THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(4)2019

Transitioning to a Hyperledger Fabric Hybrid Quantum Resistant-Classical Public Key Infrastructure

Robert E. Campbell Sr.
Capitol Technology University, Laurel, USA
Correspondence: rc@medcybersecurity.com
Received: 13 June 2019 **Accepted**: 26 July 2019 **Published**: 31 July 2019

Abstract

Hyperledger Fabric (HLF) is a permissioned, blockchain designed by IBM and uses Public Key Infrastructure (PKI), for digital signatures, and digital identities (X.509 certificates), which are critical to the operational security of its network. On 24 January 2019, Aetna, Anthem, Health Care Service Corporation, PNC Bank, and IBM announced a collaboration to establish a blockchain-based ecosystem for the healthcare industry [1]. Quantum computing poses a devastating impact on PKI and estimates of its large-scale commercial arrival should not be underestimated and cannot be predicted. The HIPAA (Health Insurance Portability and Accountability Act) and General Data Protection Regulation (GDPR), requires "reasonable" measures to be taken to protect Protected Health Information (PHI), and Personally Identifiable Information (PII). However, HLF's ecosystem is not post-quantum resistant, and all data that is transmitted over its network is vulnerable to immediate or later decryption by large scale quantum computers. This research presents independent evaluation and testing of the National Institute of Standards and Technology (NIST), based Second Round Candidate Post-Quantum Cryptography (PQC), lattice-based digital signature scheme qTESLA. The second-round submission is much improved, however; its algorithm characteristics and parameters are such that it is unlikely to be a quantum-resistant "as is," pure "plug-and-play" function and replacement for HLF's PKI. This work also proposes that qTESLA's public keys be used to create a quantum-resistant-classical hybrid PKI near-term replacement.

Keywords: *Hyperledger Fabric, PKI, HIPAA, GDPR, distributed ledger, post-quantum cryptography, qTESLA, Ring Learning with Errors, cybersecurity, enterprise blockchains*

JEL Classifications: *D02, D71, H11, P16, P48, P50*

1. Introduction

An X.509 PKI is a security architecture that uses cryptographic mechanisms to support functions such as email protection, web server authentication, signature generation, and validation. It is a specification upon which applications like Secure Multipurpose Internet Mail Extensions (S/MIME) and Transport Layer Security (TLS) are based. It also can be defined as a collection of methods, rules, policies, and roles that are required to generate, manage, provide, employ, and revoke digital certificates; it is also responsible for the management of public-key encryption. A PKI ensures the secure transfer of data over various network infrastructures, such as Intranet and Internet architectures. HLF's Enterprise Blockchain, and in general the secure communications, critical infrastructure, banking, and Internet commerce depends upon the security and reliability of PKI cryptography. Cryptographic encryption and signature algorithms are used to ensure confidentially, integrity, and authenticity of messages, data, and information. PKI is used to bind identities, and public-keys and Fabric uses Certificate Authorities (CA), as the primary trusted party that uses digital signature algorithms to sign certificates of trust. The architecture, deployment, and operation of HLF impact the blockchain network's cybersecurity risks and determine the controls best able to mitigate those risks. Key considerations include the ability of untrusted or unauthorized persons to participate in the network; and the strength of the encryption protocols. Advances in quantum computing are threatening today's global encryption standards, including PKI [2]. There is an immediate need to develop, deploy, and migrate the consortium's blockchain ecosystem to a hybrid safe PQC. PQC is cryptosystems which run on classical computers and are considered to resistant to quantum computing attacks. There are significant uncertainties associated with PQC, such as, the possibility of new quantum algorithms being developed which would cause new attacks. Also, new PQC algorithms are not

thoroughly tested and analyzed. It takes years to understand their security in a classical computing environment. This work evaluates HLF's blockchain post-quantum computing vulnerabilities and threats given global regulatory requirements and provides valuable second-round qTESLA independent testing and evaluation data and aids in the NIST Post-Quantum Cryptography Standardization Process [3]. Further, the author encourages additional independent testing, verification, and validation of qTESLA as one of the most practical hybrid quantum-resistant PKI systems.

2. Implications in this Work

Without plans for quantum-resistant cryptography and security, all data and information, including encrypted, that is transmitted today, and tomorrow is vulnerable. This would violate all known regulatory requirements for data privacy and security. HIPAA enacted in 1996 and is United States legislation that provides security and data protection for medical information [4]. GDPR requires in the case of a personal data breach notification not later than 72 hours after having become aware of it [5]. Both GDPR and HIPAA levies hefty fines and penalties due to non-compliance. GDPR non-compliance with various provisions of the GDPR shall be fined according to the gravest infringement, which can be Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher [6]. HIPAA violations of penalties and fines for noncompliance are also based on the level of perceived negligence. These fines can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for each violation [7]. It takes years of study and analysis of quantum-resistant cryptography algorithms before governments and industry can trust their security. Given the nature and the far-reaching implications of the legal and financial obligations of both these laws, it is essential to have plans and strategies to address and mitigate vulnerabilities and threats that may lead to data breaches and non-compliance. Permissioned blockchains are not immune to cyber-attacks, and further exploration of the quantum-resistant cryptography is a necessity, and, a consensus between industry and regulators regarding the appropriate cybersecurity standards to apply to blockchain solutions in the healthcare, financial and GDPR covered services industry. An honest discussion and principles approach to cybersecurity regulation all in mitigating cybersecurity risk in permissioned blockchains while allowing the technology to continue to evolve through innovation.

