Szczecin, 11.07.2022

DOCTORAL THESIS ABSTRACT

QUALITY EVALUATION METHODS OF KEY SCHEDULE ALGORITHMS IN BLOCK CIPHERS

Author: mgr inż. Michał Apolinarski
Supervisor: dr hab. inż. Krzysztof Chmiel
Auxilary supervisor: dr inż. Anna Grocholewska-Czuryło

Key schedule algorithms in block ciphers are used to generate a set of round keys from a master key (that is usually between 64 and 256 bits in length). These keys are then used in rounds (iterations) during the actual encryption or decryption process. An important requirement is that the round keys generated by this algorithm should have statistical properties similar to random sequences, which affects the process of cipher cryptanalysis.

To evaluate the statistical properties of pseudorandom sequences (ciphertext and round keys should be considered as such sequences), various types of statistical tests are applicable, including the NIST SP800-22 tests used in the competition for the AES standard to evaluate block ciphers.

In doctoral thesis NIST SP800-22 tests were used to evaluate key schedule algorithms, based on sequences of hundreds or thousands bits long round keys, generated from a single master key.

When designing a key schedule algorithm, it is necessary to find a tradeoff between the speed of round keys generation and security, especially when the designed cipher should be "lightweight", i.e. used in an environment with small, limited resources, such as an RFID card. With such limitations, it becomes problematic to determine the optimal structures that meet the given criteria. Thus, when designing a key schedule algorithm, it is worth to consider and test different variants of the operations used, such as rotation (cyclic shift), permutation, substitution, constants or other transformations.

The main goal of the dissertation is to propose the use of statistical tests and cluster analysis as an element that supports and enhances the evaluation of the design of key schedule algorithms in block ciphers. The various sub-tasks accomplished in the dissertation are.:

- Develop a method for testing and evaluating key schedule algorithms based on statistical tests and cluster analysis.
- Review and analysis of various designs of key schedule algorithms for block ciphers (including DES, LOKI97, KASUMI, AES (Rijndael), Serpent, PP-1, PP-2, IDEA, RC6, Speck).
- Theoretical and practical evaluation of the quality of selected key schedule algorithms.

11.07.2022