Interactions between Computer Algebra (Gröbner Bases) and Cryptology

Jean-Charles Faugère
SALSA Project INRIA, Centre Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy Kennedy
Boite Courrier 169, 4, Place Jussieu 75252 Paris Cedex 05
Jean-Charles.Faugere@inria.fr

Categories and Subject Descriptors: **I.1.2 SYMBOLIC AND ALGEBRAIC MANIPULATION** Algorithms Algebraic algorithms; **D.4.6 Security and Protection** Cryptographic controls; Authentication

General Terms: Algorithms, Security

Keywords: Cryptology, Public Key, Gröbner basis, Algebraic Cryptanalysis, F_5 algorithm, Multivariate Cryptography

Abstract

The associated talk surveys how computer algebra techniques have been used to break several cryptosystems.

1. Computer Algebra – Cryptology

Recently, the interaction between Gröbner basis computation and several areas of Cryptography has been put forward highlighting the importance of Computer Algebra techniques to evaluate the security of several cryptosystems. This is precisely the goal of this tutorial to describe possible interactions between Cryptography and Computer Algebra. The most famous example of such an interaction is probably the LLL algorithm [26] : it was a key ingredient to solve a Computer Algebra problem (factoring polynomials over $\mathbb{Q}$); since then, it was used in *numerous* attacks in Cryptology.

To some reduced extent, one other example of interaction between the two scientific domains are the F_5/F_4[1] algorithms [17, 18]: proposed as general algorithms to speedup Gröbner basis computations they were used to break several cryptosystems (see for instance [19, 20, 21, 25, 22, 8, 9, 10]). Another interesting example of ping pong interactions between Computer Algebra and Cryptology is the *multivariate functional decomposition problem* (FDP): while the univariate case is a well known Computer Algebra problem (efficient implementations exist in most CA systems) the multivariate case was "unsolved". For this reason it was considered as a hard problem and used by Patarin [1] to design a new cryptosystem. Then, this cryptosystem was broken by the Crypto community [2, 3, 21]. Recently, by extending the last result [21] it was possible to derive a general algorithm [24] to solve FDP in the multivariate case. Lastly, an even more efficient version of this algorithm is presented in this Issac 2009 conference.

[1]available in the Maple, Magma and Singular CA systems.

ISSAC'09, July 28–31, 2009, Seoul, Republic of Korea.
ACM 978-1-60558-609-0/09/07.

2. Two fundamental problems in Cryptography

Since almost all important data is stored and transmitted in electronic form, the modern world is completely reliant on digital technologies. This potentially exposes this data to serious threats (for instance disclosure of data to unauthorized parties). The science of cryptography, a collection of mathematical techniques used to secure the transmission and storage of information, is one of the main tools to counter these threats.

Evaluate the security of existing cryptosystems.

Investigating the security of extensively used cryptographic standards – such as AES[16], SHA, RSA[27] – against the most powerful attacks is a permanent concern. Any progress in the cryptanalysis of such standards could have a huge impact, from a scientific and also economical point of view. Thus, a fundamental problem in cryptography is to *evaluate the security of cryptosystems* against the most powerful techniques. To this end, several *general* methods have been proposed: linear cryptanalysis, differential cryptanalysis, ... Extensively used cryptographic standards – such as AES [16] – are all resistant against linear and differential attacks. In this tutorial, we will describe another general method – *Algebraic Cryptanalysis* – to study the security of the main public-key and secret-key cryptosystems.

Algebraic Cryptanalysis.

Algebraic cryptanalysis can be described as a general framework that permits to asses the security of a wide range of cryptographic schemes [5, 13, 15, 14, 19, 20, 21, 22]. In fact the recent proposal and development of algebraic cryptanalysis is now widely considered as an important breakthrough in the analysis of cryptographic primitives. The basic principle of such cryptanalysis is to model a cryptographic primitive by a set of algebraic equations. The system of equations is constructed in such a way as to have a correspondence between the solutions of this system, and a secret information of the cryptographic primitive (for instance, the secret key of an encryption scheme). Then, evaluate the security of this cryptosystem is equivalent to estimate the theoretical/practical complexity of solving the corresponding system of equations. Since one of the most efficient tool for solving algebraic system over finite field is Gröbner bases [11], it is necessary to evaluate theoretically and practically the complexity of computing Gröbner bases over $\mathbb{F}_q$ (e.g. [6]).

