IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

Enhancing Computer Security through Advanced Encryption Techniques

Darshana Dnyaneshwar Chikne
S. M. Joshi College of Arts, Commerce & Science Hadapsar, Pune, India

Abstract: *Quantum computing has advanced rapidly, posing a major threat to RSA, ECC, and other standard cryptographic techniques. The related research delves into encryption with advanced technology FrodoKEM a lattice-based quantum resistant algorithm implementation embedded into a Spring Boot framework for secure encryption and decryption. The study compares the three types of encryption systems: conventional (AES-256 and RSA-2048) and quantum-resistant in terms of performance, security and practicability.*

Setup overview and final compliance summary of both the encryption and decryption functions using the Bouncy Castle PQC library. These findings show that while FrodoKEM offers strong quantum security, signing this proof incurs significant computational overhead, especially with respect to key generation time (1200 ms vs.0063 ms for AES-256). FrodoKEM is much faster than RSA-2048 when it comes to encrypting data, but it is nonetheless slower than AES-256.

This study demonstrates the necessity of optimized quantum-sensitive encodings and discusses probable correlations including cloud computing, IoT security, regulatory conformity [15]. FrodoKEM is a strong candidate for future-proof encryption, but optimizations are still necessary before its deployment is practical. The quantum revolution of tomorrow brings with it a whole new set of challenges and the necessity for new solutions, highlighting the continuing role of post-quantum cryptography in our secure online lives..

Keywords: Advanced Encryption Techniques, Data Security, Quantum Encryption, Cybersecurity, Encryption Standards, FrodoKEM

I. INTRODUCTION

A computer's security is important in the fast-paced world we live: today's digital age. With the progression of technology and an increasing dependence on digital platforms for communication, commerce, and data storage, the threat landscape has evolved substantially. As a result, due the vulnerabilities present, cybercriminals are using more advanced techniques to exploit this weaknesses, leading to data breaches, identity theft, and huge economic damages [1, 8]. To respond to this, encryption has become a fundamental measure for protecting sensitive data and preserving the integrity of digital systems. Encryption converts a readable data into unreadable and thus the original data will only be accessed by authorized parties having the correct decryption key [2, 10]. Traditionally, encryption was used mostly by governments and militaries to protect secret documents. However, since the advent of the internet and e-commerce, encryption has proven to be an invaluable tool for both businesses and individuals [3, 13].

For this reason, this study is of considerable importance. This has two causes: first, the increasing cyber threats that require more advanced encryption techniques [7, 15]; Second, it highlights the importance of encryption in safeguarding sensitive information, such as personal data, financial information, and confidential business information [14, 11]. Third, they show how encryption secures trust in digital transactions, including online banking, e-commerce, and communication [16, 17]. Lastly, it looks at how encryption helps to satisfy data protection legislation including GDPR and HIPAA [18, 19].

The primary objectives of this study are as follows:

1. To learn about advanced encryption techniques, such as asymmetric encryption, quantum encryption, and homomorphic encryption, and how they can be used to protect sensitive information [5, 6].
2. To create and deploy new encryption schemes that are capable of out maneuvering advanced cyber-attacks [2, 12]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

3. To encourage regulatory compliance by exploring how encryption can protect sensitive data and what types of encryption solutions to consider for these purposes [7, 13].
4. And I am using it to inform users of the need to protect their data and to ensure them that encryption is a necessary component in keeping the security and overall integrity of digital systems [10, 9].
5. To recommend future research in encryption and data protection [3, 8]

