方计算协议,Keller 等人[38]首次设计了多种在多方计算中常用的数据结构,并利用不经意技术进行实现,其中包括数组、字典、优先队列等.利用文献[38]中的优先队列实现 Dijkstra 算法可以在 $O(|E|\log^5|E|+|V|\log^4|V|)$的时间内实现单源点最短路径的计算,并且可以保证源点与汇点的隐私性,其中,E 和 V 分别表示图中边和点的数量.同时,文献[38]还证明了利用提出的不经意数据结构对结合安全计算的 ORAM 进行块初始化(batch initialization),要比简单地按序初始化提升 $O(\log^3 N)$的数量级.

Wang 等人[39]在文献[38]的基础上一般化不经意数据结构的设计原则,将其归纳为两点:一种是基于指针(pointer)的技术,另一种是基于位置(locality)的技术.基于指针的技术通常用于树状 ORAM 构建中,通过父节点存储一个指向子节点的指针,可以在查找父节点到子节点的路径中直接获取子节点的位置,避免重复地查找映射表,这样可以降低 $O(\log n)$数量级的复杂度.基于位置的技术通常应用于有着二倍维度(doubling dimension)的访问模式图中.图中每一个点被划分至一个簇(cluster)中.每一个簇包含 $O(\log N)$个点,通过图中每一个点对其他簇的访问,可以追踪整个访问过程.每一个簇可以像 ORAM 的数据块一样被访问,这样,当需要读取或者更新点的信息时候,先将点所在的簇与其临近的所有簇读入缓冲区,对于其临近的簇执行虚假访问,目标点所在的簇执行真实访问,这样保证了访问的隐私性.

当 ORAM 直接用于密文数据库系统时,存在很大的局限性.Hoang 等人[70]对存在的局限性进行分析.

1) 对于面向行的数据库,在利用 ORAM 进行改进时,会将数据库中的每一行作为 ORAM 中的数据块,例如 SEAL-ORAM[71].但是这种方案在执行插入、删除或者更新时,需要移动 ORAM 中的所有数据块;同时,如果在数据库中执行类似统计或者条件查询等列相关操作时,需要下载 ORAM 中的所有数据块,这将导致很大的带宽问题;
2) 另一种方法是将数据库中的每一个数据单元作为 ORAM 中的数据块,但是这会增加映射表的大小.Hoang 等人[70]分析:可以利用文献[39]中的思想,将 $O(\log N)$个数据单元存入一个 ORAM 的数据块中来避免映射表的问题.但是这会增加按行或列查询所有数据单元的请求次数,不适用于大型数据库.

针对这两个局限性,Hoang 等人[70]提出了两种用于密文数据库系统的不经意数据结构:oblivious matrix structure(OMAT)与 oblivious tree structure(OTREE).前者为数据库中每一个表构造不经意的矩阵结构,可以支持多种查询操作而不需要下载整个 ORAM 数据库;后者为基于树的数据库实例提供不经意访问操作.对于不经意条件查询,利用文献[70]中的 OTREE 要比利用文献[39]中的方案更高效.

5.3 小 结

结合安全计算场景的 ORAM 与传统意义上客户端-服务器 ORAM 有较大的不同,具体总结为以下几点.

(1) 保护对象不同:在安全计算中,存储的数据由多方共享,任意一方的访问模式都不能泄露,而一般 ORAM 中,访问模式的保护只针对客户端,是单向的;
(2) 实现方式不同:在研究结合安全计算 ORAM 的协议设计时,需要考虑初始化过程的复杂度,这一部分往往是通过协议实现的.而一般意义上的 ORAM 数据库初始化是默认存在的;
(3) 优化策略不同:传统研究的 ORAM 主要针对客户端与服务器的带宽以及客户端本地的存储,而结合安全计算场景的 ORAM 更多地考虑计算的复杂度.

通过分析总结上述的研究工作,并结合以上与传统 ORAM 研究的不同,我们分析总结了结合安全计算 ORAM 协议目前的研究方向.

- 以优化协议性能为主要目标.与通用的 ORAM 性能优化一样,结合安全计算场景的 ORAM 也存在着复杂度太高的问题,但是优化角度不同.这里更倾向于降低 ORAM 在安全计算上的实现复杂度;
- 推广 ORAM 的使用以实现在更多场景下的安全计算.由于 ORAM 本身扎实的安全理论基础及其广泛的适用性,将 ORAM 迁移到其他安全领域实现多种类的安全计算也是研究热点之一,例如图计算、社交网络挖掘等.