Failure to comply with HIPAA, GDRP, and other regulating authorities can result in stiff penalties. Fines will increase with the volume of data or the number of records exposed or breached, and the amount of neglect. The lowest fines begin with a breach when the rules are not known, and by exercising reasonable diligence, would not have known the provisions were violated. At the other end of the spectrum are fines levied where a breach is due to negligence and not corrected appropriately.

We need a coordinated strategy and approach with specific recommendations and policies for academia, policymakers, and industry participants regarding and promoting the development of secure blockchain technologies and applications through viable cybersecurity standards. The enterprise blockchain cybersecurity risks must be understood, and risk management plans along with policies for HLF and enterprise blockchain, in general, must have policies that are by regulating authorities.

3. Significance of the Findings

IBM simultaneously is a leading developer of enterprise-grade blockchains and quantum computers. In 2018, Harriet Green, chairman, and CEO of IBM Asia Pacific, stated: "IBM sees quantum computing going mainstream within five years" [8]. Currently, there is not a specific strategy to mitigate the threat of quantum computers, and as such, all known data security and privacy laws will be violated. There are significant regulatory responsibilities of its participants that own, create, modify, store, or transmit regulated data and information. Enterprise-grade blockchains must enact holistic approaches to cybersecurity across applications, infrastructure, and processes. Cybersecurity must defend against attacks, but also maintain control of data content. This research illuminates the need for new policies to be developed for those entities whose data is regulated. To the author's knowledge, no cybersecurity policy addresses regulated data on enterprise blockchains. A cybersecurity policy outlines the assets that need protection and the threats to those assets and the rules and controls for protecting them. The policy should inform all approved users of their responsibilities to protect information about those assets. Policy management, reporting, and administration will be essential for organisations inputting their data on blockchains. Participants will need to be able to report enterprise-wide on everything users have done with regulated content to satisfy compliance requirements.

HLF's PKI system of trust is broken with the arrival of large-scale quantum computing, and all PII and PHI are at risk with no known plans to mitigate. HIPAA, GDPR, FINRA, and all known data and privacy laws that will be violated. The author has independently tested, verified, and validated qTESLA's much improved Second Round Submission to NIST Post-Quantum Cryptography Standardization Process and has proposed a hybrid quantum-resistant PKI system for replacement in HLF. The test result yields smaller key sizes; however; given today's standards and applications in use only qTESLA's public key is recommended for use in a hybrid PKI solution. qTESLA's public-key is an adequate replacement for the current ECDSA public-key. In HLF's PKI, it is the public key that is used most often and qTESLA's second submission offers an acceptable size that could reinforce a mix of the most practical quantum-resistant digital signature scheme with current ECDSA algorithms.

Given what is at risk for the blockchain implementors and its users, reasonable measures must be taken to mitigate the threat of data privacy and security. To safeguard data on a blockchain platform, the participants must be able to control who has access to their data and under what circumstances. Blockchain networks must be able to provide reasonable measures and safeguards that adhere to privacy regulations such as HIPAA, FINRA, and GDPR.

4. HLF and PKI and Membership Services Technology

IBM offers Cryptographic PKI Services that allow users to establish a PKI infrastructure and serve as a certificate authority for internal and external users, issuing and administering digital certificates. It supports the delivery of certificates through the Secure Sockets Layer (SSL) for use with applications that are accessed from a web browser or web server. It includes delivery of certificates that support the Internet Protocol Security standard (IPSEC) for use with VPN applications and delivery of certificates that support Secure Multipurpose Internet Mail Extensions (S/MIME), for use with email applications. All these functions are essential but critically vulnerable.

Fabric is a private, blockchain technology that uses smart contracts, and participants or members manage its transactions. The members of the network enroll through a "trusted" Membership Service Provider (MSP) [9]. The blockchain is advertised as an implementation of distributed ledger technology (DLT) that delivers enterprise-ready network security, scalability, confidentiality, and performance, in modular blockchain architecture.

The MSP **i**ssues, cryptography, protocols, encryption, signature keys and issues and validates certificates and user authentication to clients and peers. HLF's PKI consists of Digital Certificates, Public and Private Keys, and Certificate Authorities (CA) which issues digital certificates to parties, who then use them to authenticate messages. A CA's Certificate Revocation List (CRL) is a reference for the certificates that are no longer valid. PKI is used to generate certificates which are tied to organizations, network components, and end-users or client applications. The MSP dispenses X.509 certificates that can be used to identify components as belonging to an organization. Certificates issued by CAs can also be used to sign transactions to indicate that an organization endorses the transaction result and is a necessary precondition of it being accepted onto the ledger. These X.509 certificates are used in client application transaction proposals and smart contract transaction responses to digitally sign transactions. Its digital certificate is compliant with the X.509 standard and holds the attributes relating to the holder of the certificate. The holder's public key is distributed within the certificate, and the private signing key is not.

The public-keys and private-keys are made available and act as an authentication "anchor," and the private keys are used to produce **digital signatures**. Recipients of digitally signed messages can validate and authenticate the received message by checking that the attached signature is valid with the use of the public key. Digital identities are cryptographically validated digital certificates that comply with X.509 standard and are issued by a Certificate Authority (CA). HLF uses a list of self-signed (X.509) certificates to constitute the root of trust and a list of self-signed (X.509) certificates to form the root of trust. A CA dispenses certificates that are digitally signed by the CA and bind together the actor with the actor's public key. The above services are critical to the operation of a secure enterprise blockchain, and there must be plans and strategies in place that provide reasonable measures to adhere to regulatory policies.

