Algebraic Attack Implementation against Multivariate Quadratic Cryptosystems

Juan Grados, Pedro Lara, Renato Portugal
Laboratório Nacional de Computação Científica (LNCC)

Algebraic attacks against cryptosystems based on multivariate quadratic equations was originated with Patarin's linearisation equation attack method [Patarin 1995]. The general idea consists to convert the problem of breaking a cryptographic algorithm into solving a system of boolean equations. In this work, we propose an implementation in the `C` language that converts a system of quadratic polynomials over $GF(2^p)$ into a Conjunctive Normal Form (CNF) that can be solved by a SAT solver. To test the implementation, we choose Tao et. al's system [Tao et al. 2013], which is one of most recent proposals based on multivariate quadratic equations. The public key of this system is a sequence of multivariate quadratic polynomials $P_1, ..., P_m$ that belong to the ring $\mathbb{F}[X_1, ..., X_n]$ with $\mathbb{F} = GF(2^p)$. The evaluation of these polynomials at any given value corresponds to either the encryption procedure or the verification procedure. Inverting a multivariate quadratic map is equivalent to solving a set of quadratic equations over a finite field. To convert that system of quadratic equations over $GF(2^p)$ to a boolean system we take the following steps: 1) Convert the polynomials over $GF(2^p)$ to Algebraic Normal Form (ANF), 2) Convert the polynomials in ANF to boolean equations in CNF using `anf2cnf` tool. The CNF are output in the DIMACS format, which is the standard format that many SAT solvers use. Further details about ANF to CNF conversion can be founded in [Courtois and Bard 2006], 3) Map SAT variables and confirm the results outputed by a SAT solver.

Tab. 1 shows the number of clauses and variables generated by our tool using Tao et. al's algorithm and 4-SAT. The system consists in $m = 2n$ polynomials with n variables over $GF(2^2)$.

Table 1: Number of variables and clauses after converting Tao et. al's algorithm into a version of 4-SAT problem

Polynomials	4-SAT Variables	4-SAT Clauses
8	133	968
18	1637	12440
32	8585	66420
50	32602	255016
72	95490	751620
98	239040	1889212
128	530776	4206432

References

[Courtois and Bard 2006] Courtois, N. T. and Bard, G. V. (2006). Algebraic cryptanalysis of the data encryption standard. Cryptology ePrint Archive, Report 2006/402.

[Patarin 1995] Patarin, J. (1995). Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In Coppersmith, D., editor, *Advances in Cryptology — CRYPT0' 95*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Springer Berlin Heidelberg.

[Tao et al. 2013] Tao, C., Diene, A., Tang, S., and Ding, J. (2013). Simple Matrix Scheme for Encryption. In Gaborit, P., editor, *Post-Quantum Cryptography*, volume 7932 of *Lecture Notes in Computer Science*, pages 231–242. Springer Berlin Heidelberg.