6 不经意随机访问机研究展望

由于不经意随机访问机本身低效性的特点,导致其应用于实际的问题更加突出,例如设计安全存储系统与安全计算协议等.所以,这项技术目前的研究重点依然在于性能的提升.同时还有一个不容忽视的挑战就是不经意随机访问机应用于实际所产生的额外问题,例如在安全存储场景中的数据备份问题等.所以,未来不经意随机访问机研究需要兼顾性能、功能、应用等多方面的因素,具体表现为:

- 性能的进一步提升.不只局限于传统的讨论客户端与服务器之间的带宽以及客户端本地的存储问题,还会涉及进一步优化服务器的存储、交互轮数等其他之前很少考虑的指标.在结合安全存储场景下,也会着重考虑多用户并发访问下系统的响应时间;在安全计算场景下的计算复杂度等.因此,这一类性能优化问题将一直是 ORAM 研究的主流,这也推动 ORAM 本身不断的发展;
- 功能的进一步完善.未来的 ORAM 将会支持更多的操作,不只支持简单的读写访问,甚至可以在其上完成较为复杂的数据结构操作,例如,可以用读写进行组合实现查询删除等[27].其他场景下的功能也可以利用不经意数据结构实现(见第 5.2 节).因此,这一类方向将促进 ORAM 应用于实际;
- 实用型 ORAM 应用系统的出现.对于存储系统而言,将不仅仅像 ObliviStore[20]和 TaoStore[35]那样的原型系统,真正可以应用于存储海量数据,支持多用户并发访问以及快速响应的系统会逐步推出.同时,对于安全计算,也会出现基于 ORAM 的安全计算系统,或者是安全计算模块,可以兼容目前大多数分布式计算系统,例如 MapReduce,Spark 等.这使得云计算与大数据的技术与安全计算领域相结合.

我们认为,未来不经意随机访问机研究应该重点包含以下几个方面.

(1) 基于隐私信息检索技术的多指标性能优化的 ORAM 设计

隐私信息检索技术可以用来优化 ORAM 的平均带宽(见第 3.1.2 节)和客户端存储(见第 3.3.2 节),相比于一般的优化方案,隐私信息检索具有两种优点:(1) 可以同时解决通用 ORAM 性能提升中的两个重要指标,这是其他优化策略所不具有的;(2) 这种技术的缺陷很少,因此今年来受到广泛的关注.以隐私信息检索技术为出发点,在保证平均带宽和客户端存储最优的情况下优化别的性能指标将是未来性能提升的重点.从第 2 节的表 2 可以看出,如今在性能优化上平均带宽和客户端存储这两种性能已经达到最优的 $O(1)$.但是其他的指标依然存在相对的劣势,例如数据块的大小、交互轮数等.能否在保证前面两种性能依然是最优的基础上优化其他的性能指标,是一个非常重要的问题,继续以隐私信息检索技术为研究对象是未来的一种重要研究趋势.

(2) 不经意并行随机访问机(OPRAM)的设计与实现

OPRAM 最初是由 Boyle 等人提出[72],用来解决多主体对 ORAM 的并行访问问题.与第 4 节中多用户并发访问存储系统不同的是,OPRAM 是从模型层实现,不参考任何应用场景;而第 4 节是 ORAM 结合安全存储场景设计系统,需要添加一系列的模块才能从应用层实现.可以将 OPRAM 理解为支持多用户并发访问的 ORAM 在模型层的抽象,因此,OPRAM 将更适用于云平台以及多核处理器结构.针对 OPRAM 的设计依然以性能改进作为驱动力.其衡量指标与传统 ORAM 类似,主要是针对通信带宽以及客户端的存储.当 OPRAM 用于多核计算上时,也需要考虑计算复杂度的问题.因此,OPRAM 作为 ORAM 在并行性上的扩展,在保留 ORAM 所有的能力之外,也针对一些特殊的应用场景添加额外的功能.这一类设计将 ORAM 推向更广的应用,也是未来 ORAM 研究的重要途径之一.

