

References

- [GO96] Oded Goldreich and Rafail Ostrovsky. “Software Protection and Simulation on Oblivious RAMs”. In: *J. ACM* 43.3 (May 1996), pp. 431–473. ISSN: 0004-5411. DOI: 10.1145/233551.233553. URL: <http://doi.acm.org/10.1145/233551.233553>.
- [Goo+11] Michael T. Goodrich et al. “Privacy-Preserving Group Data Access via Stateless Oblivious RAM Simulation”. In: *CoRR* abs/1105.4125 (2011). arXiv: 1105.4125. URL: <http://arxiv.org/abs/1105.4125>.
- [Shi+11] Elaine Shi et al. “Oblivious RAM with $O(\log^3 N)$ Worst-Case Cost”. In: *Advances in Cryptology – ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 197–214. ISBN: 978-3-642-25385-0. DOI: 10.1007/978-3-642-25385-0_11. URL: https://doi.org/10.1007/978-3-642-25385-0_11.
- [SSS11] Emil Stefanov, Elaine Shi, and Dawn Song. “Towards Practical Oblivious RAM”. In: *CoRR* abs/1106.3652 (2011), pp. 1–40. arXiv: 1106.3652. URL: <http://arxiv.org/abs/1106.3652>.
- [FDD12] Christopher W. Fletcher, Marten van Dijk, and Srinivas Devadas. “A Secure Processor Architecture for Encrypted Computation on Untrusted Programs”. In: *Proceedings of the Seventh ACM Workshop on Scalable Trusted Computing*. STC ’12. Raleigh, North Carolina, USA: ACM, 2012, pp. 3–8. ISBN: 978-1-4503-1662-0. DOI: 10.1145/2382536.2382540. URL: <http://doi.acm.org/10.1145/2382536.2382540>.
- [DR13] Jonathan L. Dautrich Jr. and China V. Ravishankar. “Compromising Privacy in Precise Query Protocols”. In: *Proceedings of the 16th International Conference on Extending Database Technology*. EDBT ’13. Genoa, Italy: ACM, 2013, pp. 155–166. ISBN: 978-1-4503-1597-5. DOI: 10.1145/2452376.2452397. URL: <http://doi.acm.org/10.1145/2452376.2452397>.
- [Fle13] Christopher Wardlaw Fletcher. “Ascend: An architecture for performing secure computation on encrypted data”. PhD thesis. 2013.
- [Gen+13] Craig Gentry et al. “Optimizing ORAM and Using It Efficiently for Secure Computation”. In: *Privacy Enhancing Technologies: 13th International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–18. ISBN: 978-3-642-39077-7. DOI: 10.1007/978-3-642-39077-7_1. URL: https://doi.org/10.1007/978-3-642-39077-7_1.

- [Ren+13] Ling Ren et al. “Design space exploration and optimization of path oblivious ram in secure processors”. In: *ACM SIGARCH Computer Architecture News* 41.3 (2013), pp. 571–582.
- [Ste+13] Emil Stefanov et al. “Path ORAM: An Extremely Simple Oblivious RAM Protocol”. In: *Proceedings of the 2013 ACM SIGSAC Conference on Computer Communications Security*. CCS ’13. Berlin, Germany: ACM, 2013, pp. 299–310. ISBN: 978-1-4503-2477-9. DOI: 10.1145/2508859.2516660. URL: <http://doi.acm.org/10.1145/2508859.2516660>.
- [Maa14] Martin Maas. “PHANTOM: Practical Oblivious Computation in a Secure Processor”. MA thesis. EECS Department, University of California, Berkeley, May 2014, pp. 1–87. URL: <http://www2.eecs.berkeley.edu/Pubs/TechRpts/2014/EECS-2014-89.html>.
- [NKW15] Muhammad Naveed, Seny Kamara, and Charles V. Wright. “Inference Attacks on Property-Preserving Encrypted Databases”. In: *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*. CCS ’15. Denver, Colorado, USA: ACM, 2015, pp. 644–655. ISBN: 978-1-4503-3832-5. DOI: 10.1145/2810103.2813651. URL: <http://doi.acm.org/10.1145/2810103.2813651>.
- [CXL16] Zhao Chang, Dong Xie, and Feifei Li. “Oblivious RAM: A Dissection and Experimental Evaluation”. In: *Proc. VLDB Endow.* 9.12 (Aug. 2016), pp. 1113–1124. ISSN: 2150-8097. DOI: 10.14778/2994509.2994528. URL: <http://dx.doi.org/10.14778/2994509.2994528>.
- [Kel+16] Georgios Kellaris et al. “Generic Attacks on Secure Outsourced Databases”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’16. Vienna, Austria: ACM, 2016, pp. 1329–1340. ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978386. URL: <http://doi.acm.org/10.1145/2976749.2978386>.