5. Post-Quantum Computing Impact on HLF PKI

PQC algorithms must provide security against both classical and quantum computing attacks. Their performance is measured on classical computers and considerations are made for the potential of "drop-in replacements," which infers compatibility and interoperability with existing systems. Also, essential

requirements must include resistance to side-channel attacks and misuse.

Cryptography in HLF is used in many applications where secure communication is needed. The primary use and role are signature generation, verification, and authentication where algorithms are used to establish confidentiality, integrity, and authenticity of messages sent during communication. Public-key cryptography is used where each participant has a private key and a public key. In a public-key signature cryptosystem, the signer has a private signing key that can be used to sign messages and must keep this key secure. The public key, which is visible to anyone, can be used to verify that the signature is authentic and, if the signature scheme is secure, then repudiation is achieved and only the signer could have generated the signature. PKIs are used to bind identities to the public keys, where Certificate Authorities (CAs) play an essential role. A CA is a commonly trusted party that uses digital signature algorithms to author certificates consist of a public key and information of its owner. The security of public-key cryptography and ultimately, the private key is based on cryptography that can no longer be considered safe because of the emerging quantum computing threat. HLF relies on a PKI, which is based upon Elliptic Curve Cryptography (ECC), and it is critically vulnerable to quantum computing [10]. Specifically, the cryptography that secures web browsers (TLS), certificates, software updates, virtual private networks (IPsec), secure email (S/MIME) and many other applications are no longer safe in the PQC era [11]. Reasonable blockchain enterprise cybersecurity measures require extensive planning and testing for transition and migration to post-quantum resistant cryptography.

It is unlikely that the current PQC algorithms under review will function "as is" and will require modifications such as hybrid quantum resistant-classical PKI systems. Hybrid systems will likely be the way forward in the near term, given the uncertainties and complexities of the current crop of PQC algorithms. Current cryptographic libraries will provide support for post-quantum digital signature algorithms in PKI but will require some modifications and testing in large-scale scenarios.

In this paper, the author investigates the use of hybrid digital signature schemes, specifically qTESLA. Much testing needs to be done in real-world scenarios involving digital signatures and PKI. Protecting against quantum attacks will require changes that designers and implementers will have to accommodate. Cryptographic primitives may need to be a replaced, and protocol-level modifications may be necessary to provide new primitives. It is a complex and lengthy undertaking to migrate to a new quantum-resistant PKI. Other issues such as constrained devices, compatibility, performance characteristics, and Internet of Things (IoT) must also be considered. Currently, HLF uses the Elliptic Curve Digital Signature Algorithm, which is used for many functions such as digital signatures and TLS protocol handshakes.

6. Elliptic Curve Cryptography in HLF

Elliptic curve cryptography is a class of public-key cryptosystem which assumes that finding the elliptic curve discrete algorithm is not possible in a "reasonable" amount of time. Public key cryptography does not require any shared secret between the communicating parties. The security of elliptic curve or asymmetric cryptographic schemes relies on the believed hardness of solving "hard problems," such as integer factorization and the computation of discrete logarithms in finite fields or groups of points on an elliptic curve. The ECDSA algorithm relies critically on generating a random private key used for signing messages and a corresponding public key used for checking the signature. The bit security of this algorithm depends on the ability to compute a point multiplication and the inability to calculate the multiplicand given the original and product points. Decades ago, these were "hard problems," due to several factors such as the current state of computing power, and the time it would take for a classical computer to solve these problems. Other factors come into play, such as the length of cryptanalysis and the lack of known techniques that ensured the problems remained hard. However, the technology of computing power, cryptanalysis, and side-channel analysis always threaten the existing cryptographic standards given enough time. It can be noted that many real-world cryptographic vulnerabilities do not stem from solely a weakness in the underlying algorithms, but often from implementation flaws such as side-channel attacks, errors in software or code design flaws. An example is the vulnerabilities ECDSA signature implementation, is the property of weak randomness used during signature generation, which can compromise the long-term signing key.

The HLF CA provides features such as, registration of identities, or connects to Lightweight Directory Access Protocol (LDAP) as the user registry, issuance of Enrollment Certificates (ECerts), certificate renewal and revocation. HLF's ECDSA offers the following key size options:

Table 1. Algorithms used to generate X.509 certificates and keys are not secure [12]

Size	ASN1 OID	Signature Algorithm
256	prime256v1	ecdsa-with-SHA256
384	secp384r1	ecdsa-with-SHA384
521	secp521r1	ecdsa-with-SHA512

The approved security strengths for U.S. federal applications are 128, 192, and 256 bits. Note that a security strength of fewer than 128 bits is no longer approved because quantum algorithms reduce the bit security to 64 bits (see table 2). NIST Special Publication 800-57 Part 1 Revision 4: Recommended for Key Management, as shown in Table 2 [13]. Table 2 shows that Rivest, Shamir, and Adleman (RSA) and ECC based PKI have zero bits of security and AES requires larger keys. This table illustrates the vulnerability and single point failure, of the fully trusted CA and X509 standard based on ECC. The quantum computing threat collapses the RSA, ECC, and HLF's PKI.

