

非安全信道下的高效可搜索加密方案

程晋雪¹, 许春根¹, 徐磊¹, 赵泽茂², 薛春阳³

(1. 南京理工大学 理学院, 南京 210094; 2. 丽水学院 工学院, 浙江 丽水 323000;
3. 安徽省天长市公安局 网络安全保安大队, 安徽 天长 239300)

摘 要: 为对云存储技术中的密文数据进行安全检索, 提出一种非安全信道下的可搜索加密方案, 并给出将双系统加密方案转换到非安全信道下的双系统可搜索加密方案的一般方法。云端服务器通过与用户提供的关键词相对应的陷门, 从大量加密文件中检索包含特定关键词的文件, 而无需获知关于云中原始文件的任何信息。分析结果表明, 与传统可搜索加密数据检索方案相比, 该方案能够缩短陷门与密文的长度, 且验证过程仅需 2 次双线性对运算。

关键词: 数据检索; 双系统; 可搜索加密; 非安全信道; 合数阶双线性群

中文引用格式: 程晋雪, 许春根, 徐磊, 等. 非安全信道下的高效可搜索加密方案[J]. 计算机工程, 2019, 45(7): 188-193.

英文引用格式: CHENG Jinxue, XU Chungen, XU Lei, et al. Efficient searchable encryption scheme in unsecure channel[J]. Computer Engineering, 2019, 45(7): 188-193.

Efficient Searchable Encryption Scheme in Unsecure Channel

CHENG Jinxue¹, XU Chungen¹, XU Lei¹, ZHAO Zema², XUE Chunyang³

(1. School of Science, Nanjing University of Science and Technology, Nanjing 210094, China;

2. Institute of Technology, Lishui University, Lishui, Zhejiang 323000, China;

3. Network Security Brigade, Tianchang Municipal Public Security Bureau of Anhui Province, Tianchang, Anhui 239300, China)

[Abstract] In order to securely retrieve the ciphertext data in cloud storage technology, a searchable encryption scheme in unsecure channel is proposed, and a general method for converting the dual-system encryption scheme into the dual-system searchable encryption scheme in unsecure channel is given. Cloud servers retrieve files containing specific keywords from a large number of encrypted files through traps corresponding to the keywords provided by users without knowing any information about the original files in the cloud. Analysis results show that compared with the traditional searchable encryption data retrieval scheme, the proposed scheme can shorten the length between trapdoor and ciphertext, and the verification process only needs two bilinear pairings operations.

[Key words] data retrieval; dual-system; searchable encryption; unsecure channel; composite order bilinear pairings

DOI: 10.19678/j.issn.1000-3428.0052000

0 概述

云计算技术为当今大量数据的存储、处理与传输提供了便利与保障。云存储对云计算进行延伸与发展, 使数据具有高效可用性、易访问性, 并通过将数据外包到远程服务器来降低基础架构的成本。云存储技术因便捷的存储功能而得到广大用户的青睐, 成为目前主流的数据存储方式, 用户可以随时随地访问数据而无需使用专用机器。

云存储技术的快速发展也带来各种安全问题。目前, 用户的大量数据均以明文的形式呈现, 当用户

将其数据外包给远程服务器时, 对数据的物理访问将丢失, 且数据委托给服务器进行管理后, 云端服务器可以查看、篡改甚至删除数据。对明文数据进行搜索时, 用户将查询关键词发送给服务器以便检索相应的文档。在搜索结束后, 服务器将搜索结果返回给用户。但是, 在搜索过程中, 存储在服务器上的数据内容和查询关键词都会呈现给半可信服务器, 这将大幅降低用户数据的私密性。因此, 保护用户敏感数据的隐私成为亟需解决的问题。实现数据隐私的最常见方式是用户在外包数据给云端服务器之前对其进行加密, 一旦这些加密数据离开用户, 将受

基金项目: 江苏省自然科学基金“面向云存储的密文访问控制理论研究”(BK20141405); 浙江省自然科学基金“面向物联网的位置隐私保护技术研究”(Y15F020053)。

