Research Internship Proposal: Fast Secure Computation Meets Linear-Time Encodable Codes

Geoffroy Couteau
IRIF, Université de Paris
couteau@irif.fr

November 12, 2020

Keywords. Cryptography, Secure Computation, Coding Theory

Supervisor. Geoffroy Couteau, CNRS research scientist – couteau@irif.fr

Host. Institut de Recherche en Informatique Fondamentale (IRIF, `https://www.irif.fr/`), Université de Paris. The head of IRIF is Frédéric Magniez – magniez@irif.fr.

Place. Paris, France

1 Context

Secure computation is a fundamental branch of cryptography and a very active research area. While standard cryptography addresses the challenge of protecting communications, the goal of secure computation is to protect *computations*: it allows groups of individuals to compute together a function of their joint private inputs, while concealing all information beyond the output of the function (in particular, no individual should learn anything about the private inputs of the other participants beyond what can already be deduced from their own input and the result of the function). Secure computation has a wide area of applications, from e-voting to privacy-preserving data analysis. However, some important barriers remain that prevent secure computation to be widely deployed.

A particularly important barrier is the *preprocessing cost.* All modern secure computation protocols are built in a two-stage format: first, in a preprocessing phase, the parties securely distribute long correlated random strings among themselves. This part is independent of the parties' inputs and of the function to be evaluated; hence, it can be executed ahead of time. Second, in the online phase, the parties retrieve these correlated random string and use them to execute an extremely fast, information-theoretically secure protocol. While this approach allows for a very good concrete efficiency in the online phase, securely generating and storing a very large amount of correlated randomness is highly non-trivial, and forms the core bottleneck of all modern protocols.

2 Goal

A recent line of work [BCGI18, BCG$^+$19b, BCG$^+$20b, BCG$^+$19a, BCG$^+$20a] has developed a set of new methods to generate large amounts of correlated randomness, using a very small amount of communication, and only local (offline) computation. At the heart of this new line of work is the study of the interplay between the generation of correlated randomness, and the hardness of decoding random linear codes.

While this effectively solved the communication and storage issues of previous solution, these methods still require more computation that the traditional methods. A way to circumvent this remaining limitation would be to develop and analyze new linear error-correcting codes over the binary fields which simultaneously meet a number of fundamental properties – typically, admitting a linear-time encoding algorithm, and having a high minimal distance. Existing solutions [GDP73, TZ06, DI14] suffer from a number of drawbacks, and this area lacks a unified study of what candidates can be achieved, and what security they might offer.

The goal of this internship will be to study the literature on linear-time encodable codes with high minimal distance, analyze existing constructions (both efficiency- and security-wise), provide new candidate constructions meeting the requirements of the aforementioned line of work, and develop new protocols for securely generating correlated randomness from these objects.

3 Additional Information

A good background on error-correcting codes and their applications to cryptography (module 2.13.2) would be beneficial. A strong background on general cryptography is expected as well (module 2.12.1). Being comfortable with discrete probabilities is a plus. The internship might be continued as a PhD. For more information, please contact couteau@irif.fr.

References

[BCG$^+$19a] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, P. Rindal, and P. Scholl. Efficient two-round OT extension and silent non-interactive secure computation. In *ACM CCS 2019*, pages 291–308. ACM Press, November 2019.

[BCG$^+$19b] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Efficient pseudorandom correlation generators: Silent OT extension and more. In *CRYPTO 2019*, 2019. eprint report 2019/448.

[BCG$^+$20a] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Correlated pseudorandom functions via variable-density LPN. In *FOCS*, 2020. To appear.

[BCG$^+$20b] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Efficient pseudorandom correlation generators from ring-LPN. In *CRYPTO 2020, Part II*, *LNCS* 12171, pages 387–416. Springer, Heidelberg, August 2020.

[BCGI18] E. Boyle, G. Couteau, N. Gilboa, and Y. Ishai. Compressing vector ole. In *CCS*, 2018.

[DI14] E. Druk and Y. Ishai. Linear-time encodable codes meeting the gilbert-varshamov bound and their cryptographic applications. In *ITCS 2014*, pages 169–182. ACM, January 2014.

[GDP73] S. I. Gelfand, R. L. Dobrushin, and M. S. Pinsker. On the complexity of coding. In *Second International Symposium on Information Theory*, pages 177–184, 1973.

[TZ06] J.-P. Tillich and G. Zémor. On the minimum distance of structured ldpc codes with two variable nodes of degree 2 per parity-check equation. In *2006 IEEE International Symposium on Information Theory*, pages 1549–1553. IEEE, 2006.