Table 2. Comparison of conventional and quantum security levels of typical ciphers [14]

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

7. Evaluation of qTESLA's Second Round Submission to NIST

The National Institute of Standards and Technology (NIST) is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new public-key cryptography standards will specify one or more additional digital signature, public-key encryption algorithms. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers. The author tracked with NIST in identifying three broad aspects of evaluation criteria that would be used to compare candidate algorithms throughout the NIST PQC Standardization Process. The three elements are 1) security, 2) cost and performance, and 3) algorithm and implementation characteristics. Security is the most crucial factor when evaluating candidate post-quantum algorithms. Cost as the second-most important criterion when assessing candidate algorithms. In this case, cost includes computational efficiency and memory requirements. After security, the performance was the next most important criterion in selecting the second-round candidates [3].

qTESLA is a lattice-based signature scheme which uses the assumption that RLWE distributions are indistinguishable from random. The public key in qTESLA is, roughly speaking, a sample of an RLWE distribution. The signer keeps secret information about this sample and uses that information along with a hash function to produce signatures. Signature verification involves some simple arithmetic within the chosen ring, and then the recomputation of a hash function. qTESLA has reasonably good performance parameters that are comparable to the other lattice-based signature schemes. The submitters of qTESLA have claimed a tight security proof for the schemes in the quantum random oracle model. It was noticed that a bug in the security proof requires an adjustment of the parameters (which reduces the efficiency of the scheme). Furthermore, the security argument assumes (among other things) conjecture about the distribution of random elements in the ring. Considering that the conjecture does do not seem to fit the form of a typical security assumption, and more analysis will need to be conducted in the second round.

This section, tests, evaluates and analyzes qTESLA's second-round submission modifications in the lattice-based digital signature scheme category to NIST's post-quantum standardization project. This second-round submission is based on the hardness of the decisional Ring Learning With Errors (R- LWE) problem. qTESLA utilizes two approaches for parameter generation that includes heuristic and provably-secure. The heuristic approach is optimized for efficiency and key size, and the provably- secure is targeted to highly sensitive or classified transactions. A new feature added in the second-round submission is a key compression technique that produces a noticeable reduction in the public key size. The vendor refers to this technique as "public key splitting," and is significant because it is the public key that is used most often in typical transactions. qTESLA has submitted twelve parameter sets targeting various security levels. However, this work focuses on submissions that include public-key reduction and the most efficient submissions as the most practical hybrid (classical and quantum-resistant) PKI near-term algorithm solution [14].

8. Basic signature scheme

Informal descriptions of the algorithms that give rise to the signature scheme qTESLA are shown in Algorithms 1, 2, and 3. These algorithms require two basic terms, namely, B-short and well-rounded, which are defined below.

Let q, L_E , L_S , E, S, B, and d be system parameters that denote the modulus, the bound constant for error polynomials, the bound constant for the secret polynomial, two rejection bounds used during signing and verification that are related to L_E and L_S , the bound for the random polynomial at signing, and the rounding value, respectively. An integer polynomial y is B-short if each coefficient is at most B in absolute value. An integer polynomial w well-rounded if w is $(\lfloor q/2 \rfloor - E)$-short and $[w]_L$ is $(2^{d-1} - E)$-short.

In Algorithms 1-3, the hash oracle $H(\cdot)$ maps to H, where H denotes the set of polynomials $c \in R$ with coefficients in $\{-1, 0, 1\}$ with exactly h nonzero entries.

Algorithm 2 is described as a non-deterministic algorithm. This property implies that different randomness is required for each signature. This design feature is proposed as added to prevent some implementation attacks and protect against some fault attacks [13].

Algorithm 1 Informal description of the key generation

Require: -

Ensure: Secret key $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$, and public key $pk = (a_1, ..., a_k, t_1, ..., t_k)$

- $a_1, ..., a_k \leftarrow R_q$ ring elements.
- Choose $s \in R$ with entries from D_σ. Repeat step if the h largest entries of s sum to at least L_S .
- For $i = 1, ..., k$: Choose $e_i \in R$ with entries from D_σ. Repeat step at iteration i if the h largest entries of e_i sum to at least L_E.
- For $i = 1, ..., k$: Compute $t_i \leftarrow a_i s + e_i \in R_q$.
- Return $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$ and $pk = (a_1, ..., a_k, t_1, ..., t_k)$

Algorithm 2 Informal description of the signature generation

Require: Message m, secret key $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$

Ensure: Signature (z, c)

- Choose y uniformly at random among B-short polynomials in R_q.
- $c \leftarrow H([a_1 y]_M , ..., [a_k y]_M , m)$.
- Compute $z \leftarrow y + sc$.
- If z is not $(B - S)$-short then retry at step 1.
- For $i = 1, ..., k$: If $a_i y - e_i c$ is not well-rounded then retry at step 1.
- Return (z, c).

Algorithm 3 Informal description of the signature verification

Require: Message m, public key $pk = (a_1, ..., a_k, t_1, ..., t_k)$, and signature (z, c)

Ensure: "accept" or "reject" signature

- If z is not $(B - S)$-short then return reject.
- For $i = 1, ..., k$: Compute $w_i \leftarrow a_i z - t_i c \in R_q$.
- If $c \neq H([w_1]_M , ..., [w_k]_M , m)$ then return reject.
- Return accept.