Design of new cryptosystems.

Public key cryptography relies on the notion of (trapdoor) *one-way* function. Such a function is a function that is easy to compute (polynomial-time) on every input, but hard (at best sub-exponential) to invert given the image of a random input. One way functions themselves are constructed from *hard* problems (problems for which no polynomial-time algorithm is known). Although quite a few problems have been proposed to construct primitives, those effectively used are essentially factorization (RSA) and discrete logarithm. It is well-known that, although polynomial-time algorithms for those problems have not yet been found, they are not safe from a theoretic breakthrough, that would endanger the security of the corresponding schemes. Moreover, in quantum computers, polynomial-time algorithms [29] exist for factoring integers or solving the discrete logarithm problem over elliptic curves so that all widely used cryptosystems are threatened by quantum computing. Thus, one of the main issues in public key cryptography is to identify hard problems, and propose *new schemes* that are *not based on number theory*. In the context of this tutorial and among other problems, the hard problem of solving multivariate equations over a finite field is a very attracting problem: in one way it is very easy to evaluate polynomials but in the other way it is a NP-hard problem and it seems to be resistant against quantum computers. Another problem which is used to design cryptosystems is the ideal membership problem [30].

Open Problems presented in this talk

On the one hand algebraic techniques have been successfully applied against a number of multivariate schemes and in stream cipher cryptanalysis [5, 13, 15, 14, 19, 20, 21, 22]. On the other hand, the feasibility of algebraic cryptanalysis remains the *source of speculation* [13] for block ciphers , and an almost unexplored approach for hash functions [28, 9]. The main problem is that the size of the corresponding algebraic systems [4] are so huge (thousands of variables and equations) that nobody is able to predict correctly the complexity of solving such polynomial systems. In this talk we will present several open problems of such cryptosystems.

1. REFERENCES

[1] L. Goubin, and J. Patarin. *Asymmetric Cryptography with S-Boxes.* Information and Communication Security, First International Conference (ICICS'97), Lecture Notes in Computer Science vol. 1334, Springer–Verlag, pp. 369–380, 1997.

[2] D.F. Ye, K.Y. Lam, Z.D. Dai. *Cryptanalysis of "2R" Schemes*, Adv in Cryptology – CRYPTO 1999, Lecture Notes in Computer Science, vol. 1666, Springer–Verlag, pp. 315–325, 1999.

[3] D.F. Ye, Z.D. Dai and K.Y. Lam. *Decomposing Attacks on Asymmetric Cryptography Based on Mapping Compositions*, Journal of Cryptology (14), pp. 137–150, 2001.

[4] M. Albrecht, and C. Cid. *Algebraic Techniques in Differential Cryptanalysis.* Proceedings of the First International Conference on Symbolic Computation and Cryptography, SCC 2008, Beijing, China, April 2008.

[5] G. Ars. *Applications des bases de Gröbner à la cryptographie.* Thèse de doctorat, Université de Rennes I, 2004.

[6] M. Bardet, J-C. Faugère, B. Salvy and B-Y. Yang. *Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems.* In Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry, 2005.

[7] A. Bauer, and A. Joux. *Toward a rigorous variation of coppersmith's algorithm on three variables.* Advances in Cryptology – EUROCRYPT 2008, Lecture Notes in Computer Science, vol. 4515, Springer–Verlag, pp. 361–378, 2007.

[8] L. Bettale and J. C. Faugère and L. Perret. *Cryptanalysis of the TRMS Cryptosystem of PKC 05* AfricaCrypt 2008, Lecture Notes in Computer Science, vol. 5023, Springer-Verlag, pp. 143-155, 2008.

[9] L. Bettale and J. C. Faugère and L. Perret. *Security Analysis of Multivariate Polynomials for Hashing.* Information Security and Cryptology – Inscrypt 2008, Springer-Verlag, 2008.

