

# Open Problems in Multivariate Cryptography

Louis Goubin

[LGoubin@slb.com](mailto:LGoubin@slb.com)

Nicolas Courtois

[Ncourtois@slb.com](mailto:Ncourtois@slb.com)

SchlumbergerSema

Louveciennes

France

## Design of Block Ciphers and Hash Functions (1)

### ■ The “statistical” approach:

- Recently proposed block ciphers are built with layers of very small and simple S-boxes interconnected by linear key-dependent layers.
- Immune to statistical attacks (*e.g.* linear or differential cryptanalysis).
- These attacks are based on probabilistic characteristics.
- In this framework: security grows exponentially with the number of rounds.
- Examples: AES, Serpent, ...

## Design of Block Ciphers and Hash Functions (2)

### ■ The “algebraic” approach:

- Breaking a cipher should require “as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type” [Shannon, 1949]
- Common belief: large systems of equations become intractable very easily.
- However: what makes the problem hard to solve is not the number of variables, but the balance between the number of equations and the number of monomials:
  - The XL method [Shamir, Patarin, Courtois, Klimov, Eurocrypt'2000]
  - The XSL variant [Courtois, Pieprzyk, Asiacrypt'2002]
- Consequence: systems that are overdefined, sparse, or both, turn out to be much easier to solve than expected.

## Design of Block Ciphers and Hash Functions (3)

- This questions the security of numerous block ciphers, e.g. AES [Courtois, Pieprzyk 2002] [Murphy, Robshaw 2002]
- **Several problems remain to be solved:**
  - Study the behaviour of the XL algorithm on random systems of equations.
  - Can XL be subexponential on average ?
  - Study the relations between the XL algorithm and Gröbner bases algorithms.
  - Study the XSL algorithm on random systems of equations.
  - Study the XSL algorithm on systems of equations derived from block ciphers.
  - Evaluate the security of AES and Serpent.

## Design of Stream Ciphers and Pseudorandom Generators (1)

- Stream ciphers are usually composed of **two components**:
  - One is simple and linear: to produce a sequence with a large period.
  - One is non-linear: to alter the simple periodic sequences.
- Most of current research: optimal **disguising of the linear part**, by using non-linearity criteria:
  - High algebraic degree
  - Large distance from the set of all affine functions

Bruges - 26/11/2002

STORK Cryptography Workshop

5

## Design of Stream Ciphers and Pseudorandom Generators (2)

- However, in many current stream ciphers:
  - The output can be given as a simple multivariate equation in the key bits
  - The attacker may dispose of an important quantity of keystream.
  - → Highly overdefined systems of multivariate equations to solve.
- **Realistic attacks**:
  - Toyocrypt: attack in  $2^{39}$  [Courtois, Meier 2002]
  - Lili-128: attack in  $2^{57}$  [Courtois, 2002]

Bruges - 26/11/2002

STORK Cryptography Workshop

6

## Design of Stream Ciphers and Pseudorandom Generators (3)

### ■ **Several problems remain to be solved:**

- Study the behaviour of XL on systems of equations of degree  $>2$ .
- Study methods to find higher-order approximations by boolean functions, also known as polynomial learning in presence of noise, or decoding Reed-Muller codes.
- Study methods to lower the degree of system of multivariate equations (for example by adding additional variables).
- Propose new design criteria on stream ciphers, as done for block ciphers [Courtois, Pieprzyk 2002]