Étude pratique sur la résolution de systèmes polynomiaux correspondant à des attaques algébriques sur des primitives symétriques

Baptiste Daumen*[1] and Léo Perrin[2]

[1]Centre Inria de Paris – Institut National de Recherche en Informatique et en Automatique – France
[2]Inria de Paris – Université Paris-Sorbonne - Paris IV – France

Résumé

This work examines Arithmetisation-Oriented Primitives: cryptographic permutations developed for new protocols such as Fully Homomorphic Encryption, Multi Party Computing and Zero-Knowledge Proof. To assess their security, we focus on algebraic attacks relying on the Gröbner basis theory, which allow to find solutions of a system of equations composed of multivariate polynomials. Such an attack is well-suited to uncover weaknesses of these permutations due to their algebraic structure.
In order to fully understand how such attacks work, it is necessary to conduct both a theoretical analysis of the systems and a practical study. We focused on the second aspect, particularly on the tools used to carry out these attacks. When executed within a computer algebra system, the functions involved operate as black boxes. Then, it appears necessary to get an understanding of the algorithms implemented in these libraries. Thus, we provided a state-of-the-art overview of SageMath libraries to compute Gröbner bases: Singular, Macaulay2, Giac, msolve and Magma. In addition to this review, we developed a tool that allows to perform algebraic attacks on a chosen primitive and to model cryptographic problems while having a large choice on parameters related to the primitive itself and the attack. This tool implements many optimisations to enable the execution of a very large number of experiments and offers functions to analyse the results obtained. It would be made available to foster the research in this domain.

The first result provides a comparison of all the algorithms available in SageMath for computing a Gröbner basis, as well as a comparison of algorithms for changing term orders. In addition, for Singular and Magma, it returns the execution trace of the selected Gröbner basis algorithm, which can be essential for estimating the time complexity.

This tool makes also possible to generate random systems of equations that share the same structure as those arising from real cryptographic problems. We apply the same algebraic attack to these systems and compare the resulting timings as well as the degrees associated with the ideal (both the ideal degree and the solving degree). Time complexity seems to be lower for our systems than random ones. We have also observed than the ideal degree is lower than expected for an ideal with generators of a particular shape (Bézout bound is not tight in our case). Thus, these practical observations raise new questions related to the particular shape and properties of our systems.

*Intervenant

Some bugs have been fixed in SageMath, what make possible to perform experiments over a larger range of parameters.
Collaboration with Léo Perrin, my Master's thesis supervisor.