

一种改进的非对称可搜索加密方案

伍 琦

(江西财经大学 信息管理学院, 南昌 330032)

摘 要: 云服务器端在缓解用户本地存储压力的同时, 也存在对数据进行窃听的隐患, 用户往往选择把数据的密文形式上传到云服务器端。然而, 经典的数据加解密算法均未提供搜索功能, 影响用户的使用效率。为此, 提出一种非对称可搜索加密方案。该方案针对任何人均可生成陷门、密文可随意篡改、密钥对由用户各自生成、对身份进行加密、S 形同虚设等 5 个漏洞作改进。分析结果表明, 该方案在沿用原方案类似框架的基础上, 解决了原方案中的上述 5 个漏洞, 使通信双方的信息语义得到保障。

关键词: 云服务器; 可搜索加密; 非对称可搜索加密; 密钥对; 陷门

中文引用格式: 伍 琦. 一种改进的非对称可搜索加密方案[J]. 计算机工程, 2016, 42(8): 123-125, 133.

英文引用格式: Wu Qi. An Improved Asymmetric Searchable Encryption Scheme [J]. Computer Engineering, 2016, 42(8): 123-125, 133.

An Improved Asymmetric Searchable Encryption Scheme

WU Qi

(School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330032, China)

【Abstract】 While relieving the stress of local storage for users, cloud servers can eavesdrop on the stored data. Thus, users usually choose to upload data in the encrypted form to cloud servers. However, no classic encryption and decryption algorithm provides the ability of searching, which dramatically affects the use efficiency for users. Therefore, an asymmetric searchable encryption scheme is designed. It aims at fixing five flaws, including “trapdoor can be generated by anyone”, “ciphertext can be tampered with at will”, “key pairs are generated by users”, “encrypt identities”, and “S is of no use”. Analysis results show that the proposed scheme perfectly resolves the aforementioned five flaws in the previous scheme while maintaining its framework. The semantic information between communication sides is guaranteed.

【Key words】 cloud server; searchable encryption; asymmetric searchable encryption; key pair; trapdoor

DOI: 10.3969/j.issn.1000-3428.2016.08.023

1 概述

近年来, 随着数据量的日益增大, 越来越多的用户选择将所拥有的数据存放在云服务器端, 以缓解本地存储压力。与以往的客户机/服务器 (Client/Server, C/S) 模式不同, 人们往往认为云服务器是半可信的, 即它有可能对用户数据进行窃听, 因此, 需要对数据先进行加密再执行上传操作。然而, 传统的数据加解密算法, 如高级加密标准 (Advanced Encryption Standard, AES)、RSA、数据加密标准 (Data Encryption Standard, DES) 等, 均不支持搜索。当数据量浩大时, 不管从存储空间来看, 还是从带宽来看, 要求云用户将他/她的所有密文数据取回本

地, 再解密并提取其中所需部分是不可行的。因此, 设计可搜索密文数据的方案势在必行。文献[1]首创搜索控制、可证机密性、查询隔离、查询隐藏等安全性质, 并构造相应的可搜索加密方案。此后, 可搜索加密引起了学术界的普遍兴趣。根据索引生成和查询请求是否采用相同的密钥, 可搜索加密可细分为对称可搜索加密和非对称可搜索加密^[2]。此处, 笔者仅详细讨论后者。

文献[3]以邮件系统为例, 构造关键词搜索公钥加密 (Public Key Encryption with Keyword Search, PEKS) 模型, 基于双线性 Diffie-Hellman (Bilinear Diffie-Hellman, BDH) 假设和陷门排列分别设计了一个方案, 最后附带提出了采用 Jacobi 符

