Post Quantum Cryptography: A Comprehensive Overview of Quantum Resistant Algorithms

Emirhan Altunel

December 29, 2024

Abstract

With the advent of quantum computing, current cryptographic algorithms, such as RSA and ECC, will no longer provide adequate security against quantum attacks. This paper explores the need for quantum resistant cryptographic algorithms and presents an overview of the proposed algorithms for post quantum cryptography. We will also compare these algorithms based on their security, efficiency, and practicality for various applications.

Contents

1 Introduction

Quantum computing presents both an opportunity and a challenge to modern cryptography. The development of quantum computers capable of solving problems much faster than classical computers threatens to break widely used cryptographic algorithms, including RSA, Diffie Hellman, and Elliptic Curve Cryptography (ECC). As quantum computing continues to advance, it is essential to develop cryptographic systems that are secure against quantum attacks. This field is known as post quantum cryptography (PQC), and the National Institute of Standards and Technology (NIST) has been leading an effort to standardize quantum resistant algorithms.

This report provides an overview of the quantum resistant algorithms proposed in the NIST Post Quantum Cryptography Standardization project, comparing their strengths, weaknesses, and suitability for different use cases.

2 Post Quantum Cryptography Overview

Post quantum cryptography refers to cryptographic algorithms that are secure against the capabilities of quantum computers. The most commonly discussed quantum algorithms that threaten existing cryptographic systems are:

- **Shor's Algorithm**: This algorithm allows quantum computers to efficiently solve problems such as factoring large numbers and computing discrete logarithms, which form the basis of many classical cryptographic schemes.

- **Grover's Algorithm**: This algorithm provides a quadratic speedup for searching an unsorted database, which affects the security of symmetric key cryptography.

To counteract these quantum threats, several families of quantum resistant algorithms have been proposed, and NIST has initiated a standardization process to evaluate and select candidates for post quantum cryptographic standards.

3 Quantum Resistant Cryptographic Algorithm Categories

The proposed quantum resistant cryptographic algorithms can be grouped into several categories:

- **Lattice based Cryptography**: These algorithms rely on the hardness of lattice problems, which are believed to be resistant to quantum attacks. Examples include the Learning With Errors (LWE) problem and the Shortest Vector Problem (SVP).

- **Code based Cryptography**: These schemes are based on error correcting codes and have been studied for several decades as candidates for post quantum cryptography. McEliece is a well known example.

- **Multivariate Polynomial Cryptography**: This approach involves solving systems of multivariate polynomials over finite fields, a problem that is difficult for both classical and quantum computers.

- **Hash based Cryptography**: These algorithms are based on hash functions and are primarily used for digital signatures. The Merkle signature scheme is a representative example.

- **Isogeny based Cryptography**: This category involves elliptic curve isogenies and is a relatively new area of study in post quantum cryptography.

4 Selected NIST Candidates and Their Comparison

NIST has narrowed down its candidates to the following families, which are currently under evaluation:

4.1 Lattice based Algorithms

- **Kyber**: A key encapsulation mechanism (KEM) based on the hardness of the Module LWE problem. It is considered to be highly efficient and secure.

- **NTRU**: A public key encryption and KEM scheme based on polynomial rings, offering high efficiency and compact ciphertexts.

- **FrodoKEM**: Based on the Learning With Errors (LWE) problem, it is designed to avoid potential vulnerabilities in structured lattice based schemes.

4.2 Code based Algorithms

- **McEliece**: A public key encryption scheme based on the hardness of decoding random linear codes. It has a long history and has been shown to be quantum resistant, but its key sizes are large.

4.3 Hash based Algorithms

- **XMSS (eXtended Merkle Signature Scheme)**: A stateful hash based signature scheme that is proven to be secure against quantum attacks.
- **SPHINCS+**: A stateless hash based signature scheme that offers high security and scalability, though it has larger signatures than XMSS.

4.4 Multivariate Polynomial Cryptography

- **Rainbow**: A multivariate signature scheme based on the problem of finding solutions to systems of multivariate polynomials. It has efficient signature generation and verification but larger key sizes.

4.5 Isogeny based Cryptography

- **SIKE (Supersingular Isogeny Key Encapsulation)**: A KEM based on supersingular elliptic curve isogenies. While promising in terms of security and compactness, it is still considered experimental.

5 Comparison of Post Quantum Cryptographic Algorithms

The comparison of these algorithms can be made based on several factors:

- **Security**: All the algorithms aim to be secure against quantum adversaries, but their security assumptions vary. For instance, lattice based schemes are believed to offer the strongest security guarantees.
- **Efficiency**: The computational and storage requirements of these algorithms vary widely. Lattice based schemes like Kyber are efficient in both key generation and encryption, while code based schemes like McEliece require large keys.

- **Practicality**: Algorithms such as NTRU and Kyber are already being considered for real world applications, while others like SIKE and Rainbow are still being analyzed for their feasibility in practical deployments.
- **Signature Size and Key Size**: Hash based schemes have relatively large signature sizes, which may limit their practicality for certain applications.

6 Conclusion

As quantum computing continues to progress, the need for quantum resistant cryptography becomes more pressing. The NIST Post Quantum Cryptography Standardization project is making significant progress in identifying algorithms that can withstand quantum attacks while providing reasonable performance in practical settings. While no algorithm is perfect, a combination of lattice based, code based, and hash based schemes offers promising candidates for securing data in the post quantum era.