A Prototype for Post-Quantum Cryptographic Migration in Hyperledger Fabric

Jen-Wei Hu and Zhong-Yi Lin
National Center for High-performance Computing, NIAR, Tainan, Taiwan
Email: {0803061, 2203001}@niar.org.tw

***Abstract*—As quantum computing technology rapidly advances, it poses significant threats to traditional cryptographic systems. To address this challenge, this study implements a specific post-quantum cryptographic (PQC) hybrid signature in the open-source enterprise blockchain project Hyperledger Fabric. By leveraging the cryptographic library cfgo, the study enhances security in both digital signatures and the TLS protocol. Additionally, the performance is evaluated under different consensus mechanisms, revealing that long public keys and signatures lead to an increase in storage requirements. While the use of post-quantum signature algorithms results in a decrease in transactions per second (TPS), there is no severe performance degradation. Through this study, we aim to provide valuable insights and practical guidance for the application of PQC in operational blockchain systems, contributing to the construction of quantum-safe information infrastructure in the future.**

Keywords—Blockchain, post-quantum cryptographic, digital signature, Hyperledger Fabric

I. INTRODUCTION

With the rapid advancement of quantum computing, traditional cryptographic systems are facing significant threats. Quantum computers have the potential to break widely used public key cryptographic algorithms, such as those based on integer factorization or discrete logarithms, posing a severe risk to modern information security infrastructures, including blockchain technology. Recognizing this imminent challenge, the National Institute of Standards and Technology (NIST) achieved a major milestone in August 2024 by releasing the first set of post-quantum cryptography (PQC) standards. Among these, FIPS 204 [1] specifies the ML-DSA algorithm, based on the Dilithium signature scheme, to safeguard sensitive information against quantum computing threats.

PQFabric [2] was introduced as the first implementation of Hyperledger Fabric [3] to incorporate hybrid digital signatures. By integrating with the Open Quantum Safe (OQS) library, PQFabric utilizes hybrid digital signatures that combine one classical and one quantum-safe signature, providing protection against both classical and quantum attacks. However, PQFabric was built on Fabric v1.4, a version that has since become outdated. Key components of Fabric v1.4, such as the Raft consensus algorithm, are now deprecated. More recent consensus algorithms, such as Byzantine Fault Tolerance (BFT) [4], introduce additional complexities, including the need for signature-based voting during consensus. Furthermore, PQFabric does not address the post-quantum security of the TLS (Transport Layer Security) protocol, which is critical for secure communication between orderers and peers.

In this study, we implement a prototype based on the Hyperledger Fabric v3.0 codebase, leveraging *cfgo* [5], a cryptographic library designed to support post-quantum algorithms, to enhance security in both digital signatures and the TLS protocol. The prototype utilizes a hybrid signature scheme based on Dilithium and the classical Ed448 algorithm, providing robust protection against quantum and classical threats. Additionally, the hybrid signature scheme has been seamlessly integrated into the orderer, enabling support for various consensus mechanisms, including Zero Fault Tolerance (ZFT), Crash Fault Tolerance (CFT), and Byzantine Fault Tolerance (BFT). These modifications ensure the prototype's adaptability to diverse blockchain scenarios, effectively addressing prior challenges such as the outdated components in PQFabric and the absence of post-quantum TLS support.

II. IMPLEMENTATION

To implement post-quantum cryptography (PQC) hybrid signature algorithms on Hyperledger Fabric, modifications were made at two levels: the lower level, involving updates to the Go programming environment, and the upper level, involving changes to Hyperledger Fabric libraries.

A. Lower-Level Modifications

We used *cfgo* to implement post-quantum cryptographic signature algorithms. *cfgo* utilizes the *CIRCL* cryptographic library to support the TLS protocol. Additionally, it provides a hybrid digital signature scheme called *eddilithium3*, which combines Ed448 and CRYSTALS-Dilithium signatures. To integrate eddilithium3 with Hyperledger Fabric, we added support for its public and private key types to *cfgo's crypto/x509* library and incorporated it into Fabric's core libraries.