(3) 基于 ORAM 的安全计算系统的设计与实现

结合 ORAM 的安全计算(见第 5 节)依然以优化计算协议的复杂度作为目前的主流工作.相比于安全多方计算,这一类工作在保证计算协议的安全性上还保证了每一个计算方访问数据的隐私性.之前已经有一些工作实现了基于安全多方计算的安全计算系统,例如基于电路技术的安全两方计算系统 FairPlay[73]、多方计算系统 FairPlayMP[74]、基于秘密共享技术的多方计算系统 Sharemind[75]等.但是目前,结合 ORAM 的安全计算依然只停留于协议的设计,还没有出现基于 ORAM 的安全计算系统.因此,未来的一个重要研究方向是将结合 ORAM 的安全计算应用于实际,设计出实用型的系统.

同时,针对已有计算系统的改进也是未来的一种研究方向.例如设计实现基于 MapReduce,Spark 的安全计

算模块,其上使用 ORAM 来保护计算节点对文件系统或者是内存单元的读写访问.也可以基于流式计算系统 Storm 或者是 Spark Streaming,在实现快速的流水计算同时,保护对内存的访问模式,这种场景对 ORAM 的响应时间要求会很高.因此,未来将 ORAM 结合系统来实现是研究的一种重要的趋势.

7 结束语

不经意随机访问机是当前保护访问模式隐私的重要手段,其研究受到了学术界的广泛关注,近几年也有较大的进展,主要集中于模型在平均带宽与客户端存储上的性能优化以及与安全存储、安全计算领域相结合的应用.但是从目前来看,ORAM 在实用性上依然面临严峻的挑战,未来还有很多的工作值得去做.

本文对不经意随机访问机的研究进行综述,包括 ORAM 的相关概念、设计方法以及优化模型性能的常见策略及其优劣性,讨论了将 ORAM 用于安全存储系统设计以及安全计算领域的一般性问题,并对未来不经意随机访问机的依然存在的问题、挑战与趋势进行了分析.期望通过我们的工作,能给以后的研究者提供有益的借鉴与参考,为不经意随机访问机的进一步发展做出贡献.

致谢 在此,我们向对本文的工作给予支持和宝贵建议的评审老师和同行表示衷心的感谢!

References:

[1] Wu X, Xu L, Zhang X. Poster: A certificateless proxy re-encryption scheme for cloud-based data sharing. In: Proc. of the 18th ACM Conf. on Computer and Communications Security. ACM Press, 2011. 869−872. [doi: 10.1145/2046707.2093514]

[2] Jung T, Li XY, Wan Z, Wan M. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. IEEE Trans. on Information Forensics and Security, 2015,10(1):190−199. [doi: 10.1109/tifs.2014.2368352]

[3] Pinkas B, Reinman T. Oblivious ram revisited. In: Proc. of the 30th Annual Cryptology Conf., Vol.6223. Berlin, Heidelberg: Springer-Verlag, 2010. 502−519. [doi: 10.1007/978-3-642-14623-7_27]

[4] Islam MS, Kuzu M, Kantarcioglu M. Access pattern disclosure on searchable encryption: Ramification, attack and mitigation. In: Proc. of the 18th Network and Distributed System Security Symp., Vol.20. 2012. 1−15. [doi: 10.1.1.673.8809]

[5] Dautrich Jr JL, Ravishankar CV. Compromising privacy in precise query protocols. In: Proc. of the 16th Int'l Conf. on Extending Database Technology. ACM Press, 2013. 155−166. [doi: 10.1145/2452376.2452397]

[6] Zheng W, Dave A, Beekman JG, *et al*. Opaque: An oblivious and encrypted distributed analytics platform. In: Proc. of the 14th USENIX Symp. on Networked Systems Design and Implementation. USENIX Association, 2017. 283−298.

[7] Shaon F, Kantarcioglu M, *et al*. SGX-BigMatrix: A practical encrypted data analytic framework with trusted processors. In: Proc. of the 24st ACM Conf. on Computer and Communications Security. ACM Press, 2017. 1211−1228. [doi: 10.1145/3133956.3134095]

[8] Gordon SD, Katz J, Kolesnikov V, *et al*. Secure two-party computation in sublinear (amortized) time. In: Proc. of the 19th ACM Conf. on Computer and Communications Security. ACM Press, 2012. 513−524. [doi: 10.1145/2382196.2382251]

[9] Wang X, Chan H, Shi E. Circuit ORAM: On tightness of the goldreich-ostrovsky lower bound. In: Proc. of the 22nd ACM Conf. on Computer and Communications Security. ACM Press, 2015. 850−861. [doi: 10.1145/2810103.2813634]

[10] Oblivious RAM. https://en.wikipedia.org/wiki/Oblivious_ram

[11] Ohrimenko O, Costa M, Fournet C, *et al*. Observing and preventing leakage in MapReduce. In: Proc. of the 22nd ACM Conf. on Computer and Communications Security. ACM Press, 2015. 1570−1581. [doi: 10.1145/2810103.2813695]

[12] Dinh TTA, Saxena P, Chang EC, *et al*. M^2R: Enabling stronger privacy in MapReduce computation. In: Proc. of the 24th Symp. on USENIX Security. USENIX Association, 2015. 447−462.

