

Position paper for STORK

Lars Knudsen
Institute of Mathematics (MAT)
Technical University of Denmark (DTU)

October 2002

1 Introduction

Traditionally, cryptography has been understood as the art of providing secure communication over insecure channels. The classical solution to this problem is to use encryption and message authentication codes, such that the data can be recovered and checked for errors, only if the correct secret key is known. Although we have today a good understanding of what secure encryption and authentication is, analyzing and arguing security of concrete solutions have proved extremely difficult. Security has often been argued based on ad-hoc arguments and reputation of the designers. However, in recent years, it has been demonstrated that encryption systems secure against a range of general attacks can be constructed, and authentication schemes with provable security have been constructed. **It is an important (and open) question how far this development can be taken.**

Recently it has been shown that tools from areas which are usually regarded as being outside of cryptography, have applications in cryptography. Most recent is the XSL attack [2], a system to solve nonlinear multivariate equations over a finite field and which is conjectured to cryptanalyse the Advanced Encryption Standard (Rijndael). Other researchers claim that the new attacks are flawed. Even if the latter is the case, the XSL attack is interesting and a further study of it is mandatory. As a few other examples, it has been shown that decoding algorithms for error-correcting codes [3] and probabilistic combinatorial optimization methods (e.g., simulated annealing) have applications in cryptanalysis [1]. **It is of utmost importance that the new tools for cryptanalysis are studied extensively and that the recent development in cryptanalysis of cryptologic primitives is continued.**

References

- [1] John A. Clark, Jeremy L. Jacob. Fault Injection and a Timing Channel on an Analysis Technique. In *Advances in Cryptology - EUROCRYPT'2002*, Lecture Notes in Computer Science, vol. 2332, Springer Verlag, 2002. To appear.

- [2] N. Courtois, J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. To appear in the proceedings of Asiacrypt'2002.
- [3] T. Johansson, F. Jönsson. Fast Correlation Attacks Based on Turbo Code Techniques. In *Advances in Cryptology - CRYPTO'99*, Lecture Notes in Computer Science, vol. 1592, Springer Verlag, 1999, pp. 347–362.