B. Upper-Level Modifications

We made changes to three main areas of the Hyperledger Fabric codebase to support the hybrid signature scheme:

1) Blockchain Cryptographic Service Provider (BCCSP): The BCCSP module provides a unified cryptographic interface for Fabric's core, without being tied to any specific

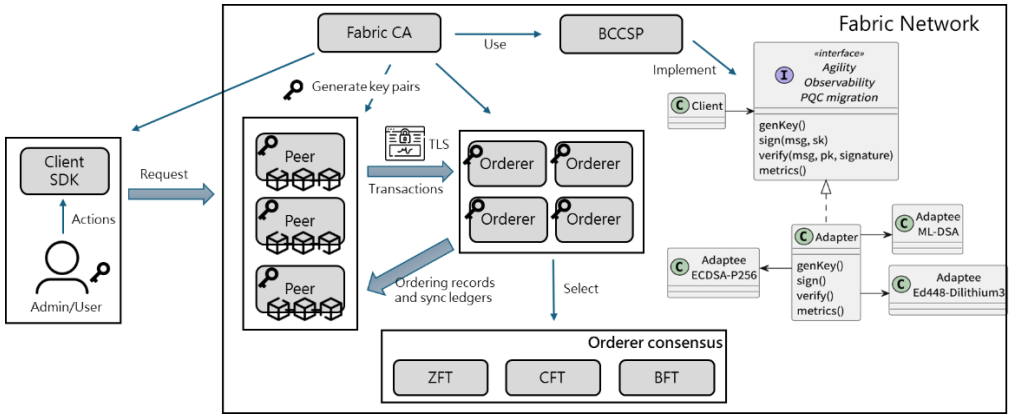

Fig. 1. Architecture of the Experimental Fabric Network

cryptographic algorithm or implementation. We integrated support for the eddilithium3 hybrid signature type from *cfgo* for use within Fabric.

2) Cryptogen Tool:

Cryptogen is used to generate cryptographic materials required within an organization. With this tool, the Certificate Authority (CA) issues digital signature certificates as X.509 credentials for orderers, peers, users, and administrators.

3) TLS Support:

To enable secure communication between orderers and peers, we added support for Ed448-Dilithium3 hybrid signatures to establish connections over both HTTPS and gRPC protocols.

TABLE I
THE EXPERIMENTAL RESULTS

Signature-Consensus	TPS (ms)	Peer (MB)	Orderer (MB)
ECDSA-ZFT	121	356	328
ECDSA-CFT	105	360	328
ECDSA-BFT	94	352	644
Ed448-Dilithium3-ZFT	98	3208	3180
Ed448-Dilithium3-CFT	94	3212	3184
Ed448-Dilithium3-BFT	70	3120	6204

III. Evaluation and Results

We evaluated our implementation on a network comprising four orderers, one Certificate Authority (CA), and three peers, each deployed on a separate virtual machine. Transactions were sent from the client to a single peer, while the remaining peers also acted as endorsers. Each virtual machine was equipped with Intel Xeon Gold 61 processors running at 2.6 GHz and 32 GB of RAM.

Our evaluation considered three consensus mechanisms provided by Hyperledger Fabric: ZFT, CFT, and BFT. The baseline cryptographic configuration uses ECDSA over curve P-256 to sign transactions, which was compared against benchmarks where nodes were configured to use the Ed448-Dilithium3 hybrid signature scheme for signing and verification. The blockchain network architecture is shown in Fig 1. For each benchmark, 100 asset creation transactions were processed to calculate transactions per second (TPS) and measure the storage consumed by both the consensus orderers and peer nodes.

The experimental results are shown in Table I. Compared to the ECDSA P256 signature scheme, the Ed448-Dilithium3 signature scheme shows a decrease in TPS of 19%, 10%, and 26% in ZFT, CFT, and BFT, respectively. Regarding storage space, the Ed448-Dilithium3 signature increases storage by 870%, 871%, and 863% in ZFT, CFT, and BFT types, respectively. Overall, although the use of post-quantum signature algorithms results in a decrease in TPS compared to traditional signature methods, there is no severe performance degradation. However, there is a significant increase in storage space resource consumption. Due to the complexity and high cost of maintaining BFT, it is recommended to implement PQC migration blockchain applications using a CFT configuration for the same hybrid signature scheme.

IV. Conclusion and Future Work

In this paper, we implement a specific post-quantum cryptographic (PQC) hybrid signature within the open-source enterprise blockchain project Hyperledger Fabric. By utilizing the cryptographic library cfgo, we enhance security for both digital signatures and the TLS protocol. We believe our work significantly contributes to the ongoing discussion on post-quantum cryptographic standards and the integration of post-quantum solutions in blockchain technology. We hope it will be beneficial to both those involved in developing these standards and those looking to implement them.

References

[1] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard, Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

[2] A. Holcomb, G. Pereira, B. Das, and M. Mosca, "PQFabric: A permissioned blockchain secure from both classical and quantum attacks," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–9.

[3] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proc. of the thirteenth EuroSys conf.*, 2018, pp. 1–15.

[4] A. Barger, Y. Manevich, H. Meir, and Y. Tock, "A byzantine fault-tolerant consensus library for hyperledger fabric," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–9.

[5] Cfgo. Cloudflare. Available at https://github.com/cloudflare/go.