Secure Multi-Party Matrix Multiplication Based on Strassen-Winograd Algorithm
Calcul Multipartite Sécurisé de Multiplications de Matrices Basé sur l'Algorithme de Strassen-Winograd

Jean-Guillaume Dumas[1], Pascal Lafourcade[2], Julio Lopez-Fenner[3], David Lucas[1], Jean-Baptiste Orfila[1], Clément Pernet[1], Maxime Puys[4]

[1]) Université Grenoble Alpes, Laboratoire Jean Kuntzmann, CNRS, UMR 5224 Grenoble, France
[2]) LIMOS, Université Clermont Auvergne, Aubiere, France
[3]) Universidad de La Frontera, Departemento de Ingeneria Matematica, Temuco, Chile
[4]) Université Grenoble Alpes, Verimag, CNRS, Grenoble, France

Secure multiparty computation (MPC) allows n players to compute together the output of some function using private input without revealing them. In the end, the players only know the result and did not learn any other information.

Amongst known applications of MPC, one can for instance cite distributed evaluation of trust. In this context, players compute confidence by combining their mutual degrees of trust. This can be seen as a matrix product $C = A \times B$, where each player knows one row of the matrix containing their partial trust towards their neighbours, and the network has to compute a distributed matrix squaring. In this specific application, it is necessary to be able to efficiently compute matrix-matrix products with several parties, and in this work, we focus on a particular data layout where each party owns one row, for multiparty matrix multiplication of dimension $n \times n$, with n Players.

While some specific multiparty algorithm, as *YTP-SS* [1] exist, they use textbook matrix multiplication algorithm, which has $O(n^3)$ arithmetic and communication complexity. As in our setting, the volume of communication usually is of the same order of magnitude of the number of operations, we want to improve on this parameter. Some practical algorithms for matrix multiplication, as Winograd's variant of Strassen's algorithm [3] have a subcubic time complexity, and here, we show how to construct an MPC protocol based on this algorithm.

By exposing how to apply it in the aforementioned MPC framework, we show that speed-up in arithmetic cost carries over for the communication cost. For this, we rely on Naccache-Stern [2] semi-homomorphic encryption scheme and its ability to perform addition and subtraction of matrices, together with additive and multiplicative masking. Strassen-Winograd algorithm involves numerous addition and subtraction on parts of the A and B matrices that are held by different players. Security concerns require then that these entries should be encrypted from the start. As a consequence, the classic matrix multiplication of [1] can no longer be used, not even as a base case for Strassen-Winograd. We therefore propose an alternative base case. Its arithmetic cost is higher, but it involves an equivalent amount of communication. We shall show that this choice, combined with the recursive Strassen-Winograd algorithm compares favourably to [1] in communication cost for matrices of dimensions already larger than $n = 81$. Furthermore, we implemented our algorithm in C++, and we show that this communication volume improvement also appears in practice.

References

[1] J.-G. Dumas, P. Lafourcade, J.-B. Orfila, and M. Puys. Dual protocols for private multi-party matrix multiplication and trust computations. *Computers & Security*, 71:51–70, 2017. URL: `http://hal.archives-ouvertes.fr/hal-01344750`, `doi:10.1016/j.cose.2017.04.013`.

[2] D. Naccache and J. Stern. A new public key cryptosystem based on higher residues. In *Proc. of the 5th ACM Conference on Computer and Communications Security*, CCS '98, pages 59–66, New York, NY, USA, 1998. ACM. `doi:10.1145/288090.288106`.

[3] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, Aug 1969. `doi:10.1007/BF02165411`.