Perfectly-Secure Multi-Party Linear Algebra

Speaker: Jules Maire, Sorbonne Université, CNRS, LIP6

December 5, 2021

Abstract

This is a joint work with Damien Vergnaud. We present new secure multi-party computation protocols for linear algebra over a finite field which improve the state of the art in terms of security. We look at the case of *perfect security*, i.e., information-theoretic without error probability. We notably propose a constant-round protocol for solving systems of m linear equations in n variables over $\mathbb{F}_p$ with $m \leq n$ with complexity $O(kn^{2.5}+m\log(p))$ (where complexity is measured in terms of the number of secure multiplications required) with $k > r(m+n-2r)+1$ where r is the rank of the system. The numerous previous proposals were not error-free: known protocols can indeed fail and thus reveal information with probability $\Omega(m/p)$.

One also constructs efficient and perfect-secure multi-party protocols for (matrix)-polynomial evaluation and other linear algebra problems, in particular the computation of the characteristic polynomial which underlies many problems.

Our protocols are simple and rely on existing computer-algebra techniques, notably Preparata-Sarwate algorithm, a simple but poorly known "baby-step giant-step" method for computing the characteristic polynomial of a matrix, and techniques due to Mulmuley for error-free linear algebra in non-zero characteristic.

Keywords. Cryptography, Secure Multi-Party Computation, Characteristic Polynomial, Preparata-Sarwate Algorithm, Rank, Moore-Penrose Pseudo-Inverse, Linear System Solving, Polynomial Evaluation