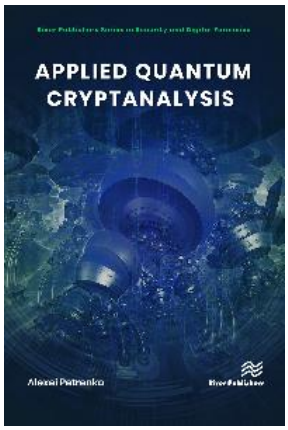

River Publishers Series in Digital Security and Forensics

Applied Quantum Cryptanalysis

Editors:
Sergei Petrenko, Innopolis University, Russia
Alexei Petrenko, Innopolis University, Russia
ISBN: 9788770227933
e-ISBN: 9788770227926
Available From: April 2023
Price: € 108.50

Description:

Today we witness an explosive growth in attention to Q-computing. Q-computing technologies, along with artificial intelligence (AI) and machine learning (ML) technologies, cloud and foggy computing, as well as technologies for collecting and streaming processing of Big Data and ETL, are constantly leading the lists of "end-to-end" information technologies for the digital economy of technologically developed countries of the world. One of the main reasons for this is the potential ability of quantum computers to solve some computational problems more efficiently than any of the most modern classical computers of the von Neumann architecture (supercomputers). The most expressive and interesting, from an applied point of view, examples of such problems are integer factorization, effectively performed by Shor's quantum algorithm, as well as record search in an unordered database, effectively solved by Grover's algorithm.

This monograph contains the best practice for solving problems of quantum cryptanalysis to improve cyber security and resilience of the digital economy. The book discusses well-known and author's software implementations of promising quantum Shor algorithms, Grover, Simon et al.

Shor's algorithm provides exponential acceleration of solving factorization problems, discrete logarithm problems (DLPs) and elliptic curve discrete logarithm problems (ECDLPs). The mentioned tasks are widely used in TLS, SSH or IPsec cryptographic applications of Internet/Intranet and IIoT/IoT networks, communication protocols based on Diffie–Hellman key agreements (dependent on the strength of the DLP or ECDLP), digital signature algorithms (DSA, ECDSA, RSA-PSS), public key encryption algorithms (El Gamal, RSA-OAEP), etc. In other words, Shor's quantum algorithm is potentially capable of violating these algorithms, and with them all the mechanisms of public-key cryptography deployed in cyberspace.

Keywords: Quantum Computers, Quantum Computing, Quantum Cryptography, Quantum Cryptanalysis, Quantum Attack, Quantum Algorithms, Logic Gates, Post-Quantum Cryptography, Post-Quantum Security.