[13] Goldreich O, Ostrovsky R. Software protection and simulation on oblivious RAMs. Journal of the ACM (JACM), 1996,43(3): 431−473. [doi: 10.1145/233551.233553]

[14] Kushilevitz E, Lu S, Ostrovsky R. On the (in) security of hash-based oblivious RAM and a new balancing scheme. In: Proc. of the 23rd Annual ACM-SIAM Symp. on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2012. 143−156. [doi: 10.1137/1.9781611973099.13]

[15] Gentry C, Halevi S, Jutla C, *et al*. Private database access with he-over-oram architecture. In: Proc. of the 13th Int'l Conf. on Applied Cryptography and Network Security. Springer-Verlag, 2015. 172−191. [doi: /10.1007/978-3-319-28166-7_9]

[16] Stefanov E, Shi E, Song D. Towards practical oblivious RAM. In: Proc. of the 17th Network and Distributed System Security Symp. 2011.

[17] Stefanov E, Dijk MV, Shi E, *et al*. Path ORAM: An extremely simple oblivious RAM protocol. In: Proc. of the 20th ACM Conf. on Computer and Communications Security. ACM Press, 2013. 299−310. [doi: 10.1145/2508859.2516660]

[18] Garg S, Mohassel P, Papamanthou C. TWORAM: Round-optimal oblivious RAM with applications to searchable encryption. IACR Cryptology ePrint Archive, 2015. 1010.

[19] Moataz T, Mayberry T, Blass EO. Constant communication ORAM with small blocksize. In: Proc. of the 22nd ACM Conf. on Computer and Communications Security. ACM Press, 2015. 862−873. [doi: 10.1145/2810103.2813701]

[20] Stefanov E, Shi E. Oblivistore: High performance oblivious cloud storage. In: Proc. of the 34th IEEE Symp. on Security and Privacy. IEEE, 2013. 253−267. [doi: 10.1109/SP.2013.25]

[21] Zahur S, Wang X, Raykova M, *et al*. Revisiting square-root ORAM: Efficient random access in multi-party computation. In: Proc. of the 37th IEEE Symp. on Security and Privacy. IEEE, 2016. 218−234. [doi: 10.1109/SP.2016.21]

[22] Batcher KE. Sorting networks and their applications. In: Proc. of the Spring Joint Computer Conf. ACM Press, 1968. 307−314. [doi: 10.1145/1468075.1468121]

[23] Ajtai M, Komlós J, Szemerédi E. An $O(n\log n)$ sorting network. In: Proc. of the 15th Annual ACM Symp. on Theory of Computing. ACM Press, 1983. 1−9. [doi: 10.1145/800061.808726]

[24] Goodrich MT. Randomized shellsort: A simple oblivious sorting algorithm. In: Proc. of the 21st Annual ACM-SIAM Symp. on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2010. 1262−1277. [doi: 10.1137/1.978161197 3075.101]

[25] Ren L, Fletcher CW, Kwon A, *et al*. Constants count: Practical improvements to oblivious RAM. In: Proc. of the 24th USENIX Conf. on Security Symp. USENIX Association, 2015. 415−430.

