Analyzing the Crossbred Algorithm for the MQ Problem

Damien Vidal*

This is a joint work with Claire Delaplace and Sorina Ionica

Given a polynomial system of m polynomials and n variables over a finite field $\mathbb{F}_p$, solving the system is proven to be NP-complete. Commonly used methods to solve these systems are algorithms computing Gröbner basis (F_4, F_5) or based on linear algebra (XL). In this work, we focus on the MQ (Multivariate Quadratic) problem, which means that we consider polynomials of degree 2. In particular, we are interested in the case where the polynomial system is defined over $\mathbb{F}_2$. In this case, exhaustive search becomes a viable way to solve a polynomial system (FES). Another approach consists in specifying some of the variable and try solving the resulting systems via algebraic approach. This is the idea behind Crossbred [JV17]) for instance.

Crossbred is one of the most efficient algorithm in practice, with implementations breaking records in the Fukuoka MQ challenge[1]. However, the theoretical complexity of the algorithm is not well understood. The authors claim it to be similar to FXL or BooleanSolve but, to the best of our knowledge, this conjecture remains to be proven. As such, the main objective of this work is to better understand it. With that in mind, we propose a variant of the Crossbred algorithm based on the matrix-F5 algorithm as described in [Bar04] in order to facilitate its analysis.

In my talk, I will present this new variant of the Crossbred algorithm. This includes an analysis on the choice of parameters for this variant and deeper comprehension of the algorithm. From the results obtained on the variant, we derive an analysis of the original Crossbred.

References

[Bar04] Magali Bardet. *Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* PhD thesis, Université Paris 6, 2004.

[JV17] Antoine Joux and Vanessa Vitse. A crossbred algorithm for solving boolean polynomial systems. In *Number-Theoretic Methods in Cryptology - NuTMiC 2017*, volume 10737 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 2017.

*damien.vidal@u-picardie.fr

[1] https://www.mqchallenge.org