Polynomial System Solving with Noise

Martin Albrecht

26th January 2010

Outline

Outline

Block Ciphers

- A block cipher E_k is a keyed family of functions $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$.
- Block ciphers are used to secure Internet traffic, encrypt hard disks, facilitate electronic banking, ...
- A well-known technique for block cipher cryptanalysis is to model the cipher as a system of polynomial equations and to attempt to solve this system.
- A recent trend is to include probabilistic equations which are true with a probability < 1.
- These probabilistic equations come from **side-channel** data leakage or from some **bias** in the cipher itself.

In block cipher cryptanalysis we are confronted with the problem of solving polynomial systems with error.

RFID Security

- Radio-frequency identification (RFID) tags are widely used in asset management, public transport, product & inventory tracking.
- In many applications confidentiality, anonymity and unforgability are desired features.
- It is a widely held consensus in the research community that standard cryptographic primitives are too heavy-weight for deployment.
- Many current proposals build on the hardness of the "Learning Parity with Noise" (LPN) problem.
- However, we do not know the exact difficulty of this problem.

In RFID security we are thus confronted with the problem of solving linear polynomial systems with error.

Lattice Based Cryptography

- Public-key cryptography allows two parties to communicate securely without exchanging a common secret key beforehand.
- Most current public-key cryptography primitives are based on problems which are easy for quantum computers.
- Researchers study **post-quantum** cryptography, a prominent example are **lattice-based** systems.
- The security of some prominent constructions can be reduced to the difficulty of the "Learning with Error" (LWE) problem.
- Recently Craig Gentry solved the long standing problem of **fully homomorphic encryption** using an explicit construction using lattices.

In lattice based cryptography we are confronted with the problem of solving linear polynomial systems with error.

Outline

The Research Problem

Max-PoSSo

Given a set of polynomials $F = \{f_0, \ldots, f_{m-1}\} \subset \mathbb{F}[x_0, \ldots, x_{n-1}]$ and two index sets $\mathcal{H}$ and $\mathcal{S}$ such that $\mathcal{H} \cap \mathcal{S} = \varnothing$ and $\mathcal{H} \cup \mathcal{S} = \{0, \ldots, m-1\}$.

Return a point $X \in \mathbb{F}^n$ such that all f_i with $i \in \mathcal{H}$ and some f_j with $j \in \mathcal{S}$ evaluate to zero on X and the number of polynomials with indices in $\mathcal{S}$ which evaluate to zero is maximised.

- Is this the adequate model for the problems above?
- How difficult is this problem?
- Under which conditions is X unique?
- Can we solve this problem for cryptographic instances in practice?

Methodology

1. Collect examples from practice of varying difficulty in the areas mentioned above. Review literature.
2. Formalise and state problems and identify classes of problems.
3. Design and develop prototypes for algorithms.
4. Where possible, prove complexity bounds.
5. Demonstrate performance by applying algorithms to cryptographic problems.

Techniques

SAT-solving Investigate applicability of Max-SAT solvers, adapt these solvers if necessary.

Linear systems Investigate and exploit the similarities between the BKW and M4RI algorithm. Exploit the "history of additions".

Gröbner bases Track algebraic dependencies during the execution of the Gröbner basis algorithm similar to Conflict Clause Learning in SAT-solving.

Linear Programming Express cryptographic problems as MIP problems and express noise as objective function.

Dissemination

I will

1. use conventional academic information transfer processes such as journal/conference articles and conference/seminar presentations,
2. include the implemented algorithms in the Sage mathematics software,
3. maintain a public website giving details of the ongoing research, and
4. use extensive industrial contacts within ISG to ensure that any industrially relevant results will be disseminated.

Beneficaries

Many people in the U.K. and abroad are using algorithms whichs security is studied in this proposal.

Within the academic community many disciplines are affected:

Cryptography: this project studies current "hot topics" in cryptography: side-channel leakage, lattice-based cryptography and lightweight cryptography in a unified manner.

Symbolic Computation: this project offers new interesting problems and first solutions and will provide both theoretical and practical results (implementations, applications).

SAT Solving: this project offers interesting new applications and interfaces with other research disciplines.

Optimisation: this projects offers interesting new applications and interfaces with other research disciplines.

Impact on my Career

- I get to work on a timely, interesting problem for three years.
- I get to build on experience I already gathered, while looking into new problems.
- This project has the potential that I can make a significant name for myself if successful.
- I can build on the independence I have already achieved.

Thank you for your consideration!