基金项目: 国家自然科学基金资助项目 (61462033)。

作者简介: 伍 琦 (1984 -), 男, 讲师、博士, 主研方向为信息安全。

收稿日期: 2015-06-11 **修回日期:** 2015-09-24 **E-mail:** wuqiocjzd@126.com

号的构建。文献[4]细致地分析了 PEKS 的一致性,证明了文献[3]方案是计算一致的,随后构造了一个统计一致的新方案,最后指出将匿名基于身份的加密(Identity Based Encryption, IBE)方案转为安全 PEKS 方案的方法。文献[5]基于 K-容忍 IBE 构造了一个 PEKS 方案,在标准模型下达到了 IND-CKA 安全。文献[6]基于 QIP 提出了一个 PEKS 方案。文献[7]构造关键词连结搜索公钥加密模型(PECK),随后基于 DLDH 假设设计方案。与前人方案比较得到,新方案的密文和私钥最节约空间。最后,将模型和方案扩展到多用户情况下。文献[8]针对文献[3]中遗留的“刷新关键词”、“移除安全信道”、“处理多关键词”等 3 个问题提出了改进方案。文献[9]指出文献[8]过于限制攻击者的能力,并为此构造强化安全模型及其下的改进方案。文献[10]提出陷门不可区分的 PEKS。文献[11]针对文献[5]中缺失的计算一致性提出一个变体,大大提高了效率。文献[12]基于大整数因子分解提出了一个 PEKS 方案。文献[13]针对移动云存储下群组成员变动频繁这一特点,设计了一个具有数据共享和密文修改功能的 PEKS 方案。文献[14]针对医疗领域常见的“单发多收”场景设计了一个 PEKS 方案,解决了前人方案中存在的密文过长问题。

文献[15]针对非对称可搜索加密领域缺失的搜索结果验证功能,利用 Elgamal 算法实现 PEKS 方案。经研究分析,该方案存在一系列安全漏洞。为此,本文针对这些漏洞进行修正,从而得到改进方案。

2 可验证的公钥可搜索加密方案

文献[15]方案包括 5 个算法,即参数生成、密文关键词及加密文件生成、陷门生成、检测、验证。简述如下所示。

(1) 参数生成算法

Alice 选大质数 p_1 及 $Z_{p_1}^*$ 中的生成元 g_1 ; 选随机整数 $x_1 (0 \leq x_1 \leq p-2)$, 计算 $y_1 = g_1^{x_1}$, 令 Alice 公钥为 (p_1, g_1, y_1) , 私钥为 x_1 。选取 g_2 和 g 分别为 $Z_{p_2}^*$ 和 Z_p^* 的生成元, Bob 公钥为 (p_2, g_2, y_2) , 私钥为 x_2 ; 服务器公钥为 (p, g, y) , 私钥为 x 。选哈希函数 $H: \{0, 1\}^* \rightarrow Z_p^*$, 确定加密及签名算法均为 Elgamal。

(2) 密文文件生成算法

假设 Alice 要发送给 Bob 含关键词 W 的文件 M 。Alice 求 $H(W)$, 选 $r_1, r_2 \in_R Z_p^*$, 计算 $S_1 = r_1^{H(W)} \bmod p$, $S_2 = r_1^{H(W)-1} r_2 \bmod p$, 令 $S = \langle S_1, S_2 \rangle$ 。

Alice 用 Bob 的公钥对 M 进行加密, 得密文 $C_1 = \langle y_{11}, y_{12} \rangle$ 。

Alice 用 x_1 对 $H(W)$ 进行签名, 得 $sig = \langle H(W), r, s \rangle$ 。

Alice 用 Bob 的公钥对自己的身份 ID_A 进行加密, 得到密文 $C_2 = \langle y_{21}, y_{22} \rangle$ 。

Alice 把 $S = \langle S_1, S_2 \rangle$ 和 $D = \langle C_1, sig, C_2 \rangle$ 上传至服务器。

(3) 陷门产生算法

当 Bob 要查询含关键词 W_1 的文件时, 他求出 $H(W_1)$, 再用服务器的公钥对其进行加密, 得到 $T_w = \langle y_{31}, y_{32} \rangle$ 。Bob 将 T_w 发给服务器。

(4) 检测算法

服务器收到 T_w 后, 将其加密以得到 $H(W_1)$ 。随后, 逐条检验各 $S = \langle S_1, S_2 \rangle$, 若满足 $S_1 = S_2^{H(W_1)}$, 则将相应的 $D = \langle C_1, sig, C_2 \rangle$ 发给 Bob。

(5) 验证算法

在 Bob 收到 D 后, 首先对 C_2 进行解密, 得到发送方身份, 然后用发送方的公钥对 sig 进行验证。若验证成功再对 C_1 进行解密; 否则, 丢弃。

经分析, 该方案存在以下漏洞:

(1) 任何人均可生成陷门。由上文可见, 陷门生成算法中仅用到了 $H(\cdot)$ 和服务器的公钥, 而此两者是任一通信方均掌握的信息, 即任意通信方可生成陷门。通常来说, 无论是对称可搜索加密还是非对称可搜索加密, 陷门的生成均应为搜索请求方的特有权利, 否则任意通信者均可发起搜索, 将大大增加服务器端的负担。故陷门生成算法应该用到搜索请求方的私钥。