9. New features

qTESLA utilizes two approaches for parameter generation, the first approach, referred to as "heuristic qTESLA," follows a heuristic parameter generation and the second approach, referred to as "provably secure qTESLA," follows a provably secure parameter generation according to existing security reductions. New in this submission is mitigation steps to address the implementation attacks as research shows the vulnerabilities of lattice-based signature schemes such as qTESLA [16]. The second and third new feature is the AVX2-optimized implementations for the parameter sets qTESLA-I, qTESLA-III, and qTESLA-V, and their variants with smaller public keys, called "public key splitting," for qTESLA-I-s, qTESLA-III-s, and qTESLA-V-s respectively. qTESLA's AVX2-optimized implementations submission included an Intel Advanced Vector Extensions 2 (AVX2) submission which significantly improved performance. The author performed experiments with qTESLA's AVX2 optimized implementation, and the results are included in this paper. The public key splitting submission is a variant that addresses public key size, which is significant because the public key size is regarded as more important than the secret key size because the former needs to be transmitted more frequently [14].

10. Mitigation of implementation attacks

Side-channel cryptanalysis considers attackers trying to take advantage of the physical interactions of cryptographic devices to achieve recovery of the secret key. In some cases, computational faults are intentionally inserted to obtain faulty values for the key recovery. Fault injections or attacks are also used to obtain information leakage under the faulty environment. These implementations-specific attacks are more efficient than the best-known cryptanalytic attacks. They are therefore generally more powerful than classical cryptanalysis and are a serious class of attacks that must be addressed. These attacks exploit timing or power consumption, electromagnetic emanation, that is correlated to some secret information during the execution of a cryptographic scheme and protection against this attack is a minimum-security requirement for standardized cryptographic implementation. qTESLA attempts to address the exploit timing leakage, power consumption, electromagnetic emanation, and cache attacks by adding constant-time execution to secure against side-channel analysis. qTESLA 's approach indicates that it is in every signing operation, it injects "fresh randomness," that will make it resilient to a catastrophic failure of the Random Number Generator (RNG) protecting against fault analysis attacks [14]. The verification and validity of the previous statements are not in the scope of this paper and will most likely require more independent tests and analysis.

11. Performance of second-round qTESLA algorithms analysis

To evaluate the performance of the provided implementations written in portable C, the author ran benchmarking suite on one machine powered by an Intel® Core™ i7-6500 CPU @ 2.50 GHz x 4 (Skylake) processor, 16 GB of RAM, 500 GB hard drive, GNOME:3.28.2, running Ubuntu 18.04.2 LTS. For compilation, GCC version 7.3.0 was used in all tests. The vendor proposed twelve parameter sets which were derived according to two approaches (i) following a "heuristic" parameter generation, and (ii) following a "provably-secure" parameter generation according to a security reduction. The proposed parameter sets are displayed in Table 3, together with their targeted security category.

The results for the optimized implementations are summarized in Tables 4, and 5, respectively. The results for AVX2 implementations are given in Tables 6, and 7, respectively. Additionally, the reference implementations are summarized in Tables 8, and 9, respectively. Results for the median and average

Table 3. Parameter sets and their targeted security [14]

Heuristic	Provably secure	Security category
qTESLA-I, qTESLA-I-s	qTESLA-p-I	NIST's category 1
qTESLA-II, qTESLA-II-s	-	NIST's category 2
qTESLA-III, qTESLA-III-s	qTESLA-p-III	NIST's category 3
qTESLA-V, qTESLA-V-s	-	NIST's category 5
qTESLA-V-size, qTESLA-V-size-s	-	NIST's category 5

Table 4. Second Round Optimized Implementation tests for 5000 iterations.

Scheme	keygen	sign	verify	total (sign + verify)
qTESLA-II	4410.7 (4963.6)	931.7 (1226.1)	232.8 (236.5)	1164.5 (1462.6)
qTESLA-II-s	4004.0 (4818.7)	981.5 (1281.4)	232.7 (235.1)	1214.2 (1516.5)
qTESLA-V-size	17177.0 (20416.5)	2161.4 (2812.1)	511.6 (514.2)	2673.0 (3326.3)
qTesla-V-size-s	17201.1 (20340.2)	2341.4 (2972.4)	516.8 (523.1)	2858.2 (3495.5)

Table 5. Second Round Optimized Implementation Key Sizes in Bytes

Scheme	Public Key	Secret Key	Signature
qTESLA-II	2336	931.7	232.8
qTESLA-II-s	800	3136	2432
qTESLA-V-size	5024	3520	4640
qTesla-V-size-s	1952	6592	5216

Table 6. Second Round AVX2 Implementation

Scheme	keygen	sign	verify	total (sign + verify)
qTESLA-I	903.2 (940.9)	206.4 (268.2)	55.1 (55.8)	261.5 (324)
qTesla-I-s	928.5 (952.4)	214.9 (276.6)	54.8 (55.9)	269.7 (332.2)
qTESLA-III	2373.5 (2677.0)	273.5 (343.5)	110.4 (111.3)	383.9 (454.8)
qTESLA-III-s	2366.8 (2713.6)	291.4 (374.2)	110.0 (112.4)	401.4 (486.6)
qTESLA-V	12577.2 (14472.8)	734.1 (951.3)	254.9 (256.0)	989.0 (1207.3)

Table 7. Second Round AVX2 Implementation Key Sizes in Bytes

Scheme	Public Key	Secret Key	Signature
qTESLA-I	1504	1216	1376
qTesla-I-s	480	2240	1568
qTESLA-III	3104	2368	2848
qTESLA-III-s	1056	4416	3232
qTESLA-V	6432	4672	5920
qTesla-V-s	1952	6592	5216