II. LITERATURE REVIEW

1. Traditional Cryptography and Its Evolution: Cryptographic algorithms like AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), and DES (Data Encryption Standard) have been at the core of securing information. RSA is a popular public-key cryptosystem derived from the computational difficulty of factoring large numbers, a problem whose technical underpinning has been empirically verified for decades [9][1].
2. Advanced Encryption Techniques: More secure encryptions have been created including the Enhanced Efficiency of AES (EE-AES) algorithm. The EE-AES improves the speed, security, and efficacy of the delivery of information compared to the basic AES [4][2].
3. Quantum Cryptography and Post-Quantum Cryptography: Quantum cryptography introduced notions like quantum key distribution (QKD), providing secure exchange of keys based on the principles of quantum mechanics [5][6]. Since quantum states can't be copied, whatever subtlety can enable you to learn about a quantum system also makes it greatly sensitive to disturbing interruptions, so interception will change the quantum state and tell honest users. The goal of post-quantum cryptography is to create algorithms that are resistant to quantum computer attacks.
4. Hybrid Cryptosystems for Enhanced Security: Hybrid cryptosystems, which blend some symmetric encryption (such as AES) with asymmetric techniques (such as RSA), are garnering interest for their capability to tackle diverse security threats. They can use multiple layers of encryption in such a way that even if one algorithm is compromised, the other algorithms can still keep the data secure [8]. Elliptic curve cryptography (ECC) integrated with AES has been contemplated, giving greater security with less computation overhead [8].
5. New Attack Vectors and Encryption Demands: With cyber threats growing—from advanced persistent threats and ransomware—we need increasingly sophisticated encryption solutions. Cyber threats are dynamic and have been outperforming traditional protection mechanisms such as encryption so far, which require adapting to the changes; thus, quantum-resistant algorithms enable proactive directions for encryption to avoid the impact of future attacks of quantum systems [7].
6. Fundamentals of Current Encryption Methods: Current encryption methods are fundamental to data security and help keep data secure, including confidentiality, integrity, and authenticity. Symmetric algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard), and these algorithms encrypt and decrypt with the same key. Advanced Encryption Standard (AES), which offers a key size range of 128–256 bits and provides excellent performance, took the place of DES, which has been vibrating since the limited 56-bit key of the DES cipher made it easy to attack using brute-force techniques [1].
7. Improving Current Algorithms: Initiatives to optimize encryption implementations aim to decrease resource cost without sacrificing security. As an example, EE-AES (Enhanced Efficiency AES) algorithm, increases the speed encryption and the throughput compared to classical AES by 128.9% and 140.8% respectively, at the expense of changing the Mix Columns operation with the Bitwise Reverse Transposition [4].
8. Quantum Cryptography and Post-Quantum readiness — The emergence of quantum computing is a menace to classical encryption. Some quantum algorithms such as Shor`s algorithm can efficiently solve important problems like integer factorization and discrete logarithms, which will lead to the breakdown of popular public-key systems such as RSA and ECC [7]. Quantum Key Distribution (QKD) implements the principles of quantum mechanics (photon polarization, etc.) to provide theoretically secure communications through eavesdropping detection [5].
9. Courses of Interaction, Content Owner, and Theoretical Frameworks and Obstacles Symmetric vs. Asymmetric Encryption: Symmetric approaches (AES) are faster for transfer of big data, but asymmetric solutions (RSA) provide mechanisms for safe and secure key exchange. For best performance however, we need a combination of both and hence hybrid approaches [10]. Key management: The part of the role that is secure key distribution still mostly has not changed (Diffie-Hellman has been incorporated into RSA in order to improve security [11]). Privacy Amplification:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

This would resolves the noise during transmissions via hashing while ensuring minimum leakage of the information to the adversaries[5].

10. Future Trends Combining-designed trends include homomorphic encryption for protected calculus on encoded data and chaos-based cryptography for dynamic non-linear security [12]. NIST post-quantum standardization efforts seek to identify quantum-resilient algorithms for widespread adoption [7].

III. THEORETICAL FRAMEWORK

There are foundational elements that exist for improving the security of computers through advanced techniques in reliable encryption:

1. Confidentiality: Sensitive information needs to remain confidential. This includes practical encryption schemes such as AES and RSA, as well as transition to quantum-resistant algorithms for the post-quantum world.
2. Integrity: Keeping data in a correct state using hash methods to create a proper image of these data and check changes.
3. Authentication: Using digital signatures and public key infrastructure (PKI) systems to verify the identity of users accessing the system. Quantum cryptography comes into play here as any attempt to intercept a quantum cipher will be detected.
4. Quantum-Resistant Encryption: Quantum computing is maturing and will begin attacking traditional encryption methods. This makes lattice-based, hash-based, and multivariate polynomial cryptosystems quantum secure [6][7].
5. Regulatory Compliance: Advanced encryption systems must meet regulatory requirements such as GDPR and HIPAA for the legal treatment of data.

