River Publishers

Quantum Security
Building Quantum-Resilient Digital Platforms for the Future

Author: Alexey Petrenko, Innopolis University, Russia

As quantum computing advances, ensuring the resilience of critical digital ecosystems and platforms within the Data Economy has become one of today's most important scientific and technological challenges. This book examines the emerging threat that quantum computing poses to digital security and explores three complementary approaches to building quantum-resilient systems.

The first approach focuses on the development and adoption of post-quantum cryptographic primitives and electronic signatures based on mathematical problems for which no efficient classical or quantum algorithms are currently known. The second examines the design and implementation of individual quantum-resistant components and connections that provide mathematically provable levels of robustness.

The third explores a more fundamental transformation: the development and software-hardware implementation of new quantum-mechanical models for digital ecosystems and Data Economy platforms, grounded in the physical principles and laws of quantum mechanics.

Bringing these three perspectives together, the book provides a comprehensive examination of quantum resilience, from post-quantum cryptography and provably secure components to fundamentally new quantum-based architectures. It presents potential solutions to the scientific and technical challenges ahead while offering researchers, engineers, cybersecurity professionals, and technology leaders a framework for understanding and preparing for a quantum-secure digital future.

TABLE OF CONTENTS

Abstract

Introduction

Definitions, Notations, and Abbreviations

1. Development of the Concept for Ensuring Quantum Resilience of Digital Platforms of "Data Economy"

1.1. Role and Position of Blockchain as a Cross Cutting Foundational Information Technology

1.2. Relevance of Ensuring Quantum Resilience for National Blockchain Ecosystems and Platforms

1.3. Potential consumers of the developed scientific and technological results

1.4. Concept for Ensuring Quantum Resilience of National Blockchain Ecosystems and Platforms

1.5. Interrelated issues of quantum resistance in blockchain ecosystems

1.6. Key stages in addressing the scientific problem

1.7. Major Lines of Research

1. Quantum-Aware Threat Modeling for National Blockchain Platforms

2.1. Information Security Threat Model for a Typical National Blockchain Platform

2.2. Micro Model of Information Security Threats for a Typical Blockchain Platform Based on the Mathematical Apparatus of Petri Nets

2.2.1. Emerging Quantum Threats to the Security of Blockchain Ecosystems

2.2.2. Potential Malicious Actors and Cyberattack Simulation Examples

2.2.3. Evaluation of Cyber Resilience in Blockchain Ecosystems and Platforms

2.3. Micromodel of Information Security Threats to National Blockchain Ecosystems and Platforms Based on R. Kalman??s Dynamic Interrelations and the Catastrophe Theory of R. Thom and V. Arnold

1. Solutions to the Quantum Stability Analysis of National Blockchain Ecosystems and Platforms

3.1. Method for Analyzing the Quantum Stability of National Blockchain Ecosystems and Platforms

3.1.1. Problem Statement of the Study

3.1.2. Method for Assessing the Stability of Blockchain Systems

3.1.3. Quantum Cryptanalysis of Blockchain Crypto Primitives

3.1.4. Modified Quantum Cryptanalysis and Its Impact on the Operational Resilience of Blockchain Systems

3.1.5. Conclusions

3.2. Application of the Quantum Fourier Transform in Cryptology

3.2.1. Statement of the research problem

3.2.2. The proposed approach

3.2.3. Conclusions

3.3. Solving optimization problems of ensuring quantum stability of national blockchain platforms using quantum annealing

3.3.1. Basic concepts and definitions

3.3.2. Statement of the research problem

3.3.3. Solutions to optimization problems

3.3.4. Conducting an experiment

3.3.5. Conclusions

1. Solving the problems of synthesizing quantum-stable national blockchain e platforms

4.1. Algebraic algorithm of digital signature with two hidden groups

4.1.1. Properties of the Underlying Algebraic Structure

4.1.2. Assessment of Security Against Known-Signature Attacks

4.1.3. Post-quantum digital signature algorithm

4.1.4. Discussion

4.2. Method for Constructing Post-Quantum Digital Signature Algorithms with Small Public Key Sizes Based on Finite Noncommutative Associative Algebras with Two Hid

4.2.1. Definition of finite non-commutative associative algebras

4.2.2. Basic crypto primitive based on FNAA

4.2.3. Application of Chaotic Mappings for Enhanced Randomization

4.2.4. Adaptive Parameter Selection for Finite Noncommutative Associative Algebra

4.2.5. Analysis of Experimental Results and Threat Model

4.3. Typical verification equations in algebraic digital signature schemes with two hidd

4.3.1. Variants of four-dimensional FNAA assignment

4.3.2. Algorithm of the first type of digital signature

4.3.3. Algorithms of the second type of digital signature

4.3.4. Algorithms of the third type of digital signature

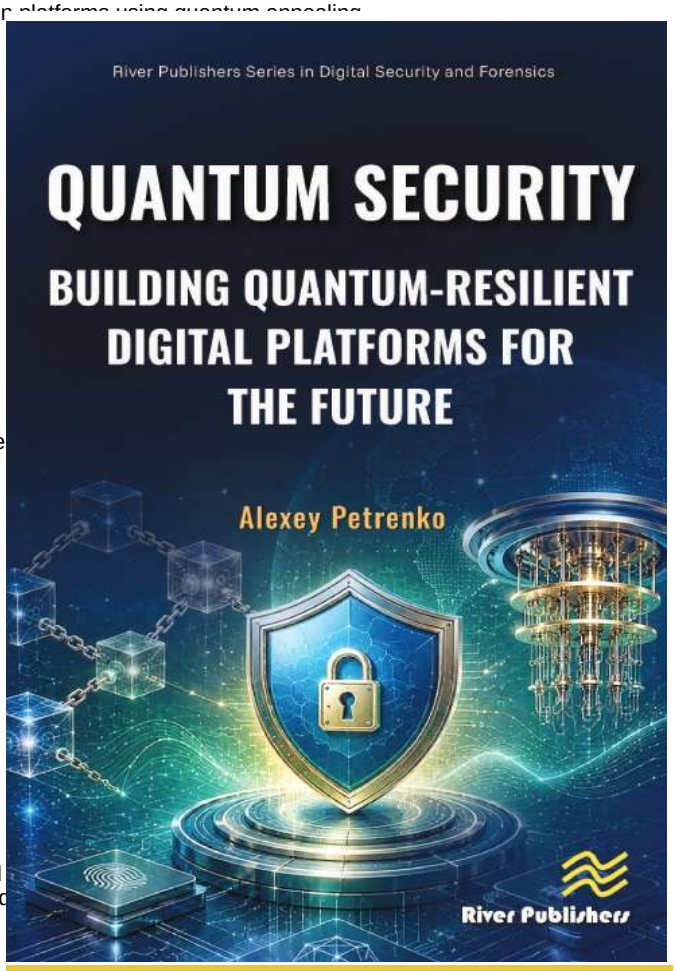
4.3.5. Discussion

Conclusion

Author information

1. Attachment.
2. Attachment
3. Attachment

D. Attachment



River Publishers Series in Digital Security and Forensics

ISBN: 9788743816409
e-ISBN: 9788743816416
Available From: February 2027
Price: € 132.11

KEYWORDS:
Quantum Security, Quantum-Resilient Digital Platforms, Blockchain and distributed ledger technology (DLT), Quantum resilience, Post-quantum cryptography, Quantum computing, Blockchain security, Cryptographic primitives, Secure digital infrastructures

www.riverpublishers.com
marketing@riverpublishers.com