Table 8. Second Round Reference Implementation

Scheme	keygen	sign	verify	total (sign + verify)
qTESLA-I	920.3 (971.5)	314.4 (425.6)	71.5 (72.6)	385.9 (498.2)
qTESLA-I-s	926.4 (968.5)	334.2 (438.1)	73.3 (74.2)	481.7 (512.3)
qTESLA-p-I	4130.2 (4316.4)	1990.4 (2605.6)	561.2 (567.9)	2551.6 (3173.5)
qTESLA-II	4466.0 (5047.9)	1536.6 (2027.2)	372.3 (375.7)	1908.9 (2402.9)
qTESLA-II-s	4452.1 (5047.0)	1647.3 (2213.9)	385.5 (386.5)	2032.8 (2600.4)
qTESLA-III	2395.5 (2669.8)	433.9 (580.0)	143.0 (145.2)	576.9 (725.2)
qTESLA-III-s	2410.5 (2735.2)	471.9 (610.8)	150.9 (153.6)	622.8 (764.4)
qTESLA-p-III	21043.7 (21569.7)	5414.6 (7247.6)	1517.4 (1529. 4)	6932.0 (8776.4)
qTESLA-V	12224.6 (14221.3)	1349.6 (1775.1)	325.9 (329.1)	1675.5 (2104.2)
qTESLA-V-s	12644.5 (14433.8)	1439.4 (1856.3)	335.4 (336.8)	1774.8 (2193.1)
qTESLA-V-size	17357.1 (20838.9)	3653.8 (4769.2)	825.2 (830.5)	4479.0 5599.7
qTESLA-V-size-s	17859.4 (21204.1)	3824.2 (5044.1)	851.3 (847.3)	4675.5 (5891.4)

(in parenthesis) are rounded to the nearest 10^2 cycles. Signing is performed on a message of 59 bytes.

This work is a follow-on to qTESLA's NIST first-round submission, and the evaluation focuses on the "new" and improved features submitted in its second-round NIST submission. This second-round submission includes an expanded category of parameters in which the author examined the most practical based on performance improvements. The most significant enhancements noted, is in the speed of key generation and the size of the public keys. Techniques, such as the AVX2 and Public key splitting, yields a dramatic improvement over the previous submissions. The public key splitting offers acceptable sizes for various NIST security category levels, While, these implementations are not provably secure as defined by NIST, meaning the algorithms may not be approved for top secret information and operations, however; they may prove useful for less critical data and processes.

Table 9: Second Round Reference Implementation Key Sizes in Bytes.

Scheme	Public Key	Secret Key	Signature
qTESLA-I	1504	1216	1376
qTESLA-I-s	480	2240	1568
qTESLA-p-I	14880	5184	2592
qTESLA-II	2336	1600	2144
qTESLA-II-s	800	3136	2432
qTESLA-III	3104	2368	2848
qTESLA-III-s	1056	4416	3232
qTESLA-V	6432	4672	5920
qTESLA-V-s	2336	8768	6688
qTESLA-V-size	5024	3520	4640
qTesla-V-size-s	1952	6592	5216

12. Optimized implementations

All comparisons are made about qTESLA's first-round NIST submission where possible, due to the fact there are new submissions and comparisons cannot be made. The optimized implementation for key sizes shows qTESLA-II vs. qTESLA-II-s shows 78.5% public-key reduction; however; there is an increase in the secret key and signature size of 236.5 % and 944.6 % respectively. Submissions for qTESLA-V-size vs. qTESLA-V-size-s shows 61.1 % public-key reduction, while there is an increase in the secret key and signature size of 87.2 % and 12.4 % respectively. (See Table 5).

12.1. AVX2 implementation

The AVX2 implementation for key generation, signing, and verification is shown in Table 6 and is compared to the new AVX2 and public-key reduction. The tests show that there is a slight increase in key generation time, signature and verification time for all categories of submission when using the public-key reduction techniques, however; these improvements are dramatic compared to the respective timing in all categories in

qTESLA's first submission [2]. (See Table 6). The AVX2 implementation for key sizes shows qTESLA-I vs. qTESLA-I-s shows 68.1 % public-key reduction; however; there is an increase in the secret key and signature size of 84.2 % and 13.9 % respectively. Submissions for qTESLA-III vs. qTESLA-III-s shows 65.9 % public-key reduction, while there is an increase in the secret key and signature size of 86.5 % and 13.4 % respectively. Finally, in this category, qTESLA-V vs. qTESLA-V-s shows 69.6 % public-key reduction, while there is an increase in the secret key and signature size of 86.5 % and 41.0 % respectively, See Table 7.

12.2. Reference implementation

The last category examined is Reference implementation, which has 12 parameters. Since many of these parameters are new, direct comparison to the previous submission cannot be made. However; the author notes overall, there is a significant reduction in key generation, signing, and verification times compared to the first-round submission. The following is a comparison of the first-round submission to the second-round submission. For example, for key generation, signing, and verification CPU cycles qTESLA-I reduced key generation cycle time by 26.4 % but increased 5.7 % signing, decreased 12.1 % verification respectively. qTESLA-p-I showed key generation cycle reduction of 23.0 %, but the 152 % increase in signing, an increase of 34.1 % verification. qTESLA-p-III showed a decrease of 16.3 % key generation, but increase signing 71.6 %, and a reduction of 28.3 % verification time (See Table 8 and [2]). The test results of the Reference implementation key sizes in bytes are in Table 9. The following observations can be made from a comparison of the first-round submission with the second-round submission; The most dramatic improvement comes with the public key splitting function, while test results show there is a corresponding increase in secret key size and signature. For example, for the public key of qTESLA-I-s vs. qTESLA-I decreased by 68.0%, but the secret key increased by 84.2 %, and the signature increased by 13.9 %. qTESLA-III-s vs. qTESLA-III show a reduction of 65.9 %, but an increase in the secret key size of 86.4 %, and an increase in the signature size by 13.4 %. Please see Table 9 for further comparisons.

