

# Open problems in multivariate cryptanalysis

## – STORK Submission –

Nicolas T. Courtois and Louis Goubin

SchlumbergerSema, CP8 Crypto Lab, 36-38 rue de la Princesse,  
78430 Louveciennes, France.  
{NCourtois,LGoubin}@s1b.com

**Abstract.** In this paper we identify some important problems that the research in cryptography needs to solve in the next 10 years.

### 1 Design of Block Ciphers and Hash Functions

Several recently proposed ciphers, for example Rijndael (known as AES) and Serpent, are built with layers of very small and simple S-boxes interconnected by linear key-dependent layers. Their security relies on the fact, that the classical methods of cryptanalysis (e.g. linear or differential attacks) are based on probabilistic characteristics, which makes their security grow exponentially with the number of rounds  $N_r$ . However these ciphers violate another cryptographic design criterion: in the famous paper from 1949, Claude E. Shannon states that breaking a good cipher should require “as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type”, see [6].

This security design criterion has been neglected by the cryptographic research for some 53 years, believing that solving large systems of equations becomes intractable very easily. However recently, the contributions by Shamir, Klimov, Patarin, Courtois [5], and by Courtois and Pieprzyk [1], show that, it is not the number of variables that makes a problem hard to solve, but the balance between the number of equations and the number of monomials. Thus systems of equations that are overdefined, sparse, or both, turn out to be much easier to solve than expected. These results rise serious questions about the security of numerous block ciphers that were so far believed very secure, for example AES, see [1, 4]. The main problems to be solved remain:

1. Study the behaviour of the XL algorithm on random systems of equations.
2. Can XL be subexponential on average ?
3. Study the relations between the XL algorithm and Gröbner bases algorithms.
4. Study the XSL algorithm on random systems of equations.
5. Study the XSL algorithm on systems of equations derived from block ciphers.
6. Evaluate the security of AES and Serpent.

## 2 Design of Stream Ciphers and Pseudorandom Generators

Stream ciphers are usually composed of two components: one is simple and linear, designed to produce a sequence with a large period, another one is non-linear, designed to alter the simple periodic sequence. Most of the current research in stream cipher design focused on optimal disguising the linear part by the so called non-linearity criteria: high algebraic degree, large distance from the set of all affine functions, etc. However, again the Shannon criterion given above was completely overlooked. In many current stream ciphers, we have:

1. The output can be given as a simple multivariate equation in the key bits.
2. We usually consider that the attacker may dispose of an important quantity of keystream.

The combination of these two leads to highly overdefined systems of multivariate equations to solve. Clearly, the design of stream ciphers has much to fear from multivariate cryptanalysis methods. A first paper on this topic has already been published, see [2]. The main problems to be solved are:

1. Study the behaviour of XL on systems of equations of degree  $> 2$ .
2. Study methods to find higher-order approximations by boolean functions, also known as polynomial learning in presence of noise, or decoding Reed-Muller codes.
3. Study methods to lower the degree of system of multivariate equations (for example by adding additional variables).
4. Propose new design criteria on stream ciphers, as done for block ciphers by Courtois and Pieprzyk [1].

## References

1. Nicolas Courtois, Josef Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*. To be presented at ASIACRYPT'2002, a preprint with a different version of the attack is available at <http://eprint.iacr.org/2002/044/>
2. Nicolas Courtois, *Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt*. To be presented at ICISC'2002, a preprint is available at <http://eprint.iacr.org/2002/087/>
3. Nicolas Courtois, *The security of Hidden Field Equations (HFE)*. In Proceedings of Cryptographers' Track, RSA Conference 2001, San Francisco, 8-12 April 2001, LNCS 2020, Springer-Verlag, pp. 266-281.
4. Sean Murphy, Matthew Robshaw, *Essential Algebraic Structure within the AES*. In Proceedings of CRYPTO'2002, LNCS 2442, Springer-Verlag, pp. 1-16.
5. Adi Shamir, Jacques Patarin, Nicolas Courtois, Alexander Klimov, *Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations*. In Proceedings of EUROCRYPT'2000, LNCS 1807, Springer-Verlag, pp. 392-407.
6. Claude Elwood Shannon, *Communication theory of secrecy systems*. In Bell System Technical Journal, Vol. 28 (1949), see in particular page 704.