华 东 师 范 大 学

专业学位研究生学位论文开题报告

论 文 题 目 前向安全的可验证多关键字搜索加密

姓　　名 常力凡

学　　号 71184501013

专 业 领 域 密码与网络安全

系　　所 密码与网络安全系

导师姓名、职称 周俊(副教授)

完 成 时 间 2020 年 6 月 20 日

一、立论依据

一、课题来源及意义

数据所有者包括个人和组织，在将数据(例如文本、图像、视频等)外包给远程云服务的过程中，希望对数据进行加密，确保数据机密性。虽然在外包数据之前对其进行加密有很多好处，但是搜索加密的数据(或者数据集)是一个很困难的事情。可加密搜索(SE)允许用户关键字搜索密文，有选择地检索感兴趣的文件。SE方案的例子包括使用关键字搜索的公钥加密，分为基于证书的关键字搜索方案和基于属性的关键字搜索方案。这两种方案都有一定的限制，在基于证书的关键字搜索方案中，数据所有者通过使用特定数据的公钥对其数据进行加密，从而共享其数据。密钥限制是证书管理，因为需要通过证书管理系统来验证证书和公钥。基于身份(或属性)的关键字搜索方案的限制是密钥托管，因为受信任的中心可以解密系统中的任何密文。
同时数据所有者搜索一个存储在不受信任的服务器上面的加密的数据库，他们希望保持查询的隐私和数据的隐私。因此论文中引入了前向安全性，前向安全能够保护过去进行的搜索不受密钥在未来暴露的威胁。如果系统具有前向安全性，就可以保证在主密钥泄露时历史通讯的安全，即使系统遭到主动攻击也是安全的。数据所有者在查询的过程中可能会泄露一些关于更新关键字的信息，会受到破坏性的自适应攻击，破坏查询的隐私。阻止这种攻击的唯一方法是设计前向的私有方案，如果新插入的元素与以前的搜索查询匹配，则该方案的更新过程不会泄漏。slam 等[1]和 Cash 等[2]研究了可搜索加密方案泄漏的现实后果，并表明即使是很小的泄漏也可以被被动攻击者利用来揭示客户端的查询，从而导致泄漏滥用攻击。对于较大的泄漏，[2]的作者表明加密数据库的完全纯文本恢复是可能的。张等人在[19]提出了，基于身份的可验证加密签名协议的安全性分析。
为了同时实现上述搜索功能，本文前向安全的可验证多关键字加密搜索功能。它允许利用现有的公共审计技术(如[33,34]中介绍的技术)，在加密数据方案上执行搜索。也就是说，一个特定的数据用户可以通过表示索引结构和无证书签名来进行多关键词搜索，验证搜索结果的正确性。它既有前向私有结构的安全性保证，又可以通过表示索引结构和无证书签名来进行多关键词搜索。

二、国内外研究现状

现在国内外已经有大量关于可加密搜索的研究，一些文献中提出了不同类型的可加密搜索方案(如单关键字搜索[7]、多关键字搜索[5,6]和可验证的关键字搜索[9,11])证明了这一点。传统的可加密搜索方案只支持精确的关键字搜索，这限制了系统的可用性，影响用户的搜索体验。因此，Li 等人[8]提出了一个模糊关键字搜索方案，利用编辑距离来处理微小的错误和格式不一致。然而，在实践中，可加密搜索方案还应该支持多关键字(连接词关键字或非连接词关键字)搜索，进一步缩小搜索范围，单个关键字搜索往往产生许多不相关的搜索结果[3,14,15]。一些云服务提供商可能出于成本的原因故意返回错误的搜索结果，比如最小化成本。因此，用户应该使用一些数据验证解决方案来确保搜索结果的正确性[4,10]。Sun 等人[11]提出了一种高效的基于树的索引结构，可以对返回的搜索结果进行

真实性检查。魏等人在[20]提出了支持数据去重的可验证模糊多关键词搜索方案。

Stefanov 等人在[16]中首次明确考虑了前向隐私。作者在他们的论文中建立了一个动态的、次线性的方案来实现前向隐私。王等人在[18]提出了前向安全的多重数字签名方案。实践中，许多实现者往往会拒绝提供前向安全；或者虽然提供前向安全，但安全系数极差。黑泽明和他的团队已经研究了可验证的 SSE 方案(即针对活跃对手的安全方案)Ohtaki [17]，以及 Bost 等人[16]最近提出的高效和动态结构，包括一个来自[16]的前向私有结构。

到目前为止，还没有一个可加密多关键字搜索架构能够同时满足阻止这些漏洞滥用攻击的安全需求，并实现最优的更新效率。因此本文提出了一种前向安全的可验证多关键字可搜索加密方案，既具有前向私有结构的安全性保证，同时实现搜索结果验证、多关键字搜索。

三、主要参考文献

[1] Islam, M.S., Kuzu, M., and Kantarcioglu, M. Access pattern disclosure on searchable encryption:Ramification, attack and mitigation. In: NDSS 2012. The Internet Society (Feb. 2012).