作者简介: 程晋雪(1992—), 女, 硕士研究生, 主研方向为密码学、信息安全; 许春根, 教授; 徐磊, 博士; 赵泽茂, 教授; 薛春阳, 学士。

收稿日期: 2018-07-03 **修回日期:** 2018-08-20 **E-mail:** xuchung@njjust.edu.cn

到一个端对端的数据隐私保护。虽然这种解决方案保证了敏感数据的隐私,但它加大了服务器对加密数据进行有效操作的难度。

为解决上述问题,可搜索加密技术应用而生,其不仅是一种加密方案,而且支持对加密数据进行关键词搜索。通过可搜索加密技术,用户可以提供与搜索关键词相对应的陷门给云端服务器,服务器将该陷门与密文文件进行匹配,从而检索包含特定关键词的文件,并将其返回给用户。通过这种方式,用户可以直接在云端进行搜索,从而提高了搜索效率,降低了不包含搜索关键词的文件的存储空间。此外,服务器除能够猜测到任意2个搜索文件是否包含相同关键词以外,不会获知关于云中原始文件的任何信息,使得该技术具有更高的安全性。

文献[1]利用基于身份的加密(Identity-Based Encryption, IBE)构造公钥可搜索加密方案 PEKS。该方案允许多个用户利用公钥进行加密,但仅拥有相应私钥的用户才能搜索加密数据。文献[2]提出一种可搜索加密审计日志的方案,该方案可以与任何数量的现有方法相结合以创建防篡改日志。此外,其为数据库查询设置一个审计日志,该日志通过哈希链实现其完整性以及 IBE,以便在加密日志上进行搜索。文献[3]设计2种可搜索加密方案。第1种方案可以保证在非自适应安全下,使用链表、数组和表格数据结构来连接不同的关键词,从而提高搜索性能。第2种方案为一种广播加密方式,其用户能够共享密文数据。文献[4]提出一种基于配对的 PEKS 方案,并进一步从 PEKS 中去除安全信道,提出一种高效的非安全信道下的 PEKS 方案。文献[5]提出带有注册关键词搜索的公钥加密方案。该方案为底层应用程序提供额外的功能,并在打击垃圾邮件方面发挥重要作用。文献[6-7]设计一种有效的可搜索加密方案。文献[8]提出非安全信道下的 PEKS 方案(SCF-PEKS)。文献[9]构建一种基于分组的结构概念,将现有可搜索加密方案转变为隐藏搜索模式的新型可搜索方案。文献[10]提出端对端的基于身份的可搜索加密方案。文献[11]提出基于混沌映射的具有指定服务器的时间感知多关键词可搜索加密方案。文献[12]提出云存储中高效安全的数据检索方案。文献[13]提出一种能够抵抗内部关键词猜测攻击的公钥可搜索加密方案。近年来,支持更多功能并具有更高安全性的可搜索加密方案相继被提出,如可验证的公钥可搜索加密方案^[14]、支持非对称排序的可搜索加密方案^[15]等。

本文提出一种信息检索方案,以实现云端数据的安全存储。已有可搜索加密方案需要终止条件,为解决该问题,设计一种在合数阶群上的双系统可搜索加密数据检索方案^[16],并提供将该双系统加密方案转换到非安全信道下的双系统可搜索加密方案

的一般方法。

1 相关知识

1.1 PEKS 方案

定义 1 带关键词的公钥可搜索加密方案 PEKS^[1]包含以下6个多项式时间算法:

1) Setup(λ):输入安全参数 λ ,算法生成一个公共参数 cp 。

2) KeyGen_{Server}:输入公共参数 cp ,算法生成服务器的公私钥对 (pk_s, sk_s) 。

3) KeyGen_{Receiver}:输入公共参数 cp ,算法生成接受者的公私钥对 (pk_r, sk_r) 。

4) PEKS:输入公共参数 cp 、服务器的公钥 pk_s 、接受者的公钥 pk_r 和一个关键词 W ,算法生成关键词 W 的一个可搜索密文 S 。

5) Trapdoor:输入公共参数 cp 、接受者的私钥 sk_r 和一个关键词 W' ,算法生成一个陷门 $T_{W'}$ 。

6) Verify:输入接受者的公钥 pk_r 、可搜索密文 $S = \text{PEKS}(pk_r, W)$ 和陷门 $T_{W'} = \text{Trapdoor}(sk_r, W')$,如果 $W = W'$,输出1;否则,输出0。

1.2 安全模型

基于文献[8]的安全模型,本文从语义安全的角度定义 SCF-PEKS 方案的安全性,以确保未获得给定关键词陷门的服务器不能分辨 PEKS 密文包含哪些关键词,同时确保未获得服务器私钥的外部攻击者(Outside Attacker, OA)即使获得了关键词的所有陷门,也无法对 PEKS 密文进行区分(这种情况称为 IND-SCF-CKA)。在下文中,将上述2种类型的攻击者分别称为 $\text{Game}_{\text{Server}}$ 和 $\text{Game}_{\text{outside}}$ 。

