A Comparative Analysis of Post-Quantum and Classical Cryptography using liboqs

1. Introduction

The advent of practical quantum computing poses a significant threat to the security of modern digital communications. Shor's algorithm, a quantum computing algorithm, can efficiently solve the integer factorization and discrete logarithm problems, which are the mathematical foundations of today's most widely used public-key cryptosystems, such as RSA and Elliptic Curve Cryptography (ECC). The eventual realization of a sufficiently powerful quantum computer would render these systems insecure, compromising vast amounts of the world's data.

In response to this threat, the field of Post-Quantum Cryptography (PQC) has emerged. PQC aims to develop new cryptographic algorithms that are secure against attacks from both classical and quantum computers. This report details the findings of a hands-on study exploring PQC through the liboqs library. The objective was to implement and analyze selected PQC schemes, specifically the Key Encapsulation Mechanism (KEM) Kyber512 and the digital signature algorithm Dilithium2, and compare their performance and size characteristics against the classical RSA-2048 standard.

2. Experimental Data and Observations

Experiments were conducted to measure key generation time, encapsulation/signing time, and decapsulation/verification time. Furthermore, the sizes of public keys, private keys, and the resulting ciphertexts or signatures were recorded. The data collected from implementing Kyber512 and Dilithium2 via liboqs, and RSA-2048 via OpenSSL, is summarized below.

Algorithm	Type	Public Key (Bytes)	Secret Key (Bytes)	Output Size (Bytes)	Keygen (ms)	Encaps/ Sign (ms)	Decaps/ Verify (ms)
Kyber512	KEM	800	1632	768 (Ciphertext)	~0.04	~0.06	~0.05
Dilithium2	Signature	1312	2528	2420 (Signature)	~0.11	~0.20	~0.08
ECDSA P-256	Signature	33 (compressed)	32	64 (Signature)	~0.02	~0.03	~0.10
RSA-2048	Signature	~270	~1200	256 (Signature)	~85.5	~1.50	~0.04

The most immediate observation is the significant difference in data sizes. Both the public/secret keys and the signature output of Dilithium2 are substantially larger than those of RSA-2048. Kyber512's keys and ciphertext are also larger than their classical ECC equivalents.

Conversely, the performance metrics reveal a different story. The PQC algorithms demonstrate remarkably fast execution times. Kyber512's entire key generation and exchange process is completed in a fraction of a millisecond. Most notably, RSA-2048's key generation is orders of magnitude slower than that of either PQC scheme. While RSA's verification is extremely fast, Dilithium2 is competitive across both signing and verification operations.

3. Analysis and Discussion

Practicality for Real-World Deployment

Based on the data, Kyber appears highly practical for real-world deployment as a replacement for classical key exchange mechanisms. Its performance is excellent, and while its key and ciphertext sizes are larger than those of ECC, they are well within manageable limits for modern network protocols like TLS. Its selection by NIST as a standard for general-purpose KEMs further solidifies its viability.

For digital signatures, the choice is more nuanced. Dilithium2 is a strong, general-purpose candidate due to its high performance. However, its signature size of over 2.4 KB is a significant drawback for bandwidth-constrained applications, such as IoT devices. In such scenarios, an algorithm like Falcon, which offers much smaller signatures, might be more practical. Therefore, the practicality of a PQC signature scheme is heavily dependent on the specific application's constraints.

Trade-offs: Security, Performance, and Size

The transition to PQC is fundamentally a series of trade-offs between future-proof security, computational performance, and data size.

- **Security**: The primary motivation for PQC is to provide long-term security against quantum adversaries. This is a non-negotiable requirement for systems intended to protect data for decades.
- **Performance vs. Size**: Our results clearly illustrate this trade-off. We trade the compact keys and signatures of RSA for the much faster operational speeds of Dilithium. For a web server handling thousands of connections per second, reducing the computational cost of signing (from 1.50 ms for RSA to 0.20 ms for Dilithium) could be a decisive advantage, making the larger signature size an acceptable cost.

- **Key Generation Cost**: The extremely slow key generation of RSA is a known issue. PQC's vastly superior performance in this area is a significant operational benefit, especially in environments where keys are frequently generated.

The Utility of Hybrid Schemes

Hybrid cryptographic schemes, which combine a classical algorithm with a PQC algorithm, offer a robust and conservative strategy for transitioning to a post-quantum world. In a hybrid key exchange, a client and server would perform both an ECC Diffie-Hellman exchange and a Kyber exchange, combining the resulting secrets to form the final session key.

The utility of this approach is twofold:

1. **Resilience Against Flaws in PQC**: PQC algorithms are relatively new. If a critical vulnerability were discovered in a chosen PQC algorithm, the classical component of the hybrid scheme would still protect the connection from classical attackers.
2. **Protection Against Quantum Threats**: A hybrid scheme provides immediate protection against the "harvest now, decrypt later" threat. If an adversary is recording current traffic secured by classical crypto, a quantum computer could decrypt it in the future. A hybrid scheme ensures that the connection is also protected by the PQC algorithm, rendering this future decryption impossible.

In essence, a hybrid scheme is secure as long as *at least one* of its constituent algorithms remains unbroken, making it an ideal risk-mitigation strategy.

4. Conclusion

This study successfully demonstrated the implementation and evaluation of post-quantum cryptographic algorithms. The results show that leading PQC candidates like Kyber and Dilithium are computationally efficient and viable for real-world use. The primary challenge in their adoption is the considerable increase in the size of keys and signatures compared to their classical predecessors.

The choice of a specific PQC algorithm requires a careful analysis of the trade-offs between performance and size in the context of a given application. For the immediate future, hybrid schemes provide a prudent path forward, ensuring security against both present and future threats while the global cryptographic community builds confidence in these next-generation algorithms

.