,A)=0$。

2 方案设计

2.1 定 义

抗关键词猜测攻击的可搜索属性基加密方案由六个算法组成:设置算法、发送者私钥生成算法、接收者私钥生成算法、加密算法、陷门生成算法、搜索算法。

设置算法:该算法由授权中心运行。算法输入系统安全参数 l,输出公共参数 pm 和主私钥 mk。授权中心发布 pm,保留 mk。

发送者私钥生成算法:该算法由授权中心运行。算法输入主私钥 mk 和发送者的身份 ID,输出发送者私钥 $sk_{s,ID}$。发送者在生成密文前,先向授权中心请求获得发送者私钥。授权中心验证用户的身份后,将发送者私钥通过安全信道发送给用户。

接收者私钥生成算法:算法由授权中心运行。算法输入主私钥 mk 和一个访问结构 T,其中接收者的属性集 $Atts$ 满足 $\gamma(Atts,T)=1$,算法输出接收者私钥 sk_r。接收者在生成陷门前,先向授权中心请求获得接收者私钥。授权中心验证用户的身份后,将接收者私钥通过安全信道发送给用户。

加密算法:算法由发送者运行。算法输入关键词 w、属性集 $Atts$、发送者的身份 ID 和发送者私钥 $sk_{s,ID}$,输出关键词密文 cph。然后发送者将密文上传到云服务器。

陷门生成算法:算法由接收者运行。算法输入关键词 w' 和接收者私钥 sk_r,输出关键词陷门 td。然后接收者将关键词陷门发送给云服务器。

搜索算法:算法由云服务器运行。算法输入关键词密文 cph 和关键词陷门 td,输出搜索结果。一旦云服务器接收到关键词陷门,便运行搜索算法。如果搜索成功,则将相应的密文返回给用户;如果搜索失败,则返回搜索失败给用户。

2.2 构 造

抗关键词猜测攻击的可搜索属性基加密方案构造如下:

设置算法:给定安全参数 l,算法生成一个素数 q。选择一个双线性对映射 $e:G\times G\rightarrow G_T$,其中 G 和 G_T 是阶为 q 的乘法循环群,g 是群 G 的生成元。$H_1:\{0,1\}^*\rightarrow G$ 和 $H_2:\{0,1\}^*\rightarrow Z_q$ 是单向哈希函数。选择随机数 $s\in Z_q$,设置公共参数 pm 和主私钥 mk 为:$pm=(H_1,H_2,e,g,q,G,G_T)$,$mk=s$。

发送者私钥生成算法:算法输入主私钥 mk 和发送者的身份 ID,输出发送者私钥 $sk_{s,ID}=H_1(ID)^s$。

接收者私钥生成算法:算法输入一个访问结构树 T,输入主私钥 $mk=s$ 作为 T 的根节点。然后自上而下地设置树的内部节点和叶子结点的值。对于访问结构树 T 的每个叶子节点 $v\in lvs(T)$,选择随机数 $t\in Z_q$,计算 $X_v=g^{q_v(0)}H_1(att(v))^t$ 和 $Y_v=H_1(ID)^t$。接收者私钥为 $sk_r=(T,\{(X_v,Y_v)\mid v\in lvs(T)\})$。

加密算法:算法输入一个关键词 w、一个属性集 $Atts$、发送者的身份 ID 和发送者私钥 $sk_{s,ID}$。选择随机数 $r_1,r_2\in Z_q$,计算 $W'_1=H_1(ID)^{r_1}$,$W'_2=H_1(ID)^{r_2}$,$W=sk_{s,ID}^{r_1H_2(w)+r_2}=H_1(ID)^{s(r_1H_2(w)+r_2)}$。对于每个属性 $at_i\in Atts$,计算 $W_{i,1}=H_1(at_i)^{r_1}$,$W_{i,2}=H_1(at_i)^{r_2}$。密文 $cph=(Atts,W'_1,W'_2,W,\{W_{i,1},W_{i,2}\mid at_i\in Atts\})$。