定义 2(IND-SCF-CKA) 令 λ 为安全参数, A 为敌手,考虑敌手 A 与挑战者 B 之间的2个游戏:

游戏 1 假设敌手 A 是一个服务器。游戏分为以下阶段:

1) 开始:运行公共参数生成算法 Setup(λ)、公私钥对生成算法 KeyGen_{Server} 和 KeyGen_{Receiver}。生成公共参数 cp 、服务器的公私钥对 (pk_s, sk_s) 和接受者的公私钥对 (pk_r, sk_r) 。发送 cp, sk_s, pk_r 给 A ,其中, sk_r 保持私密。

2) 阶段1:对于任意关键词 W ,敌手 A 适应性地对 B 进行陷门询问, B 对该询问生成 $T_{W'} = \text{Trapdoor}(sk_r, W')$ 并发送给 A 。

3) 挑战:一旦阶段1的适应性询问结束, A 发送2个挑战关键词 W_0, W_1 (限制条件是 A 没有事先对 W_0, W_1 进行陷门询问得到 T_{W_0}, T_{W_1})。挑战者 B 挑选一个随机数 $b \in \{0, 1\}$, 并计算 $C^* = \text{PEKS}(pk_s, pk_r, W_b)$ 作为挑战密文发送给 A 。

4) 阶段2:与阶段1相同,对于除关键词 W_0, W_1 以外的任意关键词 W , A 继续对 B 进行陷门询问, B 对其作出回应。

5) 猜测: A 输出 $b' \in \{0, 1\}$, 如果 $b' = b$, 则 A 赢得游戏。

A 赢得游戏 1 的优势是:

$$Adv_A^{\text{GameServer}}(\lambda) = \left| \Pr[b' = b] - \frac{1}{2} \right|$$

游戏 2 假设敌手 A 是一个 OA(包括接受者)。游戏分为以下阶段:

1) 开始: 运行公共参数生成算法 $\text{Setup}(\lambda)$ 、公私钥对生成算法 $\text{KeyGen}_{\text{Server}}$ 和 $\text{KeyGen}_{\text{Receiver}}$, 生成公共参数 cp 、服务器的公私钥对 (pk_s, sk_s) 和接受者的公私钥对 (pk_r, sk_r) 。发送 cp, sk_s, pk_r 给 A , 其中, sk_r 保持私密。

2) 阶段 1: 对于任意关键词 W , 敌手 A 适应性地对 B 进行陷门询问, B 对该询问生成 $T_{W'} = \text{Trapdoor}(sk_r, W')$ 并发送给 A 。

3) 挑战: 一旦阶段 1 的适应性询问结束, A 发送 2 个挑战关键词 W_0, W_1 (限制条件是 A 没有事先对 W_0, W_1 进行陷门询问得到 T_{W_0}, T_{W_1})。挑战者 B 挑选一个随机数 $b \in \{0, 1\}$, 并计算 $C^* = \text{PEKS}(pk_s, W)$ 作为挑战密文发送给 A 。

4) 阶段 2: 与阶段 1 相同, 对于除关键词 W_0, W_1 以外的任意关键词 W , A 继续对 B 进行陷门询问, B 对其作出回应。

5) 猜测: A 输出 $b' \in \{0, 1\}$, 如果 $b' = b$, 则 A 赢得游戏。

A 赢得游戏 2 的优势是:

$$Adv_A^{\text{GameOutside}}(\lambda) = \left| \Pr[b' = b] - \frac{1}{2} \right|$$

定义 3 对于一个多项式时间敌手 A , 如果 $Adv_A^{\text{GameServer}}(\lambda)$ 和 $Adv_A^{\text{GameOutside}}(\lambda)$ 是可忽略函数, 则 SCF-PEKS 方案在抵抗适应性选择关键词攻击下是语义安全的。

1.3 合数阶双线性群

令 G, G_T 表示 2 个合数阶为 N 的双线性群, 其中, $N = p_1 p_2 \cdots p_m, p_1, p_2, \cdots, p_m$ 是互不相同的素数。映射 $e: G \times G \rightarrow G_T$ 满足以下性质:

1) 双线性: $\forall g, h \in G, a, b \in \mathbb{Z}_N$, 有 $e(g^a, h^b) = e(g, h)^{ab}$ 。

2) 非退化性: $\forall g \in G, e(g, g) \neq 1$ 。

3) 可计算性: $\forall g \in G, e(g, g)$ 可以有效地计算。

令 G_{p_1}, G_{p_2} 和 G_{p_3} 分别表示 G 的阶为 p_1, p_2 和 p_3 的子群。选取 $h_i \in G_{p_i}, h_j \in G_{p_j}$, 其中, $i \leq j$, 则 $e(h_i, h_j)$ 是 G 中的单位元。假设 g 是 G 的一个生成元, 则易知 $g^{p_1 p_2}$ 是 G_{p_3} 的生成元, $g^{p_1 p_3}$ 是 G_{p_2} 的生成元, $g^{p_2 p_3}$ 是 G_{p_1} 的生成元。因此, 存在 α_1, α_2 , 使得 $h_1 = (g^{p_2 p_3})^{\alpha_1}, h_2 = (g^{p_1 p_3})^{\alpha_2}$ 。此时有:

$$e(h_1, h_2) = e(g^{p_2 p_3 \alpha_1}, g^{p_1 p_3 \alpha_2}) = e(g^{\alpha_1}, g^{p_3 \alpha_2})^{p_1 p_2 p_3} = 1$$

由此可知, $G_{p_1}, G_{p_2}, G_{p_3}$ 相互正交, 这一性质是构

造本文方案的重要依据。

假设 1 给定一个群生成器 G , 定义以下分布:

$$E: = (N = p_1 p_2 p_3, G, G_T, e) \xleftarrow{R} G$$

$$g \xleftarrow{R} G_{p_1}, X_3 \xleftarrow{R} G_{p_3}$$

$$D: = (G, g, X_3)$$

$$T_1 \xleftarrow{R} G_{p_1 p_2}, T_2 \xleftarrow{R} G_{p_1}$$

敌手 A 攻破假设 1 的优势是:

$$Adv1_{G,A}: = \left| \Pr[A(D, T_1) = 1] \right| - \left| \Pr[A(D, T_2) = 1] \right|$$

定义 4 对于任意的概率多项式时间敌手 A , 如果 $Adv1_{G,A}(\lambda)$ 是一个关于 λ 的可忽略函数, 则 G 满足假设 1。

假设 2 给定一个群生成器 G , 定义以下分布:

$$E: = (N = p_1 p_2 p_3, G, G_T, e) \xleftarrow{R} G$$

$$g, X_1 \xleftarrow{R} G_{p_1}$$

$$X_2, Y_2 \xleftarrow{R} G_{p_2}$$

$$X_3, Y_3 \xleftarrow{R} G_{p_3}$$

$$D: = (G, g, X_1 X_2, X_3, Y_2 Y_3)$$

$$T_1 \xleftarrow{R} G, T_2 \xleftarrow{R} G_{p_1 p_3}$$

敌手 A 攻破假设 2 的优势是:

$$Adv2_{G,A}: = \left| \Pr[A(D, T_1) = 1] \right| - \left| \Pr[A(D, T_2) = 1] \right|$$

定义 5 对于任意的概率多项式时间敌手 A , 如果 $Adv2_{G,A}(\lambda)$ 是一个关于 λ 的可忽略函数, 则 G 满足假设 2。

假设 3 给定一个群生成器 G , 定义以下分布:

$$E: = (N = p_1 p_2 p_3, G, G_T, e) \xleftarrow{R} G$$

$$\alpha, \beta, s \xleftarrow{R} \mathbb{Z}_N, g \xleftarrow{R} G_{p_1}$$

$$X_2, Y_2, Z_2 \xleftarrow{R} G_{p_2}, X_3 \xleftarrow{R} G_{p_3}$$

$$D: = (G, g, g^\alpha X_2, X_3, g^s Y_2, Z_2)$$

$$T_1 = (e(g, g)^\alpha e(g, g)^\beta)^s, T_2 \xleftarrow{R} G_{p_1 p_3}$$

敌手 A 攻破假设 3 的优势是:

$$Adv3_{G,A}: = \left| \Pr[A(D, T_1) = 1] \right| - \left| \Pr[A(D, T_2) = 1] \right|$$