[10] C. Bouillaguet, and P.-A. Fouque. *Analysis of the Collision Resistance of Radio Gatùn using Algebraic Techniques.* SAC 2008, LNCS, Springer–Verlag. *To appear.*

[11] B. Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal (German)*, PhD Thesis, Univ of Innsbruck, Math. Institute, Austria, 1965. (English Translation: J. of Symbolic Computation, Special Issue on Logic, Math and Comp Science: Interactions. Volume 41, Num. 3-4, pp 475-511, 2006).

[12] J. Buchmann, A. Pyshkin, and R-P Weinmann. *Block Ciphers Sensitive to Gröbner Basis Attacks.* Topics in Cryptology – CT RSA'06, Lecture Notes in Computer Science, vol. 3860, Springer–Verlag, pp. 313–331, 2006.

[13] N. Courtois, and J. Pieprzyk. *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations.* Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Computer Science, vol. 2501, pp. 267–287, 2002.

[14] N. Courtois. *Fast Algebraic Attacks on Stream Ciphers with Linear Feedback.* Advances in Cryptology – CRYPTO 2003, LNCS, vol. 2729, pp. 176–194, 2003.

[15] N. Courtois, and W. Meier. *Algebraic Attacks on Stream Ciphers with Linear Feedback.* Advances in Cryptology – EUROCRYPT 2003, Lecture Notes in Computer Science, vol. 2656, pp. 345–359, 2003.

[16] J. Daemen, V. Rijmen. *The Design of Rijndael: The Wide Trail Strategy.* Springer-Verlag (2001).

[17] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis: F_4.* Journal of Pure and Applied Algebra, vol. 139, pp. 61–68, 1999.

[18] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero: F_5.* Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.

[19] J.-C. Faugère, and A. Joux. *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner bases.* Advances in Cryptology – CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729, Springer-Verlag, pp. 44–60, 2003.

[20] J.-C. Faugère, and L. Perret. *Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects.* Advances in Cryptology – EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, pp. 30–47, 2006.

[21] J.-C. Faugère, and L. Perret. *Cryptanalysis of $2R^-$ Schemes.* Advances in Cryptology – CRYPTO 2006, Lecture Notes in Computer Science, vol. 4117, pp. 357–372, 2006.

[22] J.-C. Faugère, F. Levy-dit-Vehel, and L. Perret. *Cryptanalysis of MinRank.* Advances in Cryptology – CRYPTO 2008, Lecture Notes in Computer Science, vol. 5157, pp. 280–296, 2008.

[23] J. C. Faugère and L. Perret. *On the Security of UOV* pp. 103-109, Proceedings of the First International Conference on Symbolic Computation and Cryptography, SCC 2008, Beijing, China, April 2008.

[24] J.-C. Faugère, and L. Perret. *An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography.* Special Issue of the Journal of Symbolic Computation on Gröbner Bases Techniques in Cryptography and Coding Theory. 2009.

[25] P.-A. Fouque, G. Macariorat, L. Perret and J. Stern. *On the Security of the ℓ-IC Signature Scheme.* Public Key Cryptography, 14th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2008, Lecture Notes in Computer Science, vol. 4939, pp. 1–17, Springer–Verlag, 2008.

[26] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[27] R. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Dignatures and Public-Key Cryptosystems.* Communications of the ACM, 21-2, pp 120–126, 1978.

[28] M. Sugita, M. Kawazoe, L. Perret, and H. Imai. *Algebraic Cryptanalysis of 58-Round SHA-1.* Fast Software Encryption, 14th International Workshop, FSE 2007, Lecture Notes in Computer Science, vol. 4593, Springer–Verlag, pp. 349-365, 2007.

[29] P. W. Shor *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* SIAM J.Sci. Statist. Comput., 26 (1484) 1997.

[30] M. Caboara,F. Caruso, and C. Traverso *Gröbner bases for public key cryptography* ISSAC '08, ACM pp 315–324 (Linz/Hagenberg, Austria) 2008.