(2) 攻击者可将密文文件生成算法中的 C_1 替换为任一异于 M 的文件 M' 的密文, 而不被发现。例如, 可将 $C_1 = \langle y_{11}, y_{12} \rangle$ 替换为 $C'_1 = \langle y'_{11}, y'_{12} \rangle$, 其中, C'_1 是用 Bob 的公钥对异于 M 的某文件 M' 的加密结果。这样一来, 可轻易造成 Alice 和 Bob 之间的通信歧义, 达到扰乱效果。为此, 须提供保障 C_1 不被篡改的机制, 如散列、数字签名等。

(3) 密钥对由用户各自生成。通常来说, 用户的安全知识和计算能力均十分有限, 故所生成密钥有可能存在各种各样的安全隐患, 如随机性不强、长度过短、具有明显的语义特征等。因此, 密码学方案中通常由专门的密钥生成中心来执行密钥或密钥对生成工作。另外, 该协议通信各方运算处在不同的域中, 为协议实施增加了不必要的负担。通常密码学方案中, 所有运算处在统一的某个域中即可。

(4) 对身份进行加密。一般来说, 通信各方身份均公开, 而且对于具有监控整个网络能力的攻击者来说, 各通信报文的收发方是可完全掌握的信息, 因此, 不值得对身份进行加密。

(5) S 形同虚设。在检测算法中, 服务器解密出

$H(w_1)$ 后,无需判断 $S_1 = S_2^{H(w_1)}$,只需与 sig 中的 $H(W)$ 作比对即可。若 $H(w_1) = H(W)$,则把相应的 D 发给 Bob。

3 改进方案设计

新方案同样包括5个算法,具体如下所示。

(1) 参数生成算法

KG (Key Generator) 选取大质数 p 及 Z_p^* (以下操作如无说明,均在 Z_p^* 下) 中的生成元 g , 选散列函数 $H: \{0,1\}^* \rightarrow Z_p^*$ 。KG 分别为 Alice, Bob 和服务 器生成密钥对 $(sk_A, pk_A = g^{sk_A})$, $(sk_B, pk_B = g^{sk_B})$, $(sk_C, pk_C = g^{sk_C})$ 。KG 规定加密及签名算法均为 Elgamal。

(2) 文件发送算法

Alice 求 $H(W)$, 计算 $S = pk_B \cdot g^{H(W)}$ 。

Alice 求 $C = Enc_{pk_B}(M) = \langle y_1, y_2 \rangle$ 。

Alice 求 $sig = Sig_{sk_A}(H(M)) = \langle H(M), r, s \rangle$ 。

Alice 把 S 和 $\langle C, sig, ID_A \rangle$ 发给服务器。

(3) 陷门生成算法

Bob 把 $s = sk_B + H(W_1)$ 发给服务器。

(4) 文件搜索算法

服务器求 $S' = g^s$, 逐条比对各 S 与 S' , 把所有 $S = S'$ 处的 $\langle C, sig, ID_A \rangle$ 发给 Bob。

(5) 验证算法

Bob 取 ID_A 对应的公钥 pk_A , 并用其验证 sig , 若 验证成功, 用 sk_B 对 C 进行解密, 得到 M' 。Bob 求 $H(M')$, 若 $H(M') \neq H(M)$, 则丢弃。

4 改进方案分析

显然, 新方案完全弥补了前文所述的5个漏洞, 具体如下所示。

(1) 只有搜索请求方才能生成陷门。由陷门生 成算法中可见, 须用到 Bob 的私钥 sk_B , 这一信息只 有 Bob 本人才拥有, 因此, 只有搜索请求方才具备生 成陷门的能力。

(2) 攻击者无法将 C 替换为某一异于 M 的文件 M' 的密文, 而不被发现。倘若攻击者将 C 替换为 $C' = Enc_{pk_B}(M') = \langle y'_1, y'_2 \rangle$, 下面分2种情况讨论:

1) 若攻击者此时将 sig 中的第一元素替换为 $H(M')$, 由于攻击者未掌握 Alice 的私钥 sk_A , 鉴于 Elgamal 签名的不可伪造性, 攻击者无法将 sig 中的 第二元素和第三元素替换为 Alice 对 $H(M')$ 的合法 签名 r', s' , 因此 Bob 执行验证算法时, 用 Alice 的公 钥 pk_A 验证 sig 必失败, Bob 丢弃。