陷门生成算法:算法输入一个关键词 w'和接收者私钥 sk_r。选择随机数 $u\in Z_q$,对于访问结构树 T 的每个叶子节点 $v\in lvs(T)$,其中 T 是接收者私钥 sk_r中的访问结构,计算 $X'_{v,1}=X_{v,1}^{uH_2(w')}$,$X'_{v,1}=X_{v,1}^{u}$,$Y'_{v,1}=Y_{v,1}^{uH_2(w')}$,$Y'_{v,1}=Y_{v,1}^{u}$。设 $TD=g^u$,关键词陷门为 $td=(T,TD,\{(X'_{v,1},X'_{v,2},Y'_{v,1},Y'_{v,2})\mid v\in lvs(T)\})$。

搜索算法:算法输入关键词密文 cph 和关键词陷门 td。对于密文 cph 指定的属性集 $Atts$,选择一个属性集 S,S 满足陷门 td 指定的访问结构 T。如果不存在这样的属性集,则搜索失败。否则,对于每一个属性 $at_i\in S$ 及叶子结点 $v\in lvs(T)$,其中 $att(v)=at_i$,计算 $Q_{v,1}=e(X'_{v,1},W'_1)/e(Y'_{v,1},W_{i,1})=e(H_1(ID),g)^{uH_2(w')r_1q_v(0)}$ 和 $Q_{v,2}=e(X'_{v,2},W'_2)/e(Y'_{v,2},W_{i,2})=e(H_1(ID),g)^{ur_2q_v(0)}$。然后根据访问结构 T,计算 $e(H_1(ID),g)^{uH_2(w')r_1q_{root}(0)}$ 和 $e(H_1(ID),g)^{ur_2q_{root}(0)}$,从而得到 $Q_{root,1}=e(H_1(ID),g)^{uH_2(w')sr_1}$ 和 $Q_{root,2}=e(H_1(ID),g)^{usr_2}$。计算 $e(W,TD)$,如果 $e(W,TD)=Q_{root,1}Q_{root,2}$,则搜索成功;否则,搜索失败。

方案的正确性如下:

$$e(W,TD)=e(H_1(ID)^{s(r_1H_2(w)+r_2)},g^u)=e(H_1(ID),g)^{us(r_1H_2(w)+r_2)}$$

$$Q_{root,1}Q_{root,2}=e(H_1(ID),g)^{us(r_1H_2(w')+r_2)}$$

3　安全性分析

3.1　安全模型

为了保证抗关键词猜测攻击的可搜索属性基加密方案的安全性,我们考虑密文不可区分和陷门不可区分。因为内部攻击者具有比外部攻击者更强的能力,这里我们仅考虑内部攻击者。让 $\mathcal{B}$ 作为一个概率多项式时间的敌手,我们考虑两种情况。第一种情况是 $\mathcal{B}$ 作为发送者,他可以获得任意 ID 的发送者私钥以及用其加密的关键词密文,但他仍然无法区分用他未获得的 ID 的发送者私钥加密的关键词密文。第二种情况是 $\mathcal{B}$ 作为接收者,他可以获得任意属性集对应的接收者私钥以及用其生成的关键词陷门,但他仍然无法区分用他未获得的属性集对应的接收者私钥生成的关键词陷门。我们将上述两种情况定义为两个游戏。

游戏一:假设 $\mathcal{B}$ 是一个发送者。

初始化:$\mathcal{B}$ 选择一个 ID 作为挑战 ID,即 ID_{ch},发送给挑战者 C。

设置阶段:C 运行设置算法,输入安全参数,输出公共参数和主私钥。C 将公共参数发送给 $\mathcal{B}$,保留主私钥。

询问阶段 1:$\mathcal{B}$ 询问 ID_i 的发送者私钥,$i\in\{1,2,\cdots,m\}$,限制是 $ID_i\neq ID_{ch}$。C 运行发送者私钥生成算法,生成 ID_i 的发送者私钥发送给 $\mathcal{B}$。然后 $\mathcal{B}$ 询问用 ID_{ch} 的发送者私钥加密的关键词 w_j 的密文,$j\in\{1,2,\cdots,n\}$。C 先运行发送者私钥生成算法生成 ID_{ch} 的发送者私钥,然后运行加密算法生成关键词 w_j 的密文发送给 $\mathcal{B}$。

