REFERENCES

[1] A. Akavia, D. Feldman, and H. Shaul. Secure search on encrypted data via multi-ring sketch. In *Proceedings of the 25th ACM Conference on Computer and Communications Security*, CCS, 2018.

[2] E. B. Barker. Recommendation for key management, part 1: General. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2016.

[3] J. Bater, G. Elliott, C. Eggen, S. Goel, A. N. Kho, and J. Rogers. SMCQL: secure query processing for private data networks. *PVLDB*, 10(6), 2017.

[4] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In *Theory of Cryptography Conference*, TCC, 2005.

[5] J. V. Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx. Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution. In *Proceedings of the 27th USENIX Security Symposium*, USENIX, 2018.

[6] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, and M. Steiner. Highly-scalable searchable symmetric encryption with support for boolean queries. In *Advances in Cryptology*, Crypto. 2013.

[7] A. Ceselli, E. Damiani, S. D. C. D. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati. Modeling and assessing inference exposure in encrypted databases. *ACM Transactions on Information and System Security (TISSEC)*, 8(1):119–152, 2005.

[8] V. Costan and S. Devadas. Intel sgx explained. *IACR Cryptology ePrint Archive*, 2016:86, 2016.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS, 2006.

[10] M. Ermolov and M. Goryachy. How to hack a turned-off computer, or running unsigned code in intel management engine. In *Black Hat Europe*, 2017.

[11] S. Faber, S. Jarecki, H. Krawczyk, Q. Nguyen, M. Rosu, and M. Steiner. Rich queries on encrypted data: Beyond exact matches. In *European Symposium on Research in Computer Security*, pages 123–145, 2015.

[12] D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *Advances in Cryptology – EUROCRYPT 2010*, pages 44–61. Springer Berlin Heidelberg, 2010.

[13] B. Fuller, M. Varia, A. Yerukhimovich, E. Shen, A. Hamlin, V. Gadepally, R. Shay, J. D. Mitchell, and R. K. Cunningham. Sok: Cryptographically protected database search. *arXiv preprint 1703.02014*, 2017.

[14] T. Ge and S. Zdonik. Answering aggregation queries in a secure system model. In *Proceedings of the 33rd international conference on Very Large Data Bases*, VLDB, 2007.

[15] C. Gentry et al. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.

[16] P. Grubbs, K. Sekniqi, V. Bindschaedler, M. Naveed, and T. Ristenpart. Leakage-abuse attacks against order-revealing encryption. Cryptology ePrint Archive, Report 2016/895, 2016.

[17] H. Hacigümüş, B. Iyer, C. Li, and S. Mehrotra. Executing sql over encrypted data in the database-service-provider model. In *Proceedings of the ACM SIGMOD Conference on Management of Data*, SIGMOD, 2002.

[18] F. Hahn, N. Loza, and F. Kerschbaum. Practical and secure substring search. In *Proceedings of the ACM SIGMOD Conference on Management of Data*, SIGMOD, 2018.

[19] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu. Secure multidimensional range queries over outsourced data. *The VLDB Journal—The International Journal on Very Large Data Bases*, (3):333–358, 2012.

[20] B. Hore, S. Mehrotra, and G. Tsudik. A privacy-preserving index for range queries. In *Proceedings of the 30th international conference on Very Large Data Bases*, VLDB, 2004.

[21] Y. Hu, W. J. Martin, and B. Sunar. Enhanced flexibility for homomorphic encryption schemes via CRT. In *Applied Cryptography and Network Security (ACNS)*, 2012.

[22] S. Kamara and T. Moataz. Sql on structurally-encrypted databases. In *International Conference on the Theory and Application of Cryptology and Information Security*, ASIACRYPT. Springer, 2018.

[23] M. Naveed, S. Kamara, and C. V. Wright. Inference attacks on property-preserving encrypted databases. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security*, CCS, 2015.

[24] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Eurocrypt*, 1999.

[25] A. Papadimitriou, R. Bhagwan, N. Chandran, and R. Ramjee. Big data analytics over encrypted datasets with seabed. In *12th USENIX Symposium on Operating Systems Design and Implementation*, OSDI, 2016.

[26] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan. Cryptdb: protecting confidentiality with encrypted query processing. In *Proceedings of the 23rd ACM Symposium on Operating Systems Principles*, SOSP, 2011.

[27] W. Zheng, A. Dave, J. G. Beekman, R. A. Popa, J. E. Gonzalez, and I. Stoica. Opaque: An oblivious and encrypted distributed analytics platform. In *NSDI*, pages 283–298, 2017.