2) 若攻击者不对 sig 作任何改动, 则 Bob 执行 验证算法时, 验证 sig 会成功。接着用 sk_B 对 C' 进行 解密, 得到 M' 。由于 $H(\cdot)$ 的碰撞抵抗性, $H(M')$

$= H(M)$ 的概率可忽略, Bob 丢弃。

综上, 攻击者此时无法造成 Alice 和 Bob 之间的 通信歧义, 通信双方的信息语义得到保障。

(3) 所有密钥对均由 KG 生成, 确保了安全性。所 有运算均处在统一的域 Z_p^* 下, 避免了不必要的负担。

(4) 去除了对身份的加密。报文中所有通信者 身份均以明文传输, 避免了加密开销。

(5) 新方案所有组成部分均有明晰的用途, 无任 一形同虚设的部件。

5 结束语

本文针对文献[15]方案存在的5个漏洞进行改 进, 提出一种改进的非对称可搜索加密方案。分析 结果表明, 该方案能弥补原方案的缺陷, 具有较好的 实用价值。今后拟在更复杂的应用背景下设计可搜 索加密算法, 研究如群组动态变化、单发多收、服务 器完全不可信等问题。

参考文献

- [1] Song X D, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data [C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2000: 44-55.
- [2] 方黎明. 带关键字搜索公钥加密的研究 [D]. 南京: 南京航空航天大学, 2012.
- [3] Boneh D, Crescenzo G, Ostrovsky R, et al. Public Key Encryption with Keyword Search [C]//Proceedings of the 23rd Annual Eurocrypt Conference. Interlaken, Switzerland: IACR, 2004: 506-522.
- [4] Abdalla M, Bellare M, Catalano D, et al. Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions [J]. Journal of Cryptology, 2008, 21(3): 350-391.
- [5] Khader D. Public Key Encryption with Keyword Search Based on K-resilient IBE [C]//Proceedings of International Conference on Computational Science and Its Applications. Berlin, Germany: Springer-Verlag, 2006: 298-308.
- [6] Crescenzo G D, Saraswat V. Public Key Encryption with Searchable Keywords Based on Jacobi Symbols [C]//Proceedings of the 8th International Conference on Cryptology in India. Berlin, Germany: Springer-Verlag, 2007: 282-296.
- [7] Hwang Y H, Lee P J. Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System [C]//Proceedings of the 1st International Conference on Pairing-based Cryptography. Berlin, Germany: Springer-Verlag, 2007: 2-22.
- [8] Baek J, Safavi-Naini R, Susilo W. Public Key Encryption with Keyword Search Revisited [C]//Proceedings of International Conference on Computational Science and Its Applications. Berlin, Germany: Springer-Verlag, 2008: 1249-1259.

(下转第133页)