定义 6 对于任意的多项式时间敌手 A , 如果 $Adv3_{G,A}(\lambda)$ 是一个关于 λ 的可忽略函数, 则 G 满足假设 3。

2 非安全信道下的双系统可搜索加密方案

2.1 方案构建

本文方案包括以下算法:

1) **Setup**: 选择一个阶为 $N = p_1 p_2 p_3$ 的双线性群, 其中, p_1, p_2, p_3 是不同的素数。令 G_{p_i} 表示 G 的阶为 p_i 的子群, 随机选取 $u, g, h \in G_{p_1}$, 则公共参数表示为:

$$cp = \{G, G_T, e, N, u, g, h\}$$

2) $\text{KeyGen}_{\text{Server}}$: 随机均匀选取一个 $\alpha \in \mathbb{Z}_N$, 计算 $e(g, g)^\alpha$, 返回 $pk_S = (cp, e(g, g)^\alpha)$ 和 $sk_S = \alpha$ 分别作为服务器的公钥。

3) $\text{KeyGen}_{\text{Receiver}}$: 随机均匀选取一个 $\beta \in \mathbb{Z}_N$, 计算 $e(g, g)^\beta$, 返回 $pk_R = (cp, e(g, g)^\beta)$ 和 $sk_R = \beta$ 分别作为接收者的公钥。

4) PEKS: 输入关键词 $W \in \mathbb{Z}_N$ 、服务器的公钥 pk_S 和接受者的公钥 pk_R , 随机选取一个 $s \in \mathbb{Z}_N$, 计算密文:

$$C = [(u^W h)^s, g^s, (e(g, g)^\alpha e(g, g)^\beta)^s] = [C_0, C_1, C_2]$$

5) Trapdoor: 输入搜索关键词 $W' \in \mathbb{Z}_N$ 、接受者的私钥 sk_R , 随机选取一个 $r \in \mathbb{Z}_N$ 和 $R_3, R_3' \in G_{p_3}$, 计算陷门:

$$T = [g^\beta (u^{W'} h)^{r'} R_3', g^r R_3] = [T_0, T_1]$$

6) Verify: 输入密文 C 、陷门 T 和服务器的私钥 sk_S , 验证 $e(g^\alpha T_0, C_1)/e(T_1, C_0) = C_2$ 是否成立, 若等式成立, 输出 1; 否则, 输出 0。

上述方案正确性验证如下:

如果 $W' = W$, 则:

$$\begin{aligned} \frac{e(g^\alpha T_0, C_1)}{e(T_1, C_0)} &= \frac{e(g^\alpha g^\beta (u^{W'} h)^{r'} R_3', g^s)}{e(g^r R_3, (u^{W'} h)^s)} = \\ &= \frac{e(g^\alpha g^\beta, g^s) e((u^{W'} h)^{r'} R_3', g^s)}{e(g^r R_3, (u^{W'} h)^s)} = \\ &= \frac{e(g, g)^\alpha e(g, g)^\beta e(u^{W'} h, g)^{rs}}{e(u^{W'} h, g)^{rs}} = \\ &= (e(g, g)^\alpha e(g, g)^\beta)^s = C_2 \end{aligned}$$

如果 $W' \neq W$, 则:

$$e(g^\alpha T_0, C_1)/e(T_1, C_0) \neq C_2$$

2.2 semi-functional 算法

为对方案的安全性进行证明, 本文引入 2 个新的数据结构: semi-functional 陷门, semi-functional 密文。2 个数据结构的构造过程如下:

1) 令 g_2 是子群 G_{p_2} 的一个生成元, semi-functional 陷门构造过程如下:

(1) 运行 Trapdoor 生成算法生成正式陷门 $T = [T_0, T_1]$ 。

(2) 随机选择 2 个元素 $\gamma, z_k \in \mathbb{Z}_N$, 则 semi-functional 陷门为:

$$T' = (T_0 g_2^{\gamma z_k}, T_1 g_2^\gamma) = (T'_1, T'_2)$$

2) semi-functional 密文的构造方式如下:

(1) 运行 PEKS 生成算法生成正式密文 $C = [C_0, C_1, C_2]$ 。

(2) 随机选择 2 个元素 $x, z_c \in \mathbb{Z}_N$, 则 semi-functional 密文为:

$$C' = (C_0 g_2^{x z_c}, C_1 g_2^x, C_2) = (C'_0, C'_1, C'_2)$$

如果一个 semi-functional 陷门用来搜索 semi-

functional 密文, 致盲因子将被另外一个因子 $e(g_1, g_2)^{xy(z_k - z_c)}$ 所掩盖, 只有当 $z_k = z_c$, 验证算法才有效。在这种情况下, 定义陷门名义上是 semi-functional, 它有 G_{p_2} 中的项, 但并不妨碍验证。