13. Recommendations for Blockchain Implementors

HLF implementors should develop and provide a strategy or roadmap for maintaining the confidentiality, integrity, and availability of private keys and stringent cybersecurity controls to combat the quantum computing threat. Also, implementers should review their current cryptographic standards to make sure they are up to date, and that infrastructure and support exist to update when new NIST standards become available rapidly. Immediate work should begin to test and benchmark the most promising PQC candidates that could be integrated into its blockchain with interoperability and compatibility in mind. The X.509v3 standard allows for algorithm flexibility in that the Object Identifier (OID) defines the formats of public keys. Adding a new cipher OID is needed to extend X.509, but what is also required is for software will be able to comprehend and process the new OID. Currently, there are no known CAs issuing certificates for quantum-safe public keys exist, and no CAs is signing their certificates with a quantum-safe signature algorithm.

Strong blockchain network security requires the roles and responsibilities of each type of participant to be clearly defined and enforced following regulatory guidelines. It is essential to qualify, quantify, and document cybersecurity risks posed by each type of participant. It is also essential to anticipate and understand the security consequences of participants leaving and entering the network over time. Blockchain developers should anticipate and understand these threats resulting before committing regulated data to the blockchain. There should be plans for penetration testing that are similar to traditional networks using various attack scenarios and vectors, document the development process and obtain independent audits of the design and development process.

Therefore, there is an urgent requirement to develop and deploy plans to accommodate the most practical hybrid PQC algorithms that are working towards global standardization. The successful transition and migration to PQC will require significant time and effort given the complexities involved. Further, researchers should examine hybrid solutions where both classical cryptography algorithms and PQC algorithms working together to mitigate the uncertainties in the pace and development of quantum computers and the reliability of candidate PQC under the global standards community.

13.1. Recommendations for Healthcare and GDPR Covered Entities

HLF and other permissioned blockchains present unique opportunities and vulnerabilities in managing cybersecurity risks. As the healthcare industry, financial services, and GDPR covered industry begin to experiment with and commit to pilots, these entities need to understand that the risks are

appropriately identified, and this is a risk management plan. This risk management plan is required for regulated data, and there must be one for enterprise blockchains. Therefore, beyond the hype of any new technology, a thorough cybersecurity program remains vital, and all parties need to conduct due diligence to protecting the network and participating organizations from cyber threats. Also, the participation of multiple entities, each with their on-ramps into the enterprise blockchain, is a potential source of vulnerability.

Ask blockchain vendors about their quantum-safe features to protect data that is under regulatory guidance

- Query software-as-a-service or third-party platform providers about their embedded cryptographic methods and plans for an ecosystem-level solution to protect organizations and maintain contractual obligations.
- Determine how to implement best the GDPR principle of "the right to be forgotten."
- What is the ability to detect, correct fraudulent, malicious, or erroneous records?
- It is unclear which organization will be considered as the data controller and processor within the Fabric and enterprise blockchains, especially when they cross international borders.
- Create new quantum-proof policies, methods, and procedures aligned to use cases/requirements. Update asset inventory with newly implemented cryptographic details.

Healthcare, GDPR, and financial entities must not think that there are no risks associated with blockchain enterprise blockchain networks and must ask for documented risk management strategies to protect regulated data. As the HLF blockchain ecosystem becomes more diverse and grows in popularity, vendors, users, and implementors must be aware of possible cyber-attack. While blockchains offer unique structures and provide cybersecurity capabilities that are not present in today's networks, reasonable measures must be taken. The cybersecurity risk must be evaluated, documented, and its implications considered when regulated, businesses policymakers, and institutions commit protected data to any enterprise blockchain.

14. Conclusions and Future Work

This work has shown that HLF, enterprise blockchains, and current global PKI that relies on the PKI X.509 standard to ensure secure communication between various network participants are utterly vulnerable to the quantum computing threat. Falsified certificates destroy the trust, integrity, confidentiality, and non-repudiation in the entire blockchain and can have enormous consequences if measurements are not taken. It has been shown that quantum computers break ECC on which PKI depends and therefore exposes its implementers and users to potentially massive fines for non-compliance and security incidents with GDPR, FINRA and HIPAA laws. Enterprise Blockchains such as HLF are being adopted in many industries that have regulatory controls over the data. For example; GDPR regulates European Union citizens' data with the potential of massive fines irrespective of the location or headquarters of the blockchain implementation location. Financial and PII data privacy and information is becoming more heavily regulated, especially on Wall Street and in the state of New York and California. In the United States, healthcare data privacy is a significant issue with the increase in cyber-attacks, and the resulting lawsuits, fines, and penalties levied on violators.

The author argues that blockchain technology has the potential to address the documented issues of legacy health and financial information technology systems, such as interoperability, data access, speed, and privacy and the ability to adapt to changing programs. However; out-of-date cryptographic standards will be broken and will not forestall any adversaries from breaking their encryption and gaining access to highly regulated data and information. Development and deployment plans need to be developed to accommodate the most practical hybrid PQC algorithms that are working towards global standardization. Also, blockchain cybersecurity policy is required to govern acceptable use and should include standards, procedures, and guidelines.

