Fast Computations on Shared Polynomials in MPC

Lucas Ottow

University of Montpellier, LIRMM - CNRS

The aim of secure multi-party computation protocols is to allow a set of players to compute a given function on their secret inputs without revealing any other information than the result of the computation. Multiple techniques, such as the Ben-Or, Goldwasser and Widgerson protocol [BGW88] or Beaver triples [Bea92], allow a set of player to compute basic operations on shared elements of a finite field in a private manner. Therefore for a given functionality, the aim is to find protocols as efficient as possible. By efficient, we mean with a constant number of communication rounds and with as little multiplications between shares (named secure multiplications) as possible.

In their seminal article at PKC 2006, Mohassel and Franklin [MF06] proposed constant-rounds protocols for the main operations on shared polynomials with coefficients in a finite field $\mathbb{K}$. Notably, to multiply a unbounded number n of shared polynomials of degree less than d in a constant number of round (an operation called *fan-in multiplication*), their technique requires $\mathcal{O}(n^2 d)$ secure multiplications in $\mathbb{K}$. Moreover, they propose a protocol allowing parties to compute the *interpolation* over a number of d shared points and d shared values in $\mathcal{O}(d^2)$ secure multiplications. These protocols remained the most efficient since 2006. In this work, we improve the *fan-in multiplication of nonzero polynomials* from $\mathcal{O}(n^2 d)$ secure multiplications to $\mathcal{O}(\tau n d^{1+1/\tau})$, where τ is any constant integer. With similar methods, we are also able to compute *multi-point evaluation* and *interpolation* in $\mathcal{O}(\tau d^{1+1/\tau})$ secure multiplications instead of $\mathcal{O}(d^2)$.

In their article, Mohassel and Franklin also describe a way to compute the extended gcd of two shared polynomial $[f]$ and $[g]$ (of degree at most d) but acknowledge that their method is quite expensive in terms of secure multiplications as it involves matrix inversion. However, if one of the shared polynomial, say $[g]$, is known to be irreducible, then the problem can be reduced to finding the inverse of $[f]$ seen as an element of an extension field defined by $[g]$. If some pre-computation depending only on $[g]$ is allowed, then we are able to use known techniques from computer algebra by Brieulle, De Feo, Doliskani, Flori and Schost [DFDS14] [BDFD$^+$19]. This allows to efficiently transform the original problem to inverting a shared polynomial $[\phi(f)]$ modulo a *publicly known* irreducible polynomial h (in contrast to $[g]$ which is shared), which is a much easier problem. Overall, this translates to a protocol requiring $\mathcal{O}(d^2)$ secure multiplications instead of $\mathcal{O}(d^3)$ secure multiplications (if using the BGW protocol, our protocol requires $\mathcal{O}(d^{1.5})$ secure multiplications instead of $\mathcal{O}(d^2)$).

Computation on shared polynomials can be a core component of secure protocols involving private sets, such as *private disjointness test* or *private set intersection*. Using our protocol for *multi-point polynomial evaluation* and tech-

niques from [DFK+06], we are able to propose variants of protocols presented in [NAA+09], [GN19] and [LW07] which are either more efficient or always return a correct result.

The recent call of the NIST shows the need for new post-quantum threshold cryptosystems. In this prospect, many threshold variants of existing post-quantum cryptosystems are proposed. Notably, the classic McEliece cryptosystem [McE78] is one of them. For classic McEliece, shared polynomials are a natural tool to try and propose a threshold variant, as its decryption algorithm relies heavily on operations on polynomials. Notably, the authors of [THO23] one threshold variant of the McEliece cryptosystem that uses shared polynomials in its decryption protocol. With our methods, we are able to speed up some parts of the decryption protocol of this variant, as well as reducing the size of the private key. We aim to propose a IND-TCCA variant of the McEliece cryptosystem with an efficient decryption protocol.

References

BDFD+19. Ludovic Brieulle, Luca De Feo, Javad Doliskani, Jean Pierre Flori, and Éric Schost. Computing isomorphisms and embeddings of finite fields. *ACM Commun. Comput. Algebra*, 52(4):117–119, may 2019.

Bea92. Donald Beaver. Efficient multiparty protocols using circuit randomization. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 420–432. Springer, Heidelberg, August 1992.

BGW88. Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, May 1988.

DFDS14. Luca De Feo, Javad Doliskani, and Éric Schost. Fast arithmetic for the algebraic closure of finite fields. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, page 122–129, New York, NY, USA, 2014. Association for Computing Machinery.

DFK+06. Ivan Damgård, Matthias Fitzi, Eike Kiltz, Jesper Buus Nielsen, and Tomas Toft. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 285–304. Springer, Heidelberg, March 2006.

GN19. Satrajit Ghosh and Tobias Nilges. An algebraic approach to maliciously secure private set intersection. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 154–185. Springer, Heidelberg, May 2019.

LW07. Ronghua Li and Chuankun Wu. An unconditionally secure protocol for multi-party set intersection. In Jonathan Katz and Moti Yung, editors, *ACNS 07*, volume 4521 of *LNCS*, pages 226–236. Springer, Heidelberg, June 2007.

McE78. Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. The deep space network progress report 42-44, Jet Propulsion Laboratory, California Institute of Technology, January/February 1978. https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

MF06. Payman Mohassel and Matthew Franklin. Efficient polynomial operations in the shared-coefficients setting. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *PKC 2006*, volume 3958 of *LNCS*, pages 44–57. Springer, Heidelberg, April 2006.

NAA+09. G. Sathya Narayanan, T. Aishwarya, Anugrah Agrawal, Arpita Patra, Ashish Choudhary, and C. Pandu Rangan. Multi party distributed private matching, set disjointness and cardinality of set intersection with information theoretic security. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *CANS 09*, volume 5888 of *LNCS*, pages 21–40. Springer, Heidelberg, December 2009.

THO23. Kota Takahashi, Keitaro Hashimoto, and Wakaha Ogata. Chosen-ciphertext secure code-based threshold public key encryptions with short ciphertext. *Designs, Codes and Cryptography*, Oct 2023.