[26] Devadas S, Dijk MV, Fletcher CW, *et al*. Onion ORAM: A constant bandwidth blowup oblivious RAM. In: Proc. of the 13th Theory of Cryptography Conf. Springer-Verlag, 2016. 145−174. [doi: 10.1007/978-3-662-49099-0_6]

[27] Shi E, Chan THH, Stefanov E, *et al*. Oblivious RAM with $O((\log N)^3)$ worst-case cost. In: Proc. of the 17th Int'l Conf. on Theory and Application of Cryptology and Information Security, Vol.7073. 2011. 197−214. [doi: 10.1007/978-3-642- 25385-0_11]

[28] Hoang T, Ozkaptan CD, Yavuz AA, *et al*. S3ORAM: A computation-efficient and constant client bandwidth blowup ORAM with shamir secret sharing. In: Proc. of the 24th ACM Conf. on Computer and Communications Security. ACM Press, 2017. 491−505. [doi: 10.1145/3133956.3134090]

[29] Maffei M, Malavolta G, Reinert M, *et al*. Privacy and access control for outsourced personal records. In: Proc. of the 36th IEEE Symp. on Security and Privacy. IEEE, 2015. 341−358. [doi: 10.1109/sp.2015.28]

[30] Maffei M, Malavolta G, Reinert M, *et al*. Maliciously secure multi-client ORAM. IACR Cryptology ePrint Archive, 2017. 329. [doi: 10.1007/978-3-319-61204-1_32]

[31] Williams P, Sion R, Carbunar B. Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage. In: Proc. of the 15th ACM Conf. on Computer and Communications Security. ACM Press, 2008. 139−148. [doi: 10.1145/1455770. 1455790]

[32] Williams P, Sion R. Access privacy and correctness on untrusted storage. ACM Trans. on Information and System Security, 2013, 16(3):12. [doi: 10.1145/2535524]

[33] Williams P, Sion R, Tomescu A. Privatefs: A parallel oblivious file system. In: Proc. of the 19th ACM Conf. on Computer and Communications Security. ACM Press, 2012. 977−988. [doi: 10.1145/2382196.2382299]

[34] Bindschaedler V, Naveed M, Pan X, *et al*. Practicing oblivious access on cloud storage: The gap, the fallacy, and the new way forward. In: Proc. of the 22nd ACM Conf. on Computer and Communications Security. ACM Press, 2015. 837−849. [doi: 10.1145/ 2810103.2813649]

[35] Sahin C, Zakhary V, Abbadi ElA, *et al*. Taostore: Overcoming asynchronicity in oblivious data storage. In: Proc. of the 37th IEEE Symp. on Security and Privacy. IEEE, 2016. 198−217. [doi: 10.1109/SP.2016.20]

[36] Ostrovsky R, Shoup V. Private information storage. In: Proc. of the 29th Annual ACM Symp. on Theory of Computing. ACM Press, 1997. 294−303.

[37] Lu S, Ostrovsky R. Distributed oblivious RAM for secure two-party computation. In: Proc. of the 10th Conf. on Theory of Cryptography. Springer-Verlag, 2013. 377−396. [doi: 10.1007/978-3-64 2-36594-2_22]

[38] Keller M, Scholl P. Efficient, oblivious data structures for MPC. In: Proc. of the 21st Int'l Conf. on Theory and Application of Cryptology and Information Security. Springer-Verlag, 2014. 506−525. [doi: 10.1007/978-3-662-45608-8_27]

[39] Wang XS, Nayak K, Liu C, *et al*. Oblivious data structures. In: Proc. of the 21st ACM Conf. on Computer and Communications Security. ACM Press, 2014. 215−226. [doi: 10.1145/2660267.2660314]

[40] Boyle E, Gilboa N, Ishai Y. Function secret sharing. LNCS, 2015,9057:337−367. [doi: 10.1007/978-3-662-46803-6_12]

[41] Maas M, Love E, Stefanov E, *et al*. Phantom: Practical oblivious computation in a secure processor. In: Proc. of the 20th ACM Conf. on Computer and Communications Security. ACM Press, 2013. 311−324. [doi: 10.1145/2508859.2516692]

[42] Goodrich MT, Mitzenmacher M. Privacy-Preserving access of outsourced data via oblivious RAM simulation. In: Proc. of the 38th Int'l Colloquium on Automata, Languages, and Programming. Springer-Verlag, 2011. 576−587. [doi: 10.1007/978-3-642-22012-8_46]

[43] Pagh R, Rodler FF. Cuckoo hashing. In: Proc. of the 9th Annual European Symp. on Algorithms, Vol.2161. Springer-Verlag, 2001. 121−133. [doi: 10.1007/3-540-44676-1_10]

[44] Moataz T, Blass EO, Mayberry T. CHf-ORAM: A constant communication ORAM without homomorphic encryption. Technical Report, 2015/1116, Cryptology ePrint Archive, 2015.