参考文献

- [1] Birney E, Stamatoyannopoulos J A, Dutta A, et al. Identification and ANALYSIS of Functional Elements in 1% of the Human Genome by the ENCODE Pilot Project[J]. *Nature*, 2007, 447(7146): 799-816.
- [2] Girvan M, Newman M E J. Community Structure in Social and Biological Networks[J]. *Proceedings of the National Academy of Sciences*, 2002, 99(12): 7821-7826.
- [3] Ino H, Kudo M, Nakamura A. Partitioning of Web Graphs by Community Topology[C]//*Proceedings of the 14th International Conference on World Wide Web*. New York, USA: ACM Press, 2005: 661-669.
- [4] Wilkinson D M, Huberman B A. A Method for Finding Communities of Related Genes[J]. *Proceedings of the National Academy of Sciences*, 2004, 101(suppl. 1): 5241-5248.
- [5] Radicchi F, Castellano C, Cecconi F, et al. Defining and Identifying Communities in Networks[J]. *Proceedings of the National Academy of Sciences of the United States of America*, 2003, 101(9): 2658-2663.
- [6] 杨 博, 刘大有, Liu Jiming, 等. 复杂网络聚类方法[J]. *软件学报*, 2009, 20(1): 54-66.
- [7] 汪小帆, 李 翔, 陈关荣. 复杂网络理论及其应用[M]. 北京: 清华大学出版社, 2006.
- [8] Kernighan B W, Lin S. An Efficient Heuristic Procedure for Partitioning Graphs[J]. *Bell System Technical Journal*, 1970, 49(2): 291-307.
- [9] Newman M E J. Fast Algorithm for Detecting Community Structure in Networks[J]. *Physical Review E*, 2004, 69(6): 133-138.
- [10] Wu F, Huberman B A. Finding Communities in Linear Time: A Physics Approach[J]. *The European Physical Journal B-Condensed Matter and Complex Systems*, 2004, 38(2): 331-338.
- [11] Zimmermann H J. Fuzzy Set Theory and Its Applications[M]. Berlin, Germany: Springer, 2001.
- [12] Ertöz L, Steinbach M, Kumar V. Finding Clusters of Different Sizes, Shapes, and Densities in Noisy, High Dimensional Data[C]//*Proceedings of the 3rd SIAM International Conference on Data Mining*. San Francisco, USA: [s. n.], 2003: 47-58.
- [13] 马 军, 邵 陆. 模糊聚类计算的最佳算法[J]. *软件学报*, 2001, 12(4): 578-581.
- [14] Danon L, Diaz-Guilera A, Duch J, et al. Comparing Community Structure Identification[J]. *Journal of Statistical Mechanics: Theory and Experiment*, 2005, 2005(9): 9008-9017.
- [15] 李晓佳, 张 鹏, 狄增如, 等. 复杂网络中的社团结构[J]. *复杂系统与复杂性科学*, 2008, 5(3): 19-42.
- [16] Cafieri S, Hansen P, Liberti L. Locally Optimal Heuristic for Modularity Maximization of Networks[J]. *Physical Review E*, 2011, 83(5): 56105-56113.
- [17] Clauset A, Newman M E J, Moore C. Finding Community Structure in Very Large Networks[J]. *Physical Review E*, 2004, 70(6): 066111.
- [18] Chao Yuan, Chai Yi. Group Similarity Based Algorithm for Network Community Structure Detection[J]. *Acta Physica Sinica*, 2012, 61(21): 514-518.
- [19] Lou Hao, Li Shenghong, Zhao Yuxin. Detecting Community Structure Using Label Propagation with Weighted Coherent Neighborhood Propinquity[J]. *Physica A: Statistical Mechanics and Its Applications*, 2013, 392(14): 3095-3105.
- [20] Lusseau D. The Emergent Properties of a Dolphin Social Network[J]. *Proceeding of the Royal Society of London, Series B: Biological Sciences*, 2003, 270(S2): 186-188.
- [21] Newman M E J, Girvan M. Finding and Evaluating Community Structure in Networks[J]. *Physical Review E*, 2004, 69(2): 026113.
- [22] 何东晓, 周 栩, 王 佐, 等. 复杂网络社区挖掘——基于聚类融合的遗传算法[J]. *自动化学报*, 2010, 36(8): 1160-1170.
- [23] Newman M E J. Modularity and Community Structure in Networks[J]. *Proceedings of the National Academy of Sciences*, 2006, 103(23): 8577-8582.
- 编辑 刘 冰
- ~~~~~
- (上接第125页)
- [9] Rhee H S, Park J H, Susilo W, et al. Improved Searchable Public Key Encryption with Designated Tester[C]//*Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*. New York, USA: ACM Press, 2009: 376-379.
- [10] Zhao Yuanjie, Chen Xiaofeng, Ma Hua, et al. A New Trapdoor-indistinguishable Public Key Encryption with Keyword Search[J]. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2012, 3(1/2): 72-81.
- [11] Yang Haomiao, Xu Chunxiang, Zhao Hongtian. An Efficient Public Key Encryption with Keyword Scheme not Using Pairing[C]//*Proceedings of the 1st International Conference on Instrumentation, Measurement, Computer, Communication and Control*. Washington D. C., USA: IEEE Press, 2011: 900-904.
- [12] Luo Wenjun, Tan Jianming. Public Key Encryption with Keyword Search Based on Factoring[C]//*Proceedings of the 2nd International Conference on Cloud Computing and Intelligent Systems*. Washington D. C., USA: IEEE Press, 2012: 1245-1247.
- [13] Xia Qi, Ni Jianbing, Kanpogninge A, et al. Searchable Public-key Encryption with Data Sharing in Dynamic Groups for Mobile Cloud Storage[J]. *Journal of Universal Computer Science*, 2015, 21(3): 440-453.
- [14] Shao Zhiyi, Yang Bo, Zhang Wenzheng, et al. Secure Medical Information Sharing in Cloud Computing[J]. *Technology and Health Care*, 2015, 23(s1): 133-137.
- [15] 刘鹏亮, 俎龙辉, 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.
- 编辑 刘 冰