MAC0499 - Theme and supervisor indication

Luiza Barros Reis Soezima [1]

[1]University of São Paulo (USP), Instituto de Matemática e Estatística (IME)
NUSP:11221842
lbrsoezima@usp.br

1 Supervisors

- **Supervisor:** Hilder Vitor Lima Pereira [2]

  [2] Universidade Estadual de Campinas (UNICAMP), Instituto de Computação, Campinas, Brazil

  hilder@unicamp.br

- **Co-supervisor:** Alfredo Goldman [3]

  [3] University of São Paulo (USP), Instituto de Matemática e Estatística (IME)

  gold@ime.usp.br

2 Theme

Retrieving information from databases pulls a constant activity on the daily routine, concurrently, its privacy concern when it comes to sensitive data develop a parallel problem. Private information retrieval (PIR) is a privacy protocol that allows a user to download a required message from a set of messages stored in a database without revealing the index of the required message to the databases.

In other words, PIR is protocol in which from one side, a possibly untrusted server holds a public database DB with N records. On the other side, a client wants to query for record $i \in \{0 \cdots N-1\}$, without letting the server learn the queried item they are looking up (and, hence, learning the value v associated with i they are interested in). A naive solution involves the client locally downloading the whole DB, but that can be expensive: the goal of PIR is to both preserve privacy and be more efficient than the total cost of downloading the whole DB. There are many proposed solutions for this problem, and for this Capstone Project, we will explore the ones that uses FHE (Fully Homomorphic Encryption) as cryptographic primitive. [2, 5, 9, 8, 3, 4, 11, 6, 7, 10, 1]

References

[1] Asra Ali, Tancrède Lepoint, Sarvar Patel, Mariana Raykova, Phillipp Schoppmann, Karn Seth, and Kevin Yeo. Communication–computation trade-offs in pir. Cryptology ePrint Archive, Paper 2019/1483, 2019. https://eprint.iacr.org/2019/1483.

[2] Sebastian Angel, Hao Chen, Kim Laine, and Srinath Setty. Pir with compressed queries and amortized query processing. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 962–979, 2018.

[3] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 41–50, 1995.

[4] Henry Corrigan-Gibbs, Alexandra Henzinger, and Dmitry Kogan. Single-server private information retrieval with sublinear amortized time. Cryptology ePrint Archive, Paper 2022/081, 2022. https://eprint.iacr.org/2022/081.

[5] Alex Davidson, Gonçalo Pestana, and Sofía Celi. Frodopir: Simple, scalable, single-server private information retrieval. Cryptology ePrint Archive, Paper 2022/981, 2022. https://eprint.iacr.org/2022/981.

[6] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, page 169–178, New York, NY, USA, 2009. Association for Computing Machinery.

[7] Alexandra Henzinger, Matthew M. Hong, Henry Corrigan-Gibbs, Sarah Meiklejohn, and Vinod Vaikuntanathan. One server for the price of two: Simple and fast Single-Server private information retrieval. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3889–3905, Anaheim, CA, August 2023. USENIX Association.

[8] Muhammad Haris Mughees, Hao Chen, and Ling Ren. Onionpir: Response efficient single-server pir. Cryptology ePrint Archive, Paper 2021/1081, 2021. https://eprint.iacr.org/2021/1081.

[9] Sarvar Patel, Giuseppe Persiano, and Kevin Yeo. Private stateful information retrieval. Cryptology ePrint Archive, Paper 2018/1083, 2018. https://eprint.iacr.org/2018/1083.

[10] Radu Sion and Bogdan Carbunar. On the computational practicality of private information retrieval. 01 2007.

[11] Mingxun Zhou, Andrew Park, Elaine Shi, and Wenting Zheng. Piano: Extremely simple, single-server pir with sublinear server computation. Cryptology ePrint Archive, Paper 2023/452, 2023. https://eprint.iacr.org/2023/452.