Hermitian codes for Secure and Private Information Retrieval

Francesco Ghiandoni

University of Perugia (Italy)

(Joint work with M. Giulietti, E. Mezzano, M. Timpanella)

Private information retrieval (PIR) addresses the question of how to retrieve data items from a database without disclosing information about the identity of the data items retrieved. The rate of a PIR scheme is measured as the ratio of the gained information over the downloaded information. Secure PIR complements this problem by further requiring the contents of the data to be kept secure. In particular, X-secure and T-private information retrieval (XST-PIR) is a form of PIR where data security is guaranteed against collusion among up to X servers and the user's privacy is ensured against collusion among up to T servers. Cross-subspace alignment (CSA) Reed-Solomon codes have been recently proposed by Jia et al. [1] as a means to construct XST-PIR schemes. In [2] and [3] Makkonen et al. reinterpret and generalize such CSA codes as algebraic geometric (AG) codes from curves of genus $0, 1$, respectively, and from higher-genus hyperelliptic curves.
In this talk we show a XST-PIR scheme coming from hermitian codes, i.e., AG codes over the Hermitian curve. Such scheme offers interesting tradeoffs between the field size, file size, number of colluding servers, and the total number of servers. When the field size is fixed, this translates in some cases to higher retrieval rates than those of [2, 3]. In addition, the new scheme exists also for some parameters where the original ones do not.

References

[1] Z. Jia, H. Sun, and S. A. Jafar. Cross subspace alignment and the asymptotic capacity of X-secure T-private information retrieval, *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5783–5798, 2019.

[2] O. Makkonen, D. A. Karpuk, and C. Hollanti. Algebraic geometry codes for cross-subspace alignment in private information retrieval. *2024 IEEE International Symposium on Information Theory*, pp. 2874-2879, 2024.

[3] O. Makkonen, D. A. Karpuk, and C. Hollanti. Secret Sharing for Secure and Private Information Retrieval: A Construction Using Algebraic Geometry Codes. arXiv preprint arXiv:2408.00542, 2024.