挑战阶段:$\mathcal{B}$ 选择两个关键词 w_1^*、w_2^* 和一个属性集 $Atts$ 发送给 C,限制是 w_1^*、w_2^* 没有在询问阶段 1 询问过。C 随机选择 $b\in\{0,1\}$,运行加密算法生成 w_b^* 的密文发送给 $\mathcal{B}$。

询问阶段 2:$\mathcal{B}$ 继续询问更多的发送者私钥和用 ID_{ch} 的发送者私钥加密的关键词密文,唯一的限制是不能询问 ID_{ch} 的发送者私钥或者用 ID_{ch} 的发送者私钥加密关键词 w_1^*、w_2^* 的密文。

猜测阶段:最后,$\mathcal{B}$ 猜测 $b'\in\{0,1\}$ 作为 b 的值。如果 $b'=b$,$\mathcal{B}$ 赢得游戏。

游戏二:假设 $\mathcal{B}$ 是一个接收者。

初始化:$\mathcal{B}$ 选择一个属性集 $Atts$ 作为挑战,即 $Atts_{ch}$,并发送给挑战者 C。

设置阶段:C 运行设置算法,输入安全参数,输出公共参数和主私钥。C 将公共参数发送给 $\mathcal{B}$,保留主私钥。

询问阶段 1:$\mathcal{B}$ 询问属性集 $Atts_1,Atts_2,\cdots,Atts_m$ 对应的接收者私钥,限制是 $Atts_{ch}$ 不包含在 $Atts_i$ 中,其中 $i\in\{1,2,\cdots,m\}$。C 运行接收者私钥生成算法生成接收者私钥发送给 $\mathcal{B}$。然后 B 继续询问用 $Atts_{ch}$ 对应的接收者私钥生成的关键词 $w_1,w_2,\cdots,w_n$ 的陷门。C 运行接收者私钥生成算法生成 $Atts_{ch}$ 对应的接收者私钥,再运行陷门生成算法生成关键词陷门发送给 $\mathcal{B}$。

挑战阶段:$\mathcal{B}$ 选择两个关键词 w_1^*、w_2^* 发送给 C,限

制是 w_1^*、w_2^* 没有在询问阶段 1 询问过。C 随机选择 $b \in \{0,1\}$，运行陷门生成算法生成关键词 w_b^* 的陷门 td_b^* 并发送给 $\mathcal{B}$。

询问阶段 2：重复询问阶段 1，限制是不能询问用 $Atts_{ch}$ 对应的接收者私钥生成的 w_1^* 或 w_2^* 的陷门。

猜测阶段：最后，$\mathcal{B}$ 猜测 $b' \in \{0,1\}$ 作为的值。如果 $b'=b$，$\mathcal{B}$ 赢得游戏。

3.2 安全分析

密文不可区分：首先，因为哈希函数 H_1，拥有 ID_1，$ID_2,\cdots,ID_n$ 的发送者私钥 $sk_{s,ID_i}=H_1(ID_i)^s$，$i \in \{1,2,\cdots,m\}$，对得到 ID_{ch} 的发送者私钥没有任何帮助。其次，用 ID_{ch} 的发送者私钥生成关键词 w_b^* 的密文为 $W=sk_{s,ID_{ch}}^{r_1H_2(w_b^*)+r_2}=H_1(ID_{ch})^{s(r_1H_2(w_b^*)+r_2)}$。由于无法获得 ID_{ch} 的发送者私钥 $sk_{s,ID_{ch}}=H_1(ID_{ch})^s$，在拥有 $W'_1=H_1(ID_{ch})^{r_1}$ 和 $W'_2=H_1(ID_{ch})^{r_2}$ 的情况下猜对 b 的值的优势是可忽略的。

