Towards a threshold variant of the HQC cryptosystem and faster shared gcd computations

Lucas Ottow*[1]

[1]Exact Computing – LIRMM, Univ Montpellier, CNRS, Montpellier – France

Résumé

Secure multi-party computation (MPC) protocols aims to allow a set of players to compute a given function on secret inputs while learning only the result of the computation. Multiple techniques allow a set of players to compute basic operations on shared elements of a finite field in a private manner. For a given functionality, the aim is therefore to find protocols as efficient as possible (i.e. less multiplications and constant round of communication).

Threshold public key encryption is a variant of public key encryption (PKE) in which a certain number T out of a total number N participants is required to successfully decrypt a ciphertext. One way to build a threshold variant of existing PKEs is to design a (preferably efficient) MPC protocol to run the decryption algorithm of a classical PKE. Using this idea, we designed a new IND-CCA threshold scheme based on the McEliece cryptosystem, which solved security issues and is more efficient than previous works in terms of ciphertext sizes when the number of participants is large. The main step of McEliece decryption is decoding a Goppa codeword, for which we provided a somewhat efficient MPC protocol.

Following this work, we are designing a threshold scheme based on the HQC cryptosystem, which was recently standardized by the NIST as an alternative from the lattice-based primitives. The decryption algorithm of HQC require to decode Reed-Muller codewords and a Reed-Solomon codeword. They are done on a publicly known codes, contrary to McEliece whose codeword structure is hidden. However, the error weights corresponding to a given ciphertext is unknown in HQC, and might cause severe security issues if learned by an adversary. In McEliece, this issue didn't existed as the weight of the codeword is fixed for this PKE. This brings a new set of challenges towards a efficient MPC protocol for HQC decryption compared to McEliece. Nevertheless, it is possible to obtain dedicated MPC protocols for both Reed-Solomon and Reed-Muller decoding, and we use them in order to build MPC protocol for HQC decryption. We hope to use this MPC protocol in order to build an IND-CCA threshold scheme based on HQC.

In both Goppa and Reed-Solomon decoding, the main step is computing a rational function reconstruction, an operation related to the extended gcd of two univariate polynomials. In complexity theory, recent works have designed constant-depth parallel algorithms (with unbounded arity) to perform gcd computation. This allows us to design more efficient MPC protocols for extended gcd computation in special cases. These might have applications in other fields of cryptography, such as PSI and its variants. Collaboration avec Jakob Burkhardt, Pascal Giorgi, Fabien Laguillaumie et Damien Vergnaud.

*Intervenant