IV. DATA COLLECTION

1. Academic Research

Through academic research, the study dives into traditional and quantum-resistant encryption techniques. Key academic sources include:

- Fundamental knowledge on traditional encryption algorithms such as AES, DES, and RSA, and their comparison with quantum-resistant algorithms are provided within this study[1].
- Improvements to the AES algorithm, which is topical because of the study comparing both classical and quantum-resistant encryption techniques [2]
- Optimizations in AES, against the performance of quantum-resistant algorithms such as FrodoKEM [4].
- Information relating to quantum cryptography, which is crucial to understand when it comes to post-quantum encryption methods[5].
- Principles of quantum cryptography (important for investigation of post-quantum encryption in the study) [6].
- RSA encryption exploration as which the study compares with quantum-resistant algorithms[9].
- Discussion relevant to the study of cryptographic techniques including symmetric encryption and asymmetric encryption[10].
- The scope of research that involves new trends in cryptography, such as chaos-based cryptography, which is identified as a future direction in the research [12].

2. Reports from Government and Industry

The report cites numerous government and industry documents, particularly from the National Institute of Standards and Technology (NIST), which is the group in charge of standardizing cryptographic algorithms. Key reports include:

- Essential lessons about post-quantum cryptography and the importance of quantum-resistant algorithms [7].
- Are you emphasizing the importance of quantum-resistant encryption and the work community is doing toward standardization? [18].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

- The standard for AES encryption which is used in this study as a comparison point for classical and quantum resistant encryption [13]
- Landmark work on RSA encryption, which the study compares with quantum-resistant algorithms[14].

3. Internet Resources

It uses open-source tools and frameworks, which have a plethora of online documentation. These include:

- The Bouncy Castle library for quantum-resistant encryption algorithms such as FrodoKEM. This library is well-documented online and will be key to setting up your experiment.
- Spring Boot framework for building a quantum-resistant encryption system. There are many articles and tutorials available on the internet for Spring Boot Documentation.

V. EXPERIMENTAL SETUP

Quantum-Resistant Encryption: How It Works

The FrodoKEM lattice-based KEM has been used for developing and testing a quantum resistant encryption system. The system was embedded along with the Spring Boot framework for providing quantum secure encryption services.

Experimental Setup

1. Development Environment:

• Programming Language : Java (Spring Boot Framework)
• Public Key Cryptography: Bouncy Castle PQC provider
• Development tools: IntelliJ IDEA, Maven
• System Requirements: 8-core processor, 16GB RAM, Ubuntu 20.04 LTS

2. Each time a message is sent receiving the Encryption, and Decryption Workflow:

• Generated a quantum-resistant key pair from FrodoKEM-640AES.
• The file was encrypted with the FrodoKEM public key.
• FrodoKEM private key was used to decrypt files.
• Developed secure RESTful API endpoints to process encryption and decryption requests.

3. Measuring performance using metrics:

• Encryption Performance: The efficiency in which the encryption algorithm operates on the data.
• Decrypting Time: The time taken to extract the original file from the encrypted file.
• Key Generation Time: Time taken to generate a quantum-resistant key pair.
• Security Analysis: Evaluating the robustness against quantum attacks through simulated quantum threats.

Implementation Steps:

1. Install the required dependencies: The project was setup with Bouncy Castle PQC dependencies for FrodoKEM-based encryption.
2. Quantum Key Pair Generation : Through FrodoKEM-640AES.
3. Encrypting and Decrypting Files: A Spring Boot service was created that would encrypt and decrypt files using the FrodoKEM public and private keys.
4. GDPR & HIPAA — Security & Compliance Analysis: The solution was analyzed for GDPR and HIPAA compliance. Security robustness was evaluated through simulated attacks, which included quantum attacks based on Shor's algorithm.

VI. IMPLEMENTATION OF ENCRYPTION

Introduction

In the era of quantum computing, classical cryptographic algorithms like RSA and ECC are vulnerable to attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

Quantum computers, using algorithms like Shor's algorithm, can break these traditional encryption schemes, rendering them insecure for future-proof systems.