[2] Cash, D., Grubbs, P., Perry, J., and Ristenpart, T. Leakage-abuse attacks against searchable encryption. In: I. Ray, N. Li, and C. Kruegel: (eds.), ACM CCS 15, pp. 668–679. ACM Press(Oct. 2015).

[3] R. Chen, Y. Mu, G. Yang, F. Guo, X. Wang, A new general framework for secure public key encryption with keyword search, in: Proc. Australasian Conference on Information Security and Privacy (ACISP’15), vol. 9144, 2015, pp. 59–76, doi: 10.1007/978- 3- 319- 19962- 7 _ 4 .

[4] B. Kang, J. Wang, D. Shao, Certificateless public auditing with privacy preserving for cloud-assisted wireless body area networks, Mobile Inf. Syst. 2017 (2017), doi: 10.1155/2017/2925465 .

[5] H. Li, D. Liu, Y. Dai, T.H. Luan, X.S. Shen, Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage, IEEE Trans. Emerg. Top. Comput. 3 (1) (2015) 127–138, doi: 10.1109/TETC.2014.2371239 .

[6] H. Li, Y. Yang, T.H. Luan, X. Liang, L. Zhou, X.S. Shen, Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data, IEEE Trans. Dependable Secure Comput. 13 (3) (2016) 312–325, doi: 10.1109/TDSC.2015.2406704 .

[7] J. Li, Y. Shi, Y. Zhang, Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage, Int. J. Commun. Syst. 30 (1) (2017), doi: 10.1002/dac.2942 .

[8] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, W. Lou, Fuzzy keyword search over encrypted data in cloud computing, in: Proc. IEEE Conference on Computer Communications (INFOCOM’10), 2010, pp. 1–5, doi: 10.1109/INFCOM.2010.5462196 .

[9] Y. Miao, J. Ma, X. Liu, Q. Jiang, J. Zhang, L. Shen, Z. Liu, Vcksm: verifiable conjunctive keyword search over mobile e-health cloud in shared multi-owner settings, Pervasive Mob. Comput. 40 (2017) 205–219, doi: 10.1016/j.pmcj.2017.06.016 .

[10] J. Shen, J. Shen, X. Chen, X. Huang, W. Susilo, An efficient public auditing protocol with novel dynamic structure for cloud data, IEEE Trans. Inf. Forensics Secur. 12 (10) (2017) 2402–2415, doi: 10.1109/TIFS.2017.2705620 .
[11] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y.T. Hou, H. Li, Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking, IEEE Trans. Parallel Distrib. Syst. 25 (11) (2014) 3025–3035, doi: 10.1109/TPDS.2013.282.
[12] B. Wang, B. Li, H. Li, F. Li, Certificateless public auditing for data integrity in the cloud, in: Proc. IEEE Conference on Communications and Network Security (CNS’13), 2013, pp. 136–144, doi: 10.1109/CNS.2013.6682701 .
[13] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: Proc. IEEE Conference on Computer Communications (INFOCOM’10), 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5462173 .
[14] X.-F. Wang, Y. Mu, R. Chen, X.-S. Zhang, Secure channel free id-based searchable encryption for peer-to-peer group, J. Comput. Sci. Technol. 31 (5) (2016) 1012–1027, doi: 10.1007/s11390-016-1676-9 .
[15] Y. Yang, M. Ma, Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds, IEEE Trans. Inf. Forensics Secur. 11 (4) (2016) 746–759, doi: 10.1109/TIFS.2015.2509912 .
[16] Stefanov, E., Papamanthou, C., and Shi, E. Practical dynamic searchable encryption with small leakage. In: NDSS 2014. The Internet Society (Feb. 2014).
[16] Bost, R., Fouque, P.A., and Pointcheval, D. Verifiable dynamic symmetric searchable encryption: Optimality and forward security. Cryptology ePrint Archive, Report 2016/062 (2016). http://eprint.iacr.org/2016/062.
[17] Kurosawa, K. and Ohtaki, Y. UC-secure searchable symmetric encryption. In: A.D. Keromytis (ed.), FC 2012, LNCS, vol. 7397, pp. 285–298. Springer, Heidelberg (Feb. / Mar. 2012).
[18] 王晓明, 符方伟, 张震. 前向安全的多重数字签名方案[J]. 计算机学报, 2004, 027(009):1177-1181.
[19] 张振峰. 基于身份的可验证加密签名协议的安全性分析[J]. 计算机学报, 2006(09):178-183.
[20] 魏国富, 葛新瑞, and 于佳. "支持数据去重的可验证模糊多关键词搜索方案." 密码学报 5(2019).[21] Q. Zheng, X. Li, A. Azgin, Clks: Certificateless keyword search on encrypted data, in: Proc. International Conference on Network and System Security (NSS‘15), 2015, pp. 239–253, doi: 10.1007/978-3-319-25645-0_16.
[22] Bost, R. (2016, October). Σοφος: Forward secure searchable encryption. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1143-1154).
[23] Miao, Y., Weng, J., Liu, X., Choo, K. K. R., Liu, Z., & Li, H. (2018). Enabling verifiable multiple keywords search over encrypted cloud data. Information Sciences, 465, 21-37.

