MILITARY UNIVERSITY OF TECHNOLOGY

ABSTRACT OF DOCTORAL DISSERTATION

Synthesis and optimisation of quantum logic circuits representing cryptographic primitives

Adam Jagielski, MSc Eng.

This thesis addresses issues related to the study of symmetric cryptography, quantum logic, and reversible logic. In particular, it focuses on representing symmetric cryptographic primitives as reversible circuits. The research is centred around seeking efficient methods for modelling ciphers as optimized circuits. Further studies are devoted to exploring the possibilities of inferring the quantum security of ciphers using the constructed circuits.

The following research results have been conducted and described:

- Synthesis of optimal reversible logic circuits representing substitution boxes (`SBOX`) of selected ciphers and cryptographic hash functions;
- Synthesis of the complete space of identity templates;
- Investigation of correlations between classical security properties of substitution boxes (`SBOX`) and the optimal size of their implementation;
- Study of the quantum security of ciphers from the `SPARKLE` family;
- Study of the quantum security of the `Ascon` lightweight encryption standard.

The research employs modern computational techniques, including `HPC` (High Performance Computing) and `CP` (Constraint Programming) using tools such as `SAT-solvers`.

The results obtained in the research provide a basis for proving the security of the `SPARKLE` cipher and the lightweight encryption standard `Ascon`. For the first time, the research presents optimal implementations of small substitution boxes in the reversible logic regime, along with proofs of optimality. The studies have demonstrated a positive correlation between classical security parameters of substitution boxes and the implementation size as a quantum logic circuit, and the complete space of circuits realizing the identity function for dimensions not exceeding 6×7 has been determined.

Keywords: Quantum logic, Reversible logic, Symmetric cryptography, SAT-solver, Substitution boxes, SBOX, Sparkle, Ascon.