

REFERENCES

- [1] Md Momin Al Aziz, Dima Alhadidi, and Noman Mohammed. 2017. Secure approximation of edit distance on genomic data. In *BMC medical genomics*.
- [2] Gilad Asharov, Daniel Demmler, Michael Schapira, Thomas Schneider, Gil Segev, Scott Shenker, and Michael Zohner. 2017. Privacy-preserving interdomain routing at Internet scale. In *Privacy Enhancing Technologies Symposium (PETS)*.
- [3] Gilad Asharov, Shai Halevi, Yehuda Lindell, and Tal Rabin. 2018. Privacy-preserving search of similar patients in genomic data. In *Privacy Enhancing Technologies Symposium (PETS)*.
- [4] Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. 2013. More efficient oblivious transfer and extensions for faster secure computation. In *ACM SIGSAG Conference on Computer and Communications Security (CCS)*.
- [5] Mikhail J. Atallah, Florian Kerschbaum, and Wenliang Du. 2003. Secure and private sequence comparisons. In *ACM Workshop on Privacy in the Electronic Society (WPES)*.
- [6] Mikhail J. Atallah and Jiangtao Li. 2005. Secure outsourcing of sequence comparisons. In *International Journal of Information Security*.
- [7] Erman Ayday. 2016. Cryptographic solutions for genomic privacy. In *Financial Cryptography and Data Security (FC)*.
- [8] Ke Cheng, Yantian Hou, and Liangmin Wang. 2018. Secure similar sequence query on outsourced genomic data. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*.
- [9] Marco Chiesa, Daniel Demmler, Marco Canini, Michael Schapira, and Thomas Schneider. 2017. SIXPACK: securing internet exchange points against curious onlookers. In *International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*.
- [10] Daniel Demmler, Kay Hamacher, Thomas Schneider, and Sebastian Stammmler. 2017. Privacy-preserving whole-genome variant queries. In *Cryptology and Network Security (CANS)*.
- [11] Daniel Demmler, Thomas Schneider, and Michael Zohner. 2015. ABY - a framework for efficient mixed-protocol secure two-party computation. In *Network and Distributed System Security Symposium (NDSS)*.
- [12] European Bioinformatics Institute. 2017. Genome Reference Consortium Human Build 38, Ensembl release 91. http://dec2017.archive.ensembl.org/Homo_sapiens/Info/Annotation. (2017). Accessed on 2018-03-27.
- [13] Roger Allan Ford and W. Nicholson Price II. 2016. Privacy and accountability in black-box medicine. *Michigan Telecommunications and Technology Law Review* (2016).
- [14] Oded Goldreich, Silvio Micali, and Avi Wigderson. 1987. How to play any mental game. In *ACM Symposium on Theory of Computing (STOC)*.
- [15] Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti. 2015. On non-cooperative genomic privacy. In *Financial Cryptography and Data Security (FC)*.
- [16] Somesh Jha, Louis Kruger, and Vitaly Shmatikov. 2008. Towards practical privacy for genomic computation. In *IEEE Symposium on Security and Privacy (S&P)*.
- [17] Seny Kamara and Marina Raykova. 2011. Secure outsourced computation in a multi-tenant cloud. In *IBM Workshop on Cryptography and Security in Clouds*.
- [18] Vladimir I. Levenshtein. 1966. Binary codes capable of correcting deletions, insertions, and reversals. In *Soviet physics doklady*.
- [19] Md Safiur Rahman Mahdi, Mohammad Zahidul Hasan, and Noman Mohammed. 2017. Secure sequence similarity search on encrypted genomic data. In *IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies*.
- [20] Benny Pinkas, Thomas Schneider, Gil Segev, and Michael Zohner. 2015. Phasing: private set intersection using permutation-based hashing. In *USENIX Security Symposium*.
- [21] Oleksandr Tkachenko, Christian Weinert, Thomas Schneider, and Kay Hamacher. 2018. Large-scale privacy-preserving statistical computations for distributed genome-wide association studies. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*.
- [22] Bing Wang, Wei Song, Wenjing Lou, and Y. Thomas Hou. 2017. Privacy-preserving pattern matching over encrypted genetic data in cloud computing. In *IEEE Conference on Computer Communications (INFOCOM)*.
- [23] Xiao Shaun Wang, Yan Huang, Yongan Zhao, Haixu Tang, XiaoFeng Wang, and Diyue Bu. 2015. Efficient genome-wide, privacy-preserving similar patient query based on private edit distance. In *ACM SIGSAG Conference on Computer and Communications Security (CCS)*.
- [24] Kris A. Wetterstrand. 2017. DNA sequencing costs: Data from the NHGRI Genome Sequencing Program (GSP). (2017). <http://www.genome.gov/sequencingcostsdata>. Accessed on 2018-03-23.
- [25] Andrew Yao. 1986. How to generate and exchange secrets. In *Foundations of Computer Science (FOCS)*.
- [26] Ruiyu Zhu and Yan Huang. 2017. Efficient privacy-preserving general edit distance and beyond. *Cryptology ePrint Archive, Report 2017/683*. (2017). <https://ia.cr/2017/683>.