Mitigating Quantum Computing Threats and Attacks

Robert E. Campbell, Sr.

Capital Technology University

Author Note

This paper includes three prior peer-reviewed published works by the author that examines and surveys technical challenges and considerations in combating imminent quantum computing threats. These works are in the appendices section.

MITIGATING QUANTUM COMPUTING ATTACKS

Ph.D. of Technology Exegesis for Robert E. Campbell Sr.

presented on **September 5th, 2020**

APPROVED:

_____

Chair, Capital Technology University

_____

External Examiner

_____

Dean of Doctoral Programs, Capital Technology University

I understand that my exegesis will become part of the permanent collection of Capital Technology University. My signature below authorizes the release of my exegesis to any reader upon request.

_____

Robert E. Campbell, Sr.

Abstract

In 2019, we saw Google claim “Quantum Supremacy,” indicating that the pace of quantum computing has been underestimated and poorly understood. We have also seen rapid distributed ledger technology adoption in enterprise networks and critical infrastructure, with little progress in the replacement of or upgrading of one of the most fundamental aspects