Cybersecurity should begin with an assessment that includes current security policies, identification of objectives, review of requirements, and determination of existing vulnerabilities. It is imperative to begin the development of "Policy Recommendations for Enterprise Blockchains" because covered entities must know that placing their data on permissioned blockchains does not and cannot negate risks and obligations. All must understand the risks before committing regulated data, because it is required, and it is also prudent in protecting PHI, PII, GDPR, and FINRA regulated data and information. An evidence-based approach is needed to mitigate and adhere to cybersecurity regulation. All aspects must be considered such as geographic boundaries, jurisdictions and a

thorough understanding of the impact of widespread governance of global regulators

As cyber threats to the HIPAA and GDPR and covered financial entities continue to grow in dedication and sophistication permissioned blockchains can contribute to add "new and advanced cybersecurity techniques" and can be a valuable tool in mitigating those threats if the risks are understood and mitigated. Permissioned blockchains offer significant cybersecurity capabilities, share some of the same cyber risks that affect other IT systems, and have unique characteristics, all of which merit further evaluation by regulators and industry. The author encourages new conversations about the cybersecurity benefits of blockchain systems and ways to promote appropriate government policies.

Finally, this research does not indicate any of NIST Second Round candidate algorithms will be a simple "drop-in replacement," and it may require additional NIST rounds and years of follow-on research, analysis and testing for a suitable "drop-in replacement," can be identified or developed. Therefore, the author believes that qTESLA offers a possible near-term "Hybrid Quantum Resistant-Classical Public Key Infrastructure," a solution with a significant reduction in its public key size. As discussed, it is the public key that is exposed and used the most in today's PKI systems, and it is possible to modify the X.509 certificate standard to accommodate this new PQC algorithm that would only provide the public key that would be much more resistant to implementation and quantum computing attacks. Additional work and testing are needed in large scale real-world scenarios to ensure there are no significant issues with incorporating PQC PKI X.509 certificates on an industrial scale. Potential problems that need to be examined are latency, overhead, and the ability for software, hardware, and other constrained devices to interoperate such as, smartphones, smart cards, and IoT. Regardless of the estimated time of arrival of large-scale quantum computers, cybersecurity should be a primary concern to enterprises and healthcare organizations because they cannot afford to have their private communications and data decrypted even if it is ten years away.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
RC[1] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
RC[1] want to thank his PhD supervisor Dr. Ian McAndrew, Dean of doctoral programs, Capitol Technology University, for his dedication, encouragement and expert guidenace in this research.

References:

[1] J. Emond, "IBM Newsroom," 24 January 2019. [Online]. Available: https://newsroom.ibm.com/2019-01-24-Aetna-Anthem-Health-Care-Service-Corporation-PNC-Bank-and-IBM-announce-collaboration-to-establish-blockchain-based-ecosystem-for-the-healthcare-industry. [Accessed 16 May 2019].

[2] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," *The Journal of the British Blockchain Association,* vol. 2, no. 1, pp. 17-24, 2019.

[3] NIST, "Second PQC Standardization Conference," 22 August 2019. [Online]. Available: https://www.nist.gov/news-events/events/2019/08/second-pqc-standardization-conference. [Accessed 16 May 2019].

[4] NIST, "Second PQC Standardization Conference," 22 August 2019. [Online]. Available: https://www.nist.gov/news-events/events/2019/08/second-pqc-standardization-conference. [Accessed 16 May 2019].

[5] E. Commission, "2018 reform of EU data protection rules," [Online]. Available: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. [Accessed 16 May 2019].

[6] G. EU.org, "Fines and Penalties," [Online]. Available: https://www.gdpreu.org/compliance/fines-and-penalties/. [Accessed 16 May 2019]

[7] D. o. H. a. H. S. Office for Civil Rights, "Federal Registry," [Online]. Available: https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-95. [Accessed 16 May 2019].

[8] "CNBC interview: Harriet Green, Chairman and CEO of IBM Asia Pacific," , . [Online]. Available: https://www.cnbc.com/2018/03/30/ibm-sees-quantum-computing-going-mainstream-within-five-years.html. [Accessed 11 7 2019].

[9] A. M. V. V. K., Z. M. Jøsang, "The Impact of Quantum Computing on Present Cryptography," Arxiv, 31 March 2018. [Online]. Available: https://arxiv.org/pdf/1804.00200. [Accessed 16 May 2019].

[10] H. U. M. M. S. D. Bindel Nina, "Transitioning to a Quantum-Resistant Public Key Infrastructure," PQCrypto-BHMS17, 2017. [Online]. Available: https://s3.amazonaws.com/files.douglas.stebila.ca/files/research/papers/PQCrypto-BHMS17.pdf. [Accessed 16 May 2019].

[11] Hyperledger, "Fabric CA User's Guide," [Online]. Available: https://hyperledger-fabric-ca.readthedocs.io/en/latest/users-guide.html#table-of-contents. [Accessed 11 6 2019].

[12] "NIST Special Publications - NIST Computer Security ..., ",. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html. [Accessed 7 1 2019].

[13] L.. Chen, S. P. Jordan, Y.-K.. Liu, D.. Moody, R. C. Peralta, R. A. Perlner and D. C. Smith-Tone, "Report on Post-Quantum Cryptography | NIST," , 2016. [Online]. Available: https://nist.gov/publications/report-post-quantum-cryptography. [Accessed 30 12 2018].

[14] N. Bindel, "Submission to NIST's post-quantum project (2nd round)," 2019. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions. [Accessed 11 6 2019].