陷门不可区分：访问结构只允许属性满足控制策略的用户获得相应的接收者私钥，所以拥有属性集 $Atts_1$，$Atts_2,\cdots,Atts_m$ 对应的接收者私钥对获得属性集 $Atts_{ch}$ 对应的接收者私钥没有任何帮助。用属性集 $Atts_{ch}$ 对应的接收者私钥生成关键词 w_b^* 的陷门为 $e(H_1(ID),g)^{us(r_1H_2(w_b^*)+r_2)}$。假设敌手 $\mathcal{B}$ 获得了陷门中 ID 对应的发送者私钥 $H_1(ID)^s$，同时 $\mathcal{B}$ 拥有 $H_1(ID)^{r_1}$、$H_1(ID)^{r_2}$ 和 g^u。如果 $\mathcal{B}$ 能以不可忽略的优势猜对的值，那意味着 $\mathcal{B}$ 能够以不可忽略的优势获得 $e(H_1(ID),g)^{usr_1}$。令 $H_1(ID)^s=g^a$，$H_1(ID)^{r_1}=g^b$，$g^u=g^c$，那么 $\mathcal{B}$ 就能以同样的优势解决 DBDH 问题。由于 DBDH 问题是公开的困难问题，所以 $\mathcal{B}$ 区分陷门的优势是可忽略的。

4 性能分析

在这一部分，我们将本方案与文献[11]的 KP-ABKS 方案、文献[16]的 ABKS-CSC 方案和文献[17]的方案在计算代价、存储代价和功能三个方面进行对比。E 表示群 G 中的指数运算，E_T 表示群 G_T 中的指数运算，M 表示群 G 中的乘法运算，M_T 表示群 G_T 中的乘法运算，$Pair$ 表示配对运算。N 表示访问结构中叶子节点的数目，S 表示属性集中的属性个数，$|G|$ 表示群 G 中元素的存储长度。此外，由于哈希函数的计算比其他算法高效得多，这里忽略哈希函数的计算时间。从表 1 和表 2 可以看出，本方案在计算代价和存储代价方面不如 KP-ABKS 方案、ABKS-CSC 方案和文献[17]的方案，但表 3 显示本方案在陷门不可区分和抗关键词猜测攻击两个方面性能优于 KP-ABKS，在抗关键词猜测攻击方面性能优于 ABKS-CSC 方案和文献[17]的方案。

表 1 计算代价对比

方案	KeyGen	Enc	TokenGen	Search
KP-ABKS 方案	$3NE+NM$	$(S+4)E+M$	$(2N+3)E+M$	$(2S+2)Pair+SE_T+(S+1)M_T$
ABKS-CSC 方案	$(N+3)E+M$	$SM+Pair\ 3E+E_T$	$(2N+2)E+(N+2)M$	$2Pair+2M_T$
文献[17]方案	$2NE+2NM$	$(2S+2)E+(S+1)Pair+SM+SM_T$	$(2N+1)M+(3N+1)E$	$2Pair+2M_T$
本方案	$(3N+1)E+NM$	$(2S+3)E$	$(4N+1)E$	$(4S+1)Pair+2SE_T+2SM_T$

表 2 存储代价对比

方案	KeyGen	Enc	TokenGen	Search
KP-ABKS 方案	$2N\|G\|$	$(S+3)\|G\|$	$(2N+2)\|G\|$	1
ABKS-CSC 方案	$(N+2)\|G\|$	$4\|G\|$	$2\|G\|$	1
文献[17]方案	$(N+1)\|G\|$	$4\|G\|$	$2\|G\|$	1
本方案	$(2N+1)\|G\|$	$(2S+3)\|G\|$	$(4N+1)\|G\|$	1

表 3 功能对比

方案	密文不可区分	陷门不可区分	抗关键词猜测攻击
KP-ABKS 方案	√	×	×
ABKS-CSC 方案	√	√	×
文献[17]方案	√	√	×
本方案	√	√	√

5 结 语

本文提出了一种抗关键词猜测攻击的可搜索属性基加密方案。通过与 KP-ABKS 方案、ABKS-CSC 方案和文献[17]的方案进行比较，本方案在陷门不可区分和抗关键词猜测攻击两方面性能优于 KP-ABKS 方案，在抗关键词猜测攻击方面性能优于 ABKS-CSC 方案和文献[17]的方案，但在计算效率和存储代价两方面不如 KP-ABKS 方案、ABKS-CSC 方案和文献[17]的方案。所以，下一阶段的目标是在不改变方案性能的基础上提高本方案的计算效率和存储代价。

参 考 文 献

[1] Boneh D, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3027, Springer-Verlag, 2004: 506 – 522.

[2] Zhang B, Zhang F. An efficient public key encryption with conjunctive-subset keywords search[J]. Network and Computer Application, 2011, 34(1): 262 – 267.

