EUROPEAN PATENT SPECIFICATION

EP3945678 B1

Title: Method and System for Quantum-Resistant Encryption in Industrial Control Systems

Filing Date: 15 March 2021

Publication Date: 22 September 2023

Priority Date: 16 March 2020

Patent Holder: DeepShield Systems, Inc.

TECHNICAL FIELD

[0001] The present invention relates to cryptographic systems and methods, specifically to quantum-resistant encryption protocols for securing industrial control system (ICS) communications and operational technology (OT) networks against both classical and quantum computing threats.

BACKGROUND

[0002] With the advancement of quantum computing capabilities, traditional encryption methods based on factorization and discrete logarithm problems are becoming increasingly vulnerable. Industrial control systems require encryption methods that maintain security against both current and future quantum computing capabilities while meeting strict latency and processing requirements of real-time industrial operations.

SUMMARY OF INVENTION

[0003] The invention provides a novel lattice-based encryption method specifically optimized for industrial control system environments. The method implements a hybrid approach combining modified NTRU (N-th degree TRUncated polynomial ring) lattices with proprietary error correction mechanisms designed for high-reliability industrial communications.

DETAILED DESCRIPTION

1. System Architecture

[0004] The encryption system comprises:

a) A key generation module implementing Ring-LWE (Learning With Errors) algorithms

b) An industrial protocol adaptation layer

c) A real-time optimization engine

d) Hardware-accelerated polynomial multiplication units

2. Key Generation Process

[0005] The system generates encryption keys through:

1. Generation of a prime modulus p specific to the ICS protocol requirements

2. Creation of polynomial rings R = Z[X]/(X^n + 1) where n is a power of 2

3. Implementation of error sampling using a discrete Gaussian distribution

4. Application of proprietary error correction specific to industrial protocols

3. Encryption Method

[0006] The encryption process comprises:

1. Message encoding using industrial protocol-specific parameters

2. Application of lattice-based transformations

3. Integration with existing ICS security architectures

4. Real-time performance optimization for sub-millisecond latency

CLAIMS

A method for quantum-resistant encryption in industrial control systems, comprising:

a) Generating encryption keys using Ring-LWE algorithms optimized for ICS protocols

b) Implementing lattice-based transformations with industrial protocol adaptation

c) Applying error correction specific to OT network requirements

d) Maintaining deterministic performance within ICS timing constraints

The method of claim 1, wherein the lattice-based transformations include:

a) Modified NTRU operations

b) Discrete Gaussian sampling

c) Polynomial multiplication optimization

d) Protocol-specific parameter selection

A system implementing the method of claim 1, comprising:

a) Hardware-accelerated cryptographic modules

b) Industrial protocol interfaces

c) Real-time optimization engines

d) Key management infrastructure

ABSTRACT

A quantum-resistant encryption method and system for industrial control systems implementing lattice-based cryptography with specific optimizations for ICS protocols. The invention provides post-quantum security while maintaining deterministic performance requirements of industrial operations through novel combinations of Ring-LWE algorithms and proprietary error correction mechanisms.

LEGAL NOTICES

Inventors:

- Dr. Elena Rodriguez
- James Morrison
- Dr. Marcus Chen

Patent Representatives:

Blackwood & Associates LLP
1234 Technology Drive
Boston, MA 02110

European Patent Attorney:

Schmidt & Weber
Patentanw lte
M nchen, Germany

Filed and recorded at the European Patent Office

Reference Number: EP3945678

Classification: H04L 9/0618, H04L 9/0869

Priority Claims: US 63/124,891