一个 semi-functional 陷门能够验证所有正式生成的密文, 却不能验证一个 semi-functional 密文。同样, 一个 semi-functional 密文只能由正式陷门进行验证。

3 安全性证明

本节在标准模型下, 使用 $\text{Game}_{\text{Server}}$ 和 $\text{Game}_{\text{Outside}}$ 中的如下 2 个命题对本文加密方案进行安全性证明。

命题 1 在子群判定性问题下, 本文加密方案在标准模型的 $\text{Game}_{\text{Server}}$ 抗适应性选择关键词攻击下是语义安全的。

命题 1 的证明主要依赖于第 2 节中的假设 1、假设 2、假设 3 这 3 个困难性假设, 其主要论点是以下所描述的 4 种游戏在已知的困难性假设下相互之间不可区分。

1) $\text{Game}_{\text{Real}}$: 真实的安全性游戏。

2) $\text{Game}_{\text{Restricted}}$: 与真实的安全性游戏相似, 除限制攻击者不能询问与挑战关键词相同的关键词陷门。

3) Game_k : 与 $\text{Game}_{\text{Restricted}}$ 相似, 除限制所有的可搜索密文以及前 k 个陷门由 semi-functional 算法生成。

4) $\text{Game}_{\text{Final}}$: 与 Game_k 相似, 除限制挑战密文由 semi-functional 算法生成, 其中, 挑战密文用 S_w^f 表示。

设运行一个安全性游戏, 如果其中的挑战密文和陷门都是 semi-functional 的, 则此时验证效果将无效。一个概率多项式时间对手 A 至多进行 t 次陷门询问, 用如下 4 个引理则能够证明上述游戏之间的不可区分性。

引理 1 假设存在一个算法 A , 满足 $\text{Game}_{\text{Real}} \text{Adv}_A - \text{Game}_{\text{Restricted}} \text{Adv}_A = \varepsilon$, 则存在一个算法 B 以大于 $\varepsilon/2$ 的优势攻破假设 1 或者假设 2。

证明 算法 B 初始化子群判定问题的元组 $(N = p_1 p_2 p_3, G, G_T, e, g, X_3)$ 。 B 与 A 模拟 $\text{Game}_{\text{Real}}$: A 选择 2 个关键词 W 和 W^* 发送给 B , 其中, $W \neq W^*, p_2 \nmid (W - W^*)$ 。 B 计算 $a = \gcd(W - W^*, N)$, 然后令 $b = N/a$ 。因此, $p_2 \mid a$, 又由 $N = ab = p_1 p_2 p_3$, 考虑以下 2 种情况:

1) $p_1 \mid b$ 。

2) $a = p_1 p_2, b = p_3$ 。

在上述 2 种情况中, 必定有一种会以至少 $\varepsilon/2$ 的概率出现。

情况 1 B 攻破假设 1。因为 B 可以通过测试 g^b 是否为关键词来确定 $p_1 \mid b$, 从而测试 T^b 是否为关

关键词。若是,则 $T \in G_{p_1}$; 否则, $T \in G_{p_1 p_2}$ 。

情况 2 B 攻破假设 2。因为 B 可以通过测试 $(X_1 X_2)^a$ 是否为关键词来确定 $a = p_1 p_2$, 从而测试 $e((Y_2 Y_3)^b, T)$ 是否为关键词。若是,则 $T \in G_{p_1 p_3}$; 否则, $T \in G$ 。

引理 2 假设存在一个算法 A , 有 $\text{Game}_{\text{Restricted Adv}_A} - \text{Game}_0 \text{Adv}_A = \varepsilon$, 则存在一个算法 B 以 ε 的优势攻破假设 1。

证明 给定 g, X_3, T, B 与 A 模拟 $\text{Game}_{\text{Restricted}}$ 或 Game_0 如下:

1) 开始。 B 随机选择 $a, b \in \mathbb{Z}_N$, 令 $u = g^a, h = g^b$, 公共参数 $cp = (N, u, g, h)$ 。随机均匀选择 $\alpha, \beta \in \mathbb{Z}_N$, 计算 $e(g, g)^\alpha, e(g, g)^\beta$ 。令服务器的公私钥对为 $pk_s = (cp, e(g, g)^\alpha), sk_s = \alpha$, 接受者的公私钥对为 $pk_r = (cp, e(g, g)^\beta), sk_r = \beta$ 。然后发送 pk_r, pk_s, sk_s 给 A 。