二、研究方案

四、研究目标

我们的目标是实现一个更实用的支持结果验证和多关键字搜索的可加密搜索方案。我们首先构造一个前向安全加密搜索方案，它的搜索和更新协议在一次往返中执行。我们首先考虑只支持添加而不支持删除的方案。然后，我们将描述如何将此基本构造转换为支持添加和删除的可加密搜索构造，同时减少客户端存储，以及如何使其免受恶意对手的攻击。具体来说，本方案应该验证搜索结果的有效性，并允许用户提交一个搜索查询(多个关键字)并生成一个搜索令牌。

五、研究内容和拟解决的关键问题

1、多关键字搜索： 对于可验证的关键字搜索方案，有必要支持多关键字搜索，以最小化带宽资源和改善用户搜索体验(因为一个关键字搜索返回许多不相关的搜索结果)。本方案允许特定数据用户在不增加陷阱门尺寸和密文搜索大小的情况下，在单个搜索查询中发出多个关键字搜索，包括合取关键字搜索和析取关键字搜索，提高了用户的搜索体验。（合取关键字搜索意味着每个结果包含所有查询关键字，而析取关键字搜索意味着每个结果至少包含查询关键字。在本方案中，我们主要讨论了合取关键字的搜索。）

2、验证搜索结果： 这个方案允许通过在每个文件中附加一个签名来验证搜索结果的准确性。

3、前向安全的多关键字加密搜索： 本方案在保证前向隐私的同时，可支持多关键字可搜索加密，保证返回的结果准确并切完整，不会因为受到恶意攻击或者能够检验云服务提供商是否返回错误的搜索结果。

六、研究方法和手段

数据所有者在查询的过程中泄露一些关于关键字的信息，可能会受到破坏性的自适应攻击，破坏查询的隐私。阻止这种攻击的唯一方法是设计前向的私有方案，如果新插入的元素与以前的搜索查询匹配，则该方案的更新过程不会泄漏。从功能的角度来看，前向隐私是很重要的。前向私有方案允许在线构建加密的数据库。在大多数其他多关键字搜索结构中，必须首先执行索引步骤:设置阶段需要一个反向索引，其构造需要时间和空间。论文将演示所提议的方案的安全性(即，该方案实现了密文的不可分辨性和签名的不可伪造性)。

七、实验方案

首先构建一个系统，对系统初始化，然后生成秘钥和密文，添加防范恶意对手的保安措施，进行多关键字密文的检索，并且对返回的结果进行确认。

基于前向安全的多重数字签名方案[18]和[22]，论文的目标之一是实现即使签名人的签名密钥被攻击，以前所产生的多重数字签名依然是安全的。

基于无证书关键字搜索方案[21]，论文的另一个目标是实现一个更实用的支持结果验证和多关键字搜索的加密搜索方案。具体来说，本方案应该验证搜索结果的

有效性，并允许多关键字搜索。对于无证书的结果验证，本方案为每个文件附加一个签名，然后验证搜索结果的正确性。此外，该方案还需要避免证书管理和密钥托管。
基于在加密云数据上的多关键字搜索[23]，论文的综合目标是实现前向安全的可验证多关键字搜索加密。参考上述三种方案，首先构造一个前向安全关键字搜索方案，它的搜索和更新协议在一次往返中执行，但是以客户端上需要一些存储为代价。再考虑只支持添加而不支持删除的方案。然后，将描述如何将此基本构造转换为支持添加和删除的构造，同时减少客户端存储，以及如何使其免受恶意对手的攻击。

八、特色与创新

1. 本方案支持前向隐私；
2. 本方案对返回的搜索结果是可验证的，受到恶意攻击，检验云服务提供商是否返回错误的搜索结果；
3. 并且支持多关键字搜索，保证返回的结果准确并且完整。

三、论文大纲

前向安全的可验证多关键字搜索加密

四、论文工作计划

设定时间	拟完成任务
2020.04.10 ~ 2020.06.20	编写开题报告，阅读关于前向安全，搜索加密的相关论文
2020.06.21 ~ 2020.08.31	确定详细实验方案，收集相关的数据
2020.09.01 ~ 2020.12.31	构建可搜索加密的安全模型，进行实验和数据分析
2021.01.01 ~ 2021.02.28	实施与分析实验结果，与现有的安全模型进行比较
2021.03.01 ~ 2021.05.31	编写论文

五、评价和意见

1. 导师对本选题的评价 导师（签名）： 年　　月　　日
2.开题评审小组结论 开题评审小组成员（签名） 年　　月　　日

注：本表可复印，可另加附页，各单位也可根据自己的要求增加内容。