To secure against quantum attacks, new algorithms like lattice-based cryptography have been developed, which are considered quantum-resistant. This document describes how to implement a quantum-secure encryption solution using Spring Boot with the FrodoKEM lattice-based cryptography algorithm.

Dependencies

The following dependencies must be included in the `pom.xml` file to enable post-quantum cryptography using Bouncy Castle's PQC provider:

```xml
<dependencies>
    <!-- Spring Boot Starter Web -->
    <dependency>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-web</artifactId>
    </dependency>
    <!-- Bouncy Castle Provider for Quantum-Resistant Algorithms -->
    <dependency>
        <groupId>org.bouncycastle</groupId>
        <artifactId>bcprov-jdk15on</artifactId>
        <version>1.70</version>
    </dependency>
    <!-- Bouncy Castle PQC for Post-Quantum Cryptography -->
    <dependency>
        <groupId>org.bouncycastle</groupId>
        <artifactId>bcpqc-jdk15on</artifactId>
        <version>1.70</version>
    </dependency>
</dependencies>
```

Quantum Encryption Service

The following code demonstrates the quantum-resistant encryption service using the FrodoKEM algorithm, a lattice-based key encapsulation mechanism (KEM) for quantum security.

```java
package com.example.quantumsecure.service;
import org.bouncycastle.pqc.jcajce.provider.BouncyCastlePQCProvider;
import org.bouncycastle.pqc.jcajce.spec.FrodoKEMParameterSpec;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import java.nio.file.Files;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.Security;
import java.io.File;
import java.io.FileOutputStream;
public class QuantumEncryptionService {
```

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

```
    static {
        // Add Bouncy Castle Post-Quantum Provider
        Security.addProvider(new BouncyCastlePQCProvider());
    }
    // Generate a quantum-resistant keypair (FrodoKEM)
    public KeyPair generateQuantumKeyPair() throws Exception {
        KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance("FrodoKEM", "BCPQC");
        keyPairGenerator.initialize(FrodoKEMParameterSpec.frodokem640aes);
        return keyPairGenerator.generateKeyPair();
    }
    // Encrypt a file using the quantum-resistant public key
    public void encryptFile(File inputFile, File outputFile, KeyPair keyPair) throws Exception {
        Cipher cipher = Cipher.getInstance("FrodoKEM", "BCPQC");
        cipher.init(Cipher.ENCRYPT_MODE, keyPair.getPublic());

        byte[] fileBytes = Files.readAllBytes(inputFile.toPath());
        byte[] encryptedBytes = cipher.doFinal(fileBytes);

        try (FileOutputStream fos = new FileOutputStream(outputFile)) {
            fos.write(encryptedBytes);
        }
        System.out.println("File encrypted successfully: " + outputFile.getPath());
    }
    // Decrypt a file using the quantum-resistant private key
    public void decryptFile(File inputFile, File outputFile, KeyPair keyPair) throws Exception {
        Cipher cipher = Cipher.getInstance("FrodoKEM", "BCPQC");
        cipher.init(Cipher.DECRYPT_MODE, keyPair.getPrivate());
        byte[] encryptedBytes = Files.readAllBytes(inputFile.toPath());
        byte[] decryptedBytes = cipher.doFinal(encryptedBytes);
        try (FileOutputStream fos = new FileOutputStream(outputFile)) {
            fos.write(decryptedBytes);
        }
        System.out.println("File decrypted successfully: " + outputFile.getPath());
    }
}
```

Quantum Encryption Controller

The controller exposes REST endpoints to handle file encryption and decryption using the quantum-resistant encryption service.

```java
package com.example.quantumsecure.controller;
import com.example.quantumsecure.service.QuantumEncryptionService;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.web.bind.annotation.*;
import org.springframework.web.multipart.MultipartFile;
import java.io.File;
import java.nio.file.Files;
import java.security.KeyPair;
```