2) 陷门询问阶段 1。对于一个关键词 W_i , 敌手 A 适应性地对 B 进行陷门询问。 B 随机选取 $r_i, t_i, W_i \in \mathbb{Z}_N$, 计算 $T_0 = g^\beta (u^{W_i} h)^{r_i} X_3^{W_i}, T_1 = g^{r_i} X_3^{t_i}$ 并作为询问陷门发送给 A 。

3) 挑战。一旦阶段 1 的适应性询问结束, A 发送 2 个挑战关键词 W_0, W_1 (限制条件是 A 没有事先对 W_0, W_1 进行陷门询问得到 T_{W_0}, T_{W_1})。挑战者 B 挑选一个随机数 $t \in \{0, 1\}$, 并计算 $C_0 = T^{a W_t + b}, C_1 = T, C_2 = e(T, g)^a e(T, g)^\beta$ 作为挑战密文发送给 A 。

4) 陷门询问阶段 2。与阶段 1 相同, 对于除关键词 W_0, W_1 以外的任意关键词 W , A 继续对 B 进行陷门询问, B 对其作出回应。

5) 猜测。假如 $T \in G_{p_1}$, 则上述密文是一个正式密文; 假如 $T \in G_{p_1 G_{p_2}}$, 则上述密文是一个 semi-functional 可搜索密文, 且 $z_c = \alpha W_t + b$ 。其中, $z_c \bmod p_2$ 与 $a \bmod p_1$ 和 $b \bmod p_1$ 的值不相关, 则该 semi-functional 可搜索密文具有合理的分布。因此, 通过 A 的输出, B 可以从这些可能性中区分 T 。

引理 3 假设存在一个算法 A , 且其满足

$|\text{Game}_{k-1} \text{Adv}_A - \text{Game}_k \text{Adv}_A| = \varepsilon$, 则存在一个算法 B 以 ε 的优势攻破假设 2。

证明 首先给定 $g, X_1, X_2, X_3, Y_2, Y_3, T, B$ 与 A 模拟 Game_{k-1} 和 Game_k , 此过程与引理 2 的证明过程相似, 此处不再赘述。

引理 4 假设存在一个算法 A , 且其满足 $|\text{Game}_k \text{Adv}_A - \text{Game}_{\text{Final}} \text{Adv}_A| = \varepsilon$, 则存在一个算法 B 以 ε 的优势攻破假设 3。

证明 首先给定 $g, g^a X_2, X_3, g^s Y_2, Z_2, T, B$ 与 A 模拟 Game_k 和 $\text{Game}_{\text{Final}}$, 此过程与引理 2 的证明过程相似, 此处不再赘述。

命题 2 在子群判定性问题中, 本文加密方案在标准模型的 $\text{Game}_{\text{Outside}}$ 抗适应性选择关键词攻击下是语义安全的。

命题 1 的证明过程同样适用于命题 2, 原因是本文加密方案的验证算法中 g^a 和 g^b 对称。命题 2 的引理分析与命题 1 类似。由以上命题证明可以得出, $\text{Game}_{\text{Final}}$ 与真实的安全性游戏 $\text{Game}_{\text{Real}}$ 不可区分。因此, 得到如下定理:

定理 1 在标准模型下, 若假设 1、假设 2 和假设 3 同时成立, 则本文加密方案具有 IND-SCF-CKA 安全性。

4 效率对比

将本文加密方案与一些经典 PEKS 方案在效率方面进行比较分析。令 $|G|, |G_T|, |\mathbb{Z}_p|$ 分别表示 G, G_T, \mathbb{Z}_p 中元素的大小, n_p, n_e, n_o 分别表示双线性对运算、指数运算和其他运算, SCF 和 S-M 分别表示非安全信道和标准模型。各数据检索方案的陷门、密文大小、验证复杂度以及可证明安全模型等信息对比如表 1 所示。其中, yes 表示该模型为可证明安全模型, no 反之。表 1 可以看出, 相对于素数阶的可搜索加密方案, 在合数阶双线性群下, 本文方案有较短的陷门和 PEKS 密文长度, 且其验证算法只需 2 次双线性配对运算, 因此, 该方案具有更高的计算效率与安全性。

