EUROPEAN PATENT SPECIFICATION

EP3912345 B1

QUANTUM-RESISTANT ENCRYPTION MODULE FOR INDUSTRIAL CONTROL SYSTEMS

Patent Holder: DeepShield Systems, Inc.

Filing Date: March 15, 2022

Publication Date: September 21, 2023

Priority Date: March 16, 2021 (US 63/159,876)

TECHNICAL FIELD

[0001] The present invention relates to quantum-resistant cryptographic systems and methods for securing industrial control system (ICS) communications, particularly in critical infrastructure environments. More specifically, the invention provides a novel encryption module implementing post-quantum cryptographic algorithms optimized for low-latency SCADA networks and operational technology (OT) environments.

BACKGROUND

[0002] With the advancement of quantum computing capabilities, traditional cryptographic methods based on RSA and elliptic curve cryptography face increasing vulnerability to quantum attacks. Industrial control systems, particularly in critical infrastructure, require robust encryption solutions that maintain security against both classical and quantum computing threats while meeting strict operational latency requirements.

[0003] Prior attempts to implement quantum-resistant encryption in ICS environments have been limited by computational overhead and integration challenges with legacy SCADA protocols.

SUMMARY OF INVENTION

[0004] The present invention provides a quantum-resistant encryption module specifically designed for industrial control system environments. The module implements a novel lattice-based cryptographic algorithm optimized for:

a) Sub-millisecond encryption/decryption operations

b) Compatibility with common SCADA protocols including Modbus, DNP3, and IEC 61850

c) Hardware-accelerated implementation on standard ICS gateway devices

d) Minimal key size and bandwidth overhead

e) Integration with existing public key infrastructure (PKI) systems

DETAILED DESCRIPTION

[0005] The encryption module comprises:

1. Core Cryptographic Components

1 A primary lattice-based encryption engine implementing the DS-LWE (DeepShield Lattice with Weighted Errors) algorithm with the following parameters:

- Lattice dimension: n = 1024
- Modulus q = 40961
- Error distribution: discrete Gaussian with = 3.2

2 Key generation subsystem utilizing hardware entropy sources for quantum-resistant key pairs

3 Protocol adaptation layer supporting:

- Real-time protocol encapsulation
- Session key establishment
- Perfect forward secrecy

2. Implementation Architecture

1 Hardware acceleration components:

- Dedicated polynomial multiplication unit
- Optimized number theoretic transform (NTT) implementation
- Parallel processing elements for lattice operations

2 Software stack:

- Lightweight runtime environment
- Protocol handlers for industrial protocols
- Key management interface
- Monitoring and logging subsystem

CLAIMS

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

a) Generating cryptographic keys using the DS-LWE algorithm

b) Establishing secure sessions between ICS components

c) Encrypting control messages with sub-millisecond latency

d) Maintaining backward compatibility with existing protocols

The method of claim 1, wherein the encryption process maintains deterministic timing characteristics suitable for real-time industrial applications.

An apparatus implementing the method of claim 1, comprising:

a) A hardware security module

b) Protocol adaptation interfaces

c) Key management subsystem

d) Monitoring and logging capabilities

INDUSTRIAL APPLICABILITY

[0006] The invention provides immediate practical application in:

- Critical infrastructure protection
- Industrial automation systems
- Power generation and distribution networks
- Maritime control systems
- Manufacturing operations

PATENT OWNER DETAILS

Assignee: DeepShield Systems, Inc.

Inventors:

- Rodriguez, Elena
- Morrison, James
- Chen, Marcus

Address for Service:

DeepShield Systems, Inc.

1000 Technology Drive

Wilmington, DE 19801

United States

LEGAL REPRESENTATIVES

European Patent Attorneys:

Schmidt, Weber & Associates

K nigsallee 92

40212 D sseldorf

Germany

Reference Number: DSS-QR-2022-EP01

[End of Document]