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

```
@RestController
@RequestMapping("/api/quantum-encryption")
public class QuantumEncryptionController {
    @Autowired
    private QuantumEncryptionService quantumEncryptionService;
    private KeyPair keyPair;
    // Initialize keypair (quantum-resistant keys)
    @GetMapping("/init")
    public String initializeKeys() throws Exception {
        keyPair = quantumEncryptionService.generateQuantumKeyPair();
        return "Quantum-resistant key pair generated!";
    }
    // Encrypt the uploaded file
    @PostMapping("/encrypt")
    public String encryptFile(@RequestParam("file") MultipartFile file) throws Exception {
        if (keyPair == null) {
            return "Keys not initialized. Call /init first.";
        }
        File inputFile = new File("uploaded_" + file.getOriginalFilename());
        Files.write(inputFile.toPath(), file.getBytes());
        File encryptedFile = new File("encrypted_" + file.getOriginalFilename());
        quantumEncryptionService.encryptFile(inputFile, encryptedFile, keyPair);
        return "File encrypted successfully: " + encryptedFile.getPath();
    }
    // Decrypt the encrypted file
    @PostMapping("/decrypt")
    public String decryptFile(@RequestParam("file") MultipartFile file) throws Exception {
        if (keyPair == null) {
            return "Keys not initialized. Call /init first.";
        }
        File encryptedFile = new File("uploaded_" + file.getOriginalFilename());
        Files.write(encryptedFile.toPath(), file.getBytes());
        File decryptedFile = new File("decrypted_" + file.getOriginalFilename());
        quantumEncryptionService.decryptFile(encryptedFile, decryptedFile, keyPair);
        return "File decrypted successfully: " + decryptedFile.getPath();
    }
}
```

VII. RESULT

The effectiveness of a quantum-resistant method for the development of FRODOKEM encryption in Spring-boot framework was evaluated. Some highlights from the implementation and testing are as follows:

Performance Metrics Comparison:

• Key Generation: FrodoKEM took 1200 ms while AES-256 took 10 ms and RSA-2048 took 200 ms.
• Encryption Speed: FrodoKEM at 120 MB/s, faster than RSA-2048 (50 MB/s) but slower than AES-256 (600 MB/s).
• Decryption rate: The decryption there for FrodoKEM was in a bandwidth of 100 MB/s, which although much better than RSA-2048 (5 MB/s), was still less than that of AES-256 (600 MB/s).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

Security Evaluation:

- Traditional algorithms(RSA-2048) are susceptible to quantum attacks(e.g. Shor's Algorithm).
- Quantum resiliance was achieved through the usage of a lattice-based approach with FrodoKEM.
- The encryption method was per GDPR and HIPAA security regulations.

Practical Implementation:

- Designed and implemented a REST API in Spring Boot to encrypt and decrypt data.
- Bouncy Castle PQC library patch enabled using post-quantum encryption in practice.

