

Future Research in Cryptography by The University of Bergen

Inst. for Informatics, Hightechnology Center, Bergen, University of Bergen,
Bergen 5020, Norway

In all likelihood, there exists attacks on many cryptographic primitives that have not yet been discovered. It has been predicted that attacks of complexity 2^{64} on block ciphers of today's standard may be possible within the next 30 years, provided attacking such systems is given enough attention. We propose to develop new attacks and designs, both for block and stream ciphers, and for authentication codes, hash functions, signature and fingerprinting schemes.

There follows a list of some promising approaches the group in Bergen would like to take, both for the cryptanalysis of ciphers, and for the design of new cipher primitives.

- Attacks which use soft-decision decoding and message-passing techniques. These have been tentatively applied to attacks on stream ciphers, but not developed or formalised to any great extent for either stream, or block ciphers.
- The development of new attacks via the embedding of cipher systems in larger algebras. This has been the basis of the new 'BES' analysis of the AES. Other embeddings, i.e. $Z_2 \subseteq Z_4$, are currently under investigation by the group at Bergen.
- Attacks which apply list-decoding techniques, for instance by using Sudan's algorithm.
- Further mathematical development and formalisation of fault-attack and power-analysis techniques, and the design of ciphers which protect against such attacks using randomised algorithms and fault-tolerant and/or distributed computing.

- Improving correlation attacks on stream ciphers, and using number theory as a basis for attacks on stream ciphers.
- Investigating the connection between sequences and streamciphers, for instance by looking at non-linear feedback shift registers and their corresponding De Bruijn graphs.
- Little is known about the mathematical structure of nonlinear boolean functions and their extensions, although these form the primary components of virtually all practical cryptosystems. For instance, the study of Perfectly Nonlinear, Almost Perfectly Nonlinear, and Near-Perfectly Nonlinear functions is still in its infancy.
- Fingerprinting is of increasing importance in a commercial world and we propose to construct fingerprinting codes and fingerprinting schemes which can be used for copyright protection.
- The design and analysis of communications and computational networks, both fixed and ad-hoc, which are both functionally and information-theoretically secure.
- Shor's algorithm can form the basis of an attack on RSA using quantum computers. However, few quantum attacks have been developed for other primitives, such as block ciphers and stream ciphers. We suggest to investigate whether such attacks exist.
- The development of quantum cryptographic primitives, and the further development of quantum key exchange protocols.