表 1 各数据检索方案的性能对比结果

方案	陷门尺寸	密文大小	验证复杂度	可证明安全模型	
				SCF	S-M
文献[1]方案	$ G $	$ G + \mathbb{Z}_q $	$n_p + n_o$	no	no
文献[17]方案	$ G + \mathbb{Z}_q $	$3 G + 2 G_T $	$4n_p + 3n_e + n_o$	yes	yes
文献[18]方案	$2 G $	$4 G + G_T $	$4n_p + 3n_e + n_o$	yes	yes
本文方案	$2 G $	$2 G + G_T $	$2n_p$	yes	yes

5 结束语

本文提出一种非安全信道下的双系统可搜索加密方案, 以进行数据的安全存储。分析结果表明, 该

方案在静态假设的标准模型下可抵抗非安全信道上的选择关键词攻击, 其计算效率与安全性高于经典 PEKS 方案。下一步将构造更有效的多关键词, 并探究能够抵抗关键词猜测攻击的加密方案。

参考文献

- [1] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search [EB/OL]. [2018-06-25]. <http://crypto.stanford.edu/~dabo/papers/encsearch.pdf>.
- [2] WATERS B R, BALFANZ D, DURFEE G, et al. Building an encrypted and searchable audit log [EB/OL]. [2018-06-25]. http://www.cs.utexas.edu/users/bwaters/publications/papers/audit_log.pdf.
- [3] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable symmetric encryption: improved definitions and efficient constructions [C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2006: 79-88.
- [4] GU Chunxiang, ZHU Yuefei, PAN Heng. Efficient public key encryption with keyword search schemes from pairings [EB/OL]. [2018-06-25]. <https://eprint.iacr.org/2006/108.pdf>.
- [5] TANG Qiang, CHEN Liqun. Public-key encryption with registered keyword search [C]//Proceedings of European Conference on Public Key Infrastructures. Berlin, Germany: Springer, 2009: 163-178.
- [6] LEWKO A. Tools for simulating features of composite order bilinear groups in the prime order setting [C]//Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2012: 318-335.
- [7] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption [C]//Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2010: 62-91.
- [8] FANG Liming, SUSILO W, GE Chunpeng, et al. Public key encryption with keyword search secure against keyword guessing attacks without random oracle [J]. Information Sciences, 2013, 238: 221-241.
- [9] LIU Chang, ZHU Liehuang, WANG Mingzhong, et al. Search pattern leakage in searchable encryption: attacks and new construction [J]. Information Sciences, 2014, 265: 176-188.
- [10] WANG Xiaofen, WU Yi, CHEN Rongmao, et al. Secure channel free id-based searchable encryption for peer-to-peer group [J]. Journal of Computer Science and Technology, 2016, 31(5): 1012-1027.
- [11] ZHOU Yousheng, XU Guangxia, WANG Yong, et al. Chaotic map-based time-aware multi-keyword search scheme with designated server [J]. Wireless Communications and Mobile Computing, 2016, 16(13): 1851-1858.
- [12] 徐磊, 许春根, 蔚晓玲. 云存储上高效安全的数据检索方案 [J]. 密码学报, 2016, 3(4): 330-339.
- [13] HUANG Qiong, LI Hongbo. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks [J]. Information Sciences, 2017, 403/404: 1-14.
- [14] 刘鹏亮, 郑龙辉, 白翠翠, 等. 一种可验证的公钥可搜索加密方案 [J]. 计算机工程, 2014, 40(11): 118-120.
- [15] 林楠, 费益军, 王宇飞, 等. 云环境下一种排序非对称的可搜索加密方案 [J]. 计算机工程, 2015, 41(11): 190-193.
- [16] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions [C]//Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology. Berlin, Germany: Springer, 2009: 619-636.
- [17] FANG Liming, SUSILO W, GE Chunpeng, et al. A secure channel free public key encryption with keyword search scheme without random oracle [C]//Proceedings of the 8th International Conference on Cryptology and Network Security. Berlin, Germany: Springer, 2009: 248-258.
- [18] CHEN Zhenhua, WU Chunying, WANG Daoshun, et al. Conjunctive keywords searchable encryption with efficient pairing, constant ciphertext and short trapdoor [C]//Proceedings of Pacific-Asia Workshop on Intelligence and Security Informatics. Berlin, Germany: Springer, 2012: 176-189.

编辑 吴云芳