Analysis of a Symmetric Primitive
Operating on Large Fields

Léo Perrin

6 Months Internship Offer for Spring–Summer 2022

Recent advances in the design of zero-knowledge proof systems (e.g., STARKs [BBHR18]) have outlined the need for a new type of symmetric primitives. These have to provide the same security guarantees as more classical ones, e.g., such hash functions are still expected to be one-way, however they are defined over a different alphabet. While primitives like the AES or SHA-256 are defined over bit-strings, the new ones operate on a finite field $F_q$ of size $q$, where $q$ is usually greater than $2^{63}$, and is either a prime number or a power of 2.

This change in the underlying alphabet has massive consequences for the security analysis of these primitives. Indeed, while small finite fields such as $F_{256}$ have been used before (such as in the S-box of the AES [AES01]), care was taken to “break” the finite field structure by using subcomponents that were not defined over it (in the case of the AES, the S-box is composed with an affine permutation of $(F_2)^8$). It is not the case for these new designs, meaning for instance that subfields (when $q = 2^n$), or multiplicative subgroups (when $q$ is a prime) are additional structure that need to be taken into account.

The aim of this internship will be to analyse the security of one such primitive, i.e. Ciminion [DGGK21], or Reinforced Concrete [BGK+21]. Do they actually offer the security guarantees that are expected of such algorithms?

References