[3] Dong Q X, Guan Z, Wu L, et al. Fuzzy keyword search over encrypted data in the public key setting[C]//Web-Age Information Management, LNCS 7923, Springer-Verlag, 2013: 729 – 740.

[4] Lv Z Q, Hong C, Zhang M, et al. Expressive and secure searchable encryption in the public key setting[C]//Springer International Publishing, LNCS 8783, Springer-Verlag, 2014: 364 – 376.

[5] Chen R M, Mu Y, Yang G M, et al. Server-aided public key encryption with keyword search[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2833 – 2842.

[6] Huang Q, Li H. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks [J]. Information Sciences, 2017, 403/404: 1 – 14.

[7] Kaushik K, Varadharajan V, Nallusamy R. Multi-user attribute based searchable encryption[C]//IEEE 14th International Conference on Mobile Data Management. IEEE Computer Society, 2013: 200 – 205.

[8] Wang C, Li W, Li Y. A ciphertext-policy attribute-based encryption scheme supporting keyword search function [M]//Cyberspace Safety and Security, Springer International Publishing, 2013: 377 – 386.

[9] 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, 2017, 60(5):130 – 141.

[10] Li S, Xu M. Attribute-based public encryption with keyword search[J]. Chinese Journal of Computers, 2014, 37(5): 1017 – 1024.

[11] Zheng Q, Xu S, Ateniese G. VABKS: Verifiable attribute-based keywordsearch over outsourced encrypted data[C]// IEEE Conference on Computer Communications, 2014: 522 – 530.

[12] Sun W, Yu S, Lou W. Protecting your right: Attribute-based keywordsearch with fine-grained owner-enforced search authorization in the cloud[C]//IEEE INFOCOM, 2014: 226 – 234.

[13] Miao Y B, Ma J F, Liu X M, et al. m2-ABKS: attribute-based multi-keyword search over encrypted personal health records in multi-owner setting[J]. Medical Systems, 2016, 40(11):1 – 12.

[14] 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): 1099 – 1131.

[15] 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, DOI: 10.1109/TSC.2017.2757467.

[16] Yang Y, Han J, Willy S, et al. ABKS-CSC: attribute-based keyword search with constant-size ciphertexts[J]. Security and Communication Networks, 2016, 9(18): 5003 – 5015.

[17] Han J, Yang Y, Liu J K, et al. Expressive attribute-based keyword search with constant-size ciphertext[J]. Soft Computing, 2018, 22(15): 5163 – 5177.

[18] Byun J W, Rhee H S, Park H A, et al. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[C]//Secure Data Management, LNCS 5060, Springer-Verlag, 2006: 75 – 83.

[19] Yau W C, Heng S, Goi B. Off-line keyword guessing attacks on recent public key encryption with keyword search schemes [C]//Autonomic and Trusted Computing, LNCS 5060, Springer-Verlag, 2008: 100 – 105.

[20] Yau W C, Phan R C, Heng S H, et al. Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester[J]. International Journal of Computer Mathmatics, 2013, 90(12): 2581 – 2587.

(上接第 219 页)

[23] Christlein V, Riess C, Jordan J, et al. An evaluation of popular copy-move forgery detection approaches[J]. IEEE Transactions on Information Forensics & Security, 2012, 7 (6):1841 – 1854.

[24] Amerini I, Ballan L, Caldelli R, et al. A SIFT-based forensic method for copy-move attack detection and transformation recovery[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(3):1099 – 1110.

[25] Kulis B, Grauman K. Kernelized locality-sensitive hashing for scalable image search[C]//IEEE International Conference on Computer Vision. IEEE, 2010:2130 – 2137.

[26] Gong Y, Lazebnik S, Gordo A, et al. Iterative quantization: a Procrustean approach to learning binary codes for large-scale image retrieval. [J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2013, 35(12):2916 – 2929.

[27] Jin Z, Li C, Lin Y, et al. Density sensitive hashing[J]. IEEE Transactions on Cybernetics, 2017, 44(8):1362 – 1371.

[28] Raginsky M. Locality-sensitive binary codes from shift-invariant kernels[C]//Advances in Neural Information Processing Systems, 2009:1509 – 1517.