Research project **AC**

Algebraic cryptanalysis

Supervisor 1 Ronald Cramer and Marc Stevens
E-mail cramer@cwi.nl and stevens@cwi.nl
Institution Universiteit Leiden, and Centrum Wiskunde & Informatica (CWI)

Supervisor 2 TBA
E-mail TBA
Institution TBA

Research project short description:

This project focuses on developing algebraic cryptanalysis techniques and applying these on (lightweight) cryptographic primitives to analyze the security thereof.

In practice, private information is secured using encryption, typically using a cryptographic primitive such as a stream cipher or a block cipher. Algebraic cryptanalysis is used to analyze the security of cryptographic primitives against algebraic attacks and has been applied to, e.g., KeeLoq [CBW08], DES [CB07] and AES [MR02] Such algebraic attacks essentially consist of two steps. Firstly, to convert the cipher into a system of polynomial equations. Secondly, to solve the system of equations and extract the secret key from the solution.

An algebraic attack on a cryptographic primitive can be represented as an MQ problem – a system of multi-variate quadratic equations – typically over $\mathbb{F}_2$. The general MQ problem is an NP-hard problem over any field. However, when the system is overdefined, one can do significantly better using linearization techniques such as L [KS99], XL [CKPS00] and XSL [CP02]. These techniques are based on transforming a system of polynomial equations into a linear system by replacing all monomials (e.g., $x_i x_j$) with a new variable (e.g., y_{ij}), essentially losing some information. If this new system has enough equations then few enough solutions are found, which makes it possible to exhaustively search the desired unique solution to the original system among them that satisfies all additional equations of the form $y_{ij} = x_i x_j$. More equations for this linear system can be created by considering products $\prod_{j=1}^{D} x_{i_j} \times l_k$ of monomials of some fixed degree D and equations l_k, however the number of variables after linearization also grows.

The aim of this project is to develop more advanced techiques that can be applied to specific MQ problems with special properties arising from cryptanalysis, as well as applying those techniques to construct attacks against suitable cryptographic primitives.

References

[CB07] Nicolas Courtois and Gregory V. Bard, *Algebraic Cryptanalysis of the Data Encryption Standard*, IMA Int. Conf. (Steven D. Galbraith, ed.), Lecture Notes in Computer Science, vol. 4887, Springer, 2007, pp. 152–169.

[CBW08] Nicolas Courtois, Gregory V. Bard, and David Wagner, *Algebraic and Slide Attacks on KeeLoq*, FSE (Kaisa Nyberg, ed.), Lecture Notes in Computer Science, vol. 5086, Springer, 2008, pp. 97–115.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, EUROCRYPT (Bart Preneel, ed.), Lecture Notes in Computer Science, vol. 1807, Springer, 2000, pp. 392–407.

[CP02] Nicolas Courtois and Josef Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, ASIACRYPT (Yuliang Zheng, ed.), Lecture Notes in Computer Science, vol. 2501, Springer, 2002, pp. 267–287.

[KS99] Aviad Kipnis and Adi Shamir, *Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization*, CRYPTO (Michael J. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 19–30.

[MR02] Sean Murphy and Matthew J. B. Robshaw, *Essential Algebraic Structure within the AES*, CRYPTO (Moti Yung, ed.), Lecture Notes in Computer Science, vol. 2442, Springer, 2002, pp. 1–16.