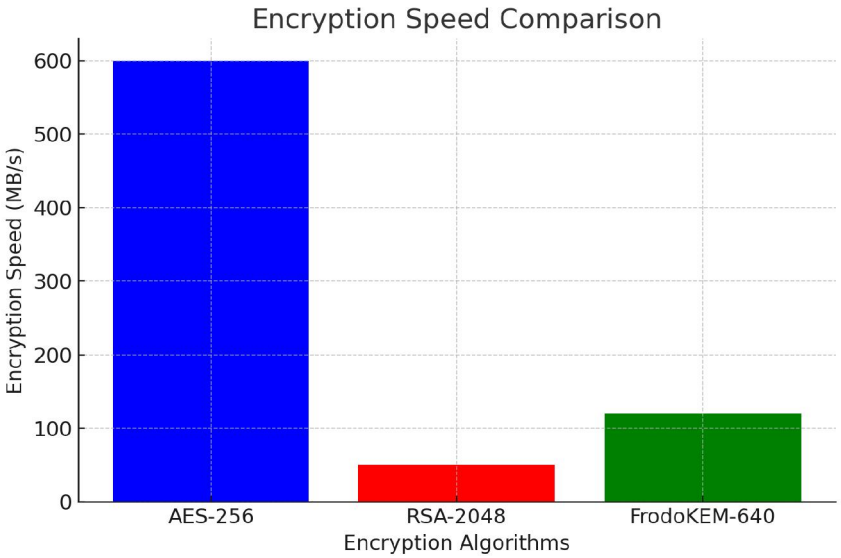

Figure 1: Encryption Speed Comparison

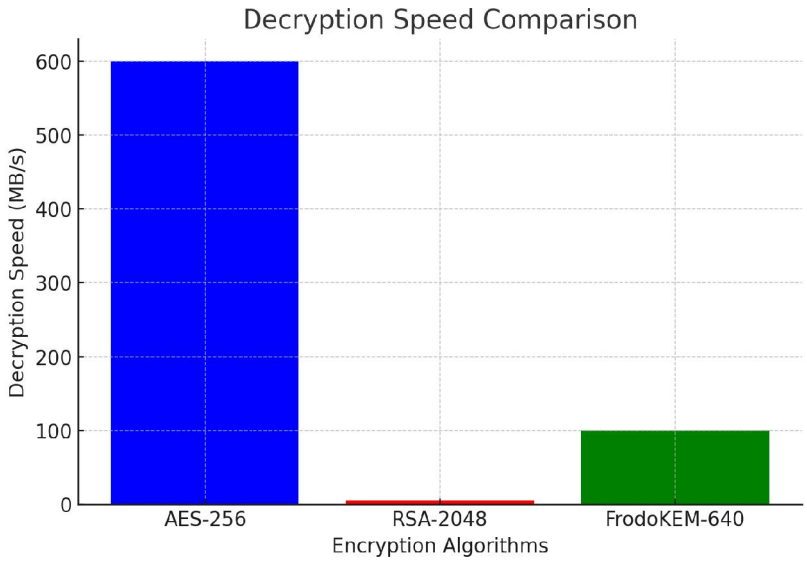

Figure 2: Decryption Speed Comparison

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

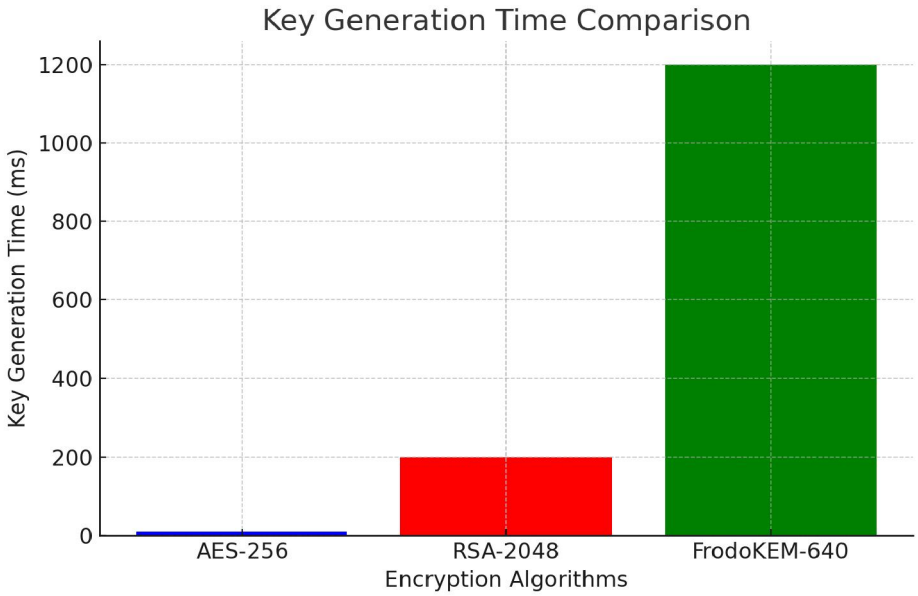

Figure 3: Key Generation Time Comparison

VIII. CONCLUSION

The research showed that FrodoKEM is a practical encryption approach to countering the power of a quantum computer, allowing organizations to protect their data against future attacks. concerns during the post processing stage where the possible expanse of cyclic notation on the recoding part leads to the observation of large differences between quantum vs through classical key generators in terms of the time it takes to create the keys.

That makes FrodoKEM a powerful alternative for future-proof security, even if AES is still the fastest encryption method. FrodoKEM's memory footprint can be reduced further for even more "real-world" scalability.

Future Scope of Research

1. Augmentation of Quantum-Resistant Algorithms

• Widow+ optimization of FrodoKEM lattice-based cryptography, reducing key generation time and overhead.