[45] Dautrich J, Stefanov E, Shi E. Burst ORAM: Minimizing ORAM response times for bursty access patterns. In: Proc. of the 23rd Symp. on USENIX Security. USENIX Association, 2014. 749−764. [doi: 10.1007/BF02483924]

[46] Gentry C, Goldman KA, Halevi S, *et al*. Optimizing ORAM and using it efficiently for secure computation. In: Proc. of the 13th Int'l Symp. on Privacy Enhancing Technologies, Vol.7981. Springer-Verlag, 2013. 1−18. [doi: 10.1007/ 978-3-642-39077-7_1]

[47] Mayberry T, Blass EO, Chan AH. Efficient private file retrieval by combining ORAM and PIR. In: Proc. of the 20th Network and Distributed System Security Symp. 2014. [doi: 10.14722/ndss.2014.23033]

[48] Dautrich J, Ravishankar C. Combining ORAM with PIR to minimize bandwidth costs. In: Proc. of the 5th ACM Conf. on Data and Application Security and Privacy. ACM Press, 2015. 289−296. [doi: 10.1145/2699026.2699117]

[49] Apon D, Katz J, Shi E, *et al*. Verifiable oblivious storage. In: Proc. of the 17th Int'l Conf. on Practice and Theory in Public-Key Cryptography. Springer-Verlag, 2014. 131−148. [doi: 10.1007/978-3-642-54631-0_8]

[50] Damgard I, Jurik M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In: Proc. of the 4th Int'l Workshop on Practice and Theory in Public Key Cryptography, Vol.1992. Springer-Verlag, 2001. 119−136. [doi: 10.1007/ 3-540-44586-2_9]

[51] Goldberg I. Improving the robustness of private information retrieval. In: Proc. of the 28th IEEE Symp. on Security and Privacy. IEEE, 2007. 131−148. [doi: 10.1109/SP.2007.23]

[52] Abraham I, Fletcher CW, Nayak K, *et al*. Asymptotically tight bounds for composing ORAM with PIR. In: Proc. of the 20th Int'l Conf. on Practice and Theory in Public-Key Cryptography. Springer-Verlag, 2017. 91−120. [doi: 10.1007/978-3-662-54365-8_5]

[53] Boneh D, Mazieres D, Popa RA. Remote oblivious storage: Making oblivious RAM practical. Manuscript, 2011. http://dspace.mit.edu/bitstream/handle/1721.1/62006/MIT-CSAIL-TR-2011-018.pdf

[54] Fletcher CW, Naveed M, Ren L, *et al*. Bucket ORAM: Single online roundtrip, constant bandwidth oblivious RAM. IACR Cryptology ePrint Archive, 2015. 1065.

[55] Chung KM, Pass R. A simple ORAM. IACR Cryptology ePrint Archive, 2013. 243.

[56] Chung KM, Liu Z, Pass R. Statistically-Secure ORAM with $O(\log^2 n)$ overhead. In: Proc. of the 20th Int'l Conf. on Theory and Application of Cryptology and Information Security. Springer-Verlag, 2014. 62−81. [doi: 10.1007/978-3- 662-45608-8_4]

[57] Sanchez AM. Toward efficient data access privacy in the cloud. IEEE Communications Magazine, 2013,51(11):39−45. [doi: 10.1109/MCOM.2013.6658650]

[58] Moataz T, Mayberry T, Blass EO, *et al*. Resizable tree-based oblivious RAM. In: Proc. of the 19th Int'l Conf. on Financial Cryptography and Data Security. Springer-Verlag, 2015. 147−167. [doi: 10.1007/978-3-662-47854-7_9]

[59] Goodrich MT, Mitzenmacher M, Ohrimenko O, *et al*. Privacy-Preserving group data access via stateless oblivious RAM simulation. In: Proc. of the 23rd Annual ACM-SIAM Symp. on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2012, 13(Suppl 1):157−167. [doi: 10.1137/1.9781611973099.14]

[60] Williams P, Sion R, Sotakova M. Practical oblivious outsourced storage. ACM Trans. on Information and System Security, 2011, 14(2):20. [doi: 10.1145/2019599.2019605]

[61] Williams P, Sion R. Single round access privacy on outsourced storage. In: Proc. of the 19th ACM Conf. on Computer and Communications Security. ACM Press, 2012. 293−304. [doi: 10.1145/2382196.2382229]

