

Position on: Design and Analysis of Block Ciphers.

Alex Biryukov

Katholieke Universiteit Leuven, Dept. ESAT/SCD-COSIC,
Kasteelpark Arenberg 10,
B-3001 Leuven-Heverlee, Belgium
{abiryuko}@esat.kuleuven.ac.be

Abstract. In this note we present our views on the perspectives of design and cryptanalysis of block-ciphers. We try to look 5-10 years into the future and state what are the main goals for the research in this area.

"I think there is a world market
for maybe five computers."
Thomas Watson, Chairman of
IBM, 1943.

1 Introduction

Symmetric block ciphers are one of the main elements in many cryptographic systems. While the primary usage of block ciphers is for encryption, they are often used at the core of pseudo-random generators, hash functions and message authentication codes.

Cryptanalysis of block ciphers has received much attention from the cryptographic community, especially in the last decade and as a result many powerful methods of analysis have emerged (differential, linear, higher order differential, interpolation, impossible differential, related-key, sliding, boomerang, square attack). What most of these methods have in common (with exception of related key and slide attack) is an attempt to push statistical patterns through as many iterations of the cipher as possible in order to measure non-random behavior at the output, thus distinguishing a cipher from a truly random permutation. A new generation of block-ciphers (among them the NIST's Advanced Encryption Standard Rijndael), was constructed with understanding of these techniques and is thus not vulnerable to (at least a straightforward application of) these attacks. The task of designing ciphers immune to these statistical attacks is made easier, due to the fact that the complexity of the attacks grows exponentially with the number of rounds of a cipher. This ensures that the data and the time requirements of the attacks quickly become impractical. This is the current state of the art in the field.

Not trying to go into prediction of future far ahead we would like to enumerate research goals of potential interest for the next 5-10 years as we see it today:

- Finding new "active" methods of cryptanalysis, that benefit from adaptive chosen plaintext/chosen ciphertext queries (for ex. differential and linear techniques use only "passive" queries, jojo-game and boomerang attacks are adaptive but in a very simple way).
- Methods of analysis that benefit from (possibly heavy) preprocessing done once, and that allow faster on-line attacks. Except for the tradeoff techniques, conventional attacks rarely use preprocessing.
- Building symmetric primitives that are efficient and with security related to difficult mathematical problems. This direction of research would help to bridge the gap between theory and practice.
- Do recent re-linearization attacks pose a threat to a large class of symmetric primitives? What other algebraic attacks exist?
- Is it possible to use conventional building blocks (S-boxes, SPNs, Feistel structure, etc) to build a trapdoor blockcipher? Solution to this problem would provide us with new efficient asymmetric primitives and will also shed the light on abilities of malicious cipher designer.
- How to estimate an optimal (in terms of security) number of rounds for an iterative cipher. Currently no method except trying all known attacks exists.
- As modern iterative ciphers start using more and more rounds, it will be interesting to find more attacks that are independent of the number of rounds, or are polynomial in the number of rounds.