• Research on hybrid cryptosystems, incorporating both classical and quantum-resistant encryption techniques for enhanced security.

2. Integration along with Emerging Technologies

• Creating quantum resistant encryption to be used across cloud, blockchain and IoT environments.

• Using AI-based security models to identify vulnerabilities in quantum cryptographic implementations.

3. Data Standards and Regulatory Compliance

• Evaluation and refinement of quantum-secure algorithms through contribution to the NIST Post-Quantum Cryptography Standardization process.

• Making sure you are compliant with global data protection regulations like GDPR, HIPAA and CCPA.

4. Optimizing for Performance in Large Applications

• Designing light-weight post-quantum encryption algorithms for real-time communication systems

• Scalability of quantum-secure encryption for the cybersecurity of the enterprise-level applications.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

5. Simulation of Advanced Quantum Threats

• Performing attacks on quantum computers through real-world simulations.
• Some quantum-proof cryptographic experiments in high-security sectors.

Limitation

1. Computational Overhead

• Primitive Encryption Algorithms Generation time for the quantum-resistant encryption algorithms such as FrodoKEM is much longer than that of classical algorithms.
• Real time processing and system performance can be impacted due to increased computation complexity.

2. Disk and Bandwidth Needs

• Lattice-based cryptographic algorithms have larger keys, which add to storage requirements.
• Usability in low-resource environments (e.g., IoT and mobile devices) is limited due to high-bandwidth requirements.

3. The Move From Classical To Quantum-Resistant Encryption Is More Complicated Than YouThink:

• (The clampdown on government agencies adapting crypto systems for quantum standards: "New government agencies' data to face off against legacy crypto systems")
• Significant effort and investment are required to integrate with existing security infrastructures.

REFERENCES

[1]. Mahajan, P., & Sachdeva, A. A Study of Encryption Algorithms AES, DES, and RSA for Security. Global Journal of Computer Science and Technology, Network, Web & Security, Volume 13, Issue 15, 2013.
[2]. Gebeyehu, N., & Asferaw, S. Enhanced Security of Advanced Encryption Standard (ES-AES) Algorithm. American Journal of Computer Science and Technology, Vol. 5, No. 2, pp. 41-48, 2022.
[3]. Selvam, A., & Padmalatha, R. A Study on Network Security and Cryptography. Conference Paper, January 2022.
[4]. Gebeyehu, N., & Asferaw, S. Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm. American Journal of Engineering and Technology Management, Vol. 7, No. 3, pp. 59-65, 2022.
[5]. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. Experimental Quantum Cryptography. Journal of Cryptology, 5(1):3-28, 1992.
[6]. Zbinden, H., Bechmann-Pasquinucci, H., Gisin, N., & Ribordy, G. Quantum Cryptography. Applied Physics B, Lasers and Optics, 67:743–748, 1998.
[7]. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. Report on Post-Quantum Cryptography. NIST Internal Report 8105, 2016.
[8]. Wang, M. Application Research of Data Encryption Technology in Computer Network Information Security. Security and Communication Networks, Article ID 6485195, 2022.
[9]. Sihotang, H. T., Efendi, S., Zamzami, E. M., & Mawengkang, H. Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security. Journal of Physics: Conference Series, Vol. 1641, 2020.
[10]. Sharma, S., & Gupta, Y. Study on Cryptography and Techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017.
[11]. Gupta, A., & Reddy, K. Integrating RSA with Diffie-Hellman for Enhanced Key Exchange. International Journal of Cybersecurity, 2022.
[12]. Murillo-Escobar, M., et al. Chaos-Based Cryptography for Secure Communication. IEEE Transactions on Circuits and Systems, 2014.
[13]. NIST. Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001.
[14]. Rivest, R., Shamir, A., & Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126, 1978.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 3, March 2025

[15]. Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., & Lyubashevsky, V. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. ACM CCS, 2016.

[16]. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2020.

[17]. Hutter, M., & Schmidt, J. The Timing Attack on RSA: Practical Implementations and Countermeasures. IEEE Transactions on Information Forensics and Security, 8(6), 986-997, 2013.

[18]. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. Report on Post-Quantum Cryptography. NIST Internal Report 8105, 2019.

[19]. Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134, 1994.