Key-recovery of McEliece scheme for alternant codes of order 3 using Gröbner basis

Rocco Mora

Inria, Sorbonne Université

Abstract

Over the last ten years, several attempts have been made to break the McEliece scheme by setting up an algebraic system satisfied by the secret key and then solve it with Gröbner bases techniques. This approach was successful in the case where the number of unknowns is small enough. This happens to be the case for several McEliece schemes based on quasi-cyclic or quasi-dyadic Goppa codes which have very small public and secret key sizes. However, the general case still remains open.

We have started a systematic study of this issue by studying the algebraic system arising in the case of a slightly more general family of codes than Goppa codes, namely alternant codes, and by looking at very high rate codes which is the case where we expect that the Gröbner basis computation stays at a low degree due to the fact that there are in this case many linear equations that help in reducing the number of unknowns. This is also the regime where the system can be distinguished from a random code [FGO$^+$13]. Experiments showed that the computation of the Gröbner basis stays at a very small degree when the degree of the alternant is very small and our work was here to understand why and to improve this Gröbner basis approach.

We have introduced in this setting new ideas and have namely found a way to bring in new algebraic equations of low degree which are not in the ideal of the algebraic system introduced in [FOPT10] and that take into account that the variables describing the secret key have to satisfy some constraints : the "support" variables should be different from each other and the "multiplier" variables should be different from 0. These new equations are not only instrumental in reducing even further the largest degree attained by the Gröbner basis computation but also allow us to understand and predict the complexity of the Gröbner basis computation and to prove that this computation is of polynomial complexity.

This work could be seen as a first step towards understanding the effectiveness of attacking the McEliece scheme in the high rate regime (this corresponds to the case where the degree of the alternant code is small) and could lead to assess whether or not this approach is for instance able to break the 20-year-old digital signature CFS which corresponds to such a regime.

References

[FGO$^+$13] Jean-Charles Faugère, Valérie Gauthier, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high rate McEliece cryptosystems. *IEEE Trans. Inform. Theory*, 59(10):6830–6844, October 2013.

[FOPT10] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 279–298, 2010.