[62] Stefanov E, Shi E. Multi-Cloud oblivious storage. In: Proc. of the 33rd ACM Conf. on Computer and Communications Security. ACM Press, 2013. 247−258. [doi: 10.1145/2508859.2516673]

[63] Sun XN, Jiang H, Xu QL. Multi-User binary tree based ORAM scheme. Ruan Jian Xue Bao/Journal of Software, 2016,27(6): 1475−1486 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5002.htm [doi: 10.13328/j.cnki.jos.005002]

[64] Yao AC. Protocols for secure computations. In: Proc. of the 23rd Annual Symp. on Foundations of Computer Science. IEEE, 1982. 160−164. [doi: 10.1109/SFCS.1982.88]

[65] Goldwasser S, Micali S, Wigderson A. How to play any mental game, or a completeness theorem for protocols with an honest majority. In: Proc. of the 19th Annual ACM Symp. on Theory of Computing, Vol.87. ACM Press, 1987. 218−229. [doi: 10.1145/28395.28420]

[66] Faber S, Jarecki S, Kentros S, *et al*. Three-Party ORAM for secure computation. In: Proc. of the 21st Int'l Conf. on Theory and Application of Cryptology and Information Security. Springer-Verlag, 2015. 360−385. [doi: 10.1007/978-3- 662-48797-6_16]

[67] Doerner J. Scaling ORAM for secure computation. In: Proc. of the 24th ACM Conf. on Computer and Communications Security. ACM Press, 2017. 523−535. [doi: 10.1145/3133956.3133967]

[68] Wang XS, Huang Y, Chan THH, *et al*. SCORAM: Oblivious RAM for secure computation. In: Proc. of the 21st ACM Conf. on Computer and Communications Security. ACM Press, 2014. 191−202. [doi: 10.1145/2660267.2660365]

[69] Xiao W, Dov G, Jonathan K. Simple and efficient two-server ORAM. IACR Cryptology ePrint Archive, 2018. 005.

[70] Thang H, Ceyhun DO, Gabriel H, Attila AY. Efficient oblivious data structures for database services on the cloud. IACR Cryptology ePrint Archive, 2017. 1238.

[71] Zhao C, Dong X, Li F. Oblivious ram: A dissection and experimental evaluation. In: Proc. of the 42nd Int'l Conf. on Very Large Databases. ACM Press, 2016. 1113−1124. [doi: 10.14778/2994509.2994528]

[72] Boyle E, Chung KM, Pass R. Oblivious parallel RAM and applications. In: Proc. of the 13th Theory of Cryptography Conf. Springer-Verlag, 2016. 175−204. [doi: 10.1007/978-3-662-49099-0_7]

[73] Malkhi D, Nisan N, Pinkas B, *et al*. Fairplay—A secure two-party computation system. In: Proc. of the 13th Symp. on USENIX Security. USENIX Association, 2004. 20−20.

[74] Ben-David A, Nisan N, Pinkas B. FairplayMP: A system for secure multi-party computation. In: Proc. of the 15th ACM Conf. on Computer and Communications Security. ACM Press, 2008. 257−266. [doi: 10.1145/1455770.1455804]

[75] Bogdanov D, Laur S, Willemson J. Sharemind: A framework for fast privacy-preserving computations. In: Proc. of the 13th European Symp. on Research in Computer Security, Vol.5283. Springer-Verlag, 2008. 192−206. [doi: 10.1007/978-3-540-88313-5_13]

附中文参考文献:

[63] 孙晓妮,蒋瀚,徐秋亮.基于二叉树存储的多用户 ORAM 方案.软件学报,2016,27(6):1475−1486. http://www.jos.org.cn/1000-9825/5002.htm [doi: 10.13328/j.cnki.jos.005002]

吴鹏飞(1994－),男,江苏淮安人,博士生,主要研究领域为分布式系统安全,隐私保护,大数据安全.

钱文君(1994－),女,博士生,主要研究领域为可信计算,系统安全,大数据计算安全,隐私保护.

沈晴霓(1970－),女,博士,教授,博士生导师,CCF 高级会员,主要研究领域为操作系统与虚拟化安全,云计算,大数据安全与隐私,可信计算.

李聪(1990－),男,博士生,CCF 学生会员,主要研究领域为公钥密码,区块链,云计算安全.

秦嘉(1993－),男,硕士生,主要研究领域为加密共享,隐私保护.

吴中海(1968－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为大数据系统与分析,大数据与云安全,嵌入式系统.