Linear Codes for Secure Computation

Clément Ducros, Geoffroy Couteau

CNRS, IRIF, Université de Paris
cducros@irif.fr,couteau@irif.fr

1 Abstract

The presentation discusses new ideas to push forward the mathematical study of linear codes in the context of their application to secure computation. Coding theory is a well-studied area that has led to many important results outside its original domain (data transmission over noisy channels), especially in the world of cryptography. Recently, in a line of work initiated by Geoffroy Couteau (one of the advisors), the hardness of decoding linear codes has been shown to have profound applications in the context of *Secure Multiparty Computation* (MPC). MPC is the branch of cryptography that studies the design of protocols for distributed computing on sensitive data held by individuals, concealing all information beyond the output of the protocol. We show that the existence of linear codes with specific properties would imply extremely efficient secure computation protocols.

About MPC. Secure Multiparty Computation is a branch of cryptography initiated by the work of Yao in 1986 [Yao86]. The objective of MPC is simple to understand: it enables users to compute diverse functions of their secret entries, but at the same time makes sure that those entries remain perfectly hidden. More formally, a secure computation protocol contains a number n of players $(P_1, ..., P_n)$, each one owning a secret value x_i. This value must remain secret throughout the process and no one other than P_i should know it. The players want to compute functions $(f_1, ..., f_n)$ with their inputs $x_1, ..., x_n$, such that at the end, each one has the information $f_i(x_1, ..., x_n)$. The protocol must verify two properties: it has to be *correct*, i.e. each P_i really get the value $f_i(x_1, ..., x_n)$; and it has to be *secure* i.e. that groups of cheating players cannot learn anything about the remaining private inputs. Nowadays MPC has major application, if you have a large computational power. It has already been applied in various real-world situations where important calculations had to be done on private data: e.g. in tax-fraud detection [BJSV15], electronic voting, auctions in agriculture markets [BCD$^+$09]. Currently, however, the protocols have a major drawback: the above examples required months of computation. To expand the use of MPC, it is necessary to reduce the complexity of the protocols. In particular, communication between the players is the core bottleneck of secure computation.

A new way to do MPC. Boyle, Couteau, Gilboa, Ishai, Kohl and Scholl laid the foundations of a novel application of coding theory as a promising approach to overcome the main efficiency bottleneck of secure computation: securely generating long correlated strings. This line of work led to important and significant improvements [BCG$^+$17, BCGI18, BCG$^+$19b, BCG$^+$19a, SGRR19, BCG$^+$20b, BCG$^+$20a] which allow for communication-efficient secure generation of correlated randomness, for several types of correlations (each particular type of correlation enables a family of MPC protocols, e.g. standard OT correlations enable 2-party computation over the boolean field, more complex correlations enable computation over arbitrary fields, etc).

Syndrome decoding and Coding Theory. The core idea of [BCG$^+$20a] is to develop a new tool to create random correlation. The construction relies on a new pseudo-random function (a function indistinguishable from a random function). This pseudo-random function is in fact derived from a variant of syndrome decoding, in which we use exponential size matrices with variable density and exponential noise vectors with also variable density. The pseudo-random function is then directly related with this variable-density matrix, and thus coding theory emerges. We study the security of this new assumption against a large family of decoding algorithms, including essentially all known algorithms such as information set decoding, Gaussian elimination, BKW, statistical decoding and many others. Building on an earlier but erroneous proof in [BCG+a], we formally prove that no such attack can efficiently solve the new syndrome decoding problem. We will also demonstrate several improvements to the construction and its concrete security analysis.

References

BCD$^+$09. P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft. Secure multiparty computation goes live. In *Financial Cryptography and Data Security*, pages 325–343, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

BCG$^+$17. E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, and M. Orrù. Homomorphic secret sharing: Optimizations and applications. In *ACM CCS 2017*, pages 2105–2122. ACM Press, October / November 2017.

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, Part III*, *LNCS* 11694, pages 489–518. Springer, Heidelberg, August 2019.

BCG$^+$20a. E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl. Correlated pseudorandom functions from variable-density LPN. In *61st FOCS*, pages 1069–1080. IEEE Computer Society Press, November 2020.

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 *ACM CCS 2018*, pages 896–912. ACM Press, October 2018.

BJSV15. D. Bogdanov, M. Jõemets, S. Siim, and M. Vaht. How the estonian tax and customs board evaluated a tax fraud detection system based on secure multi-party computation. In *Financial Cryptography and Data Security*, pages 227–234, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

SGRR19. P. Schoppmann, A. Gascón, L. Reichert, and M. Raykova. Distributed vector-OLE: Improved constructions and implementation. In *ACM CCS 2019*, pages 1055–1072. ACM Press, November 2019.

Yao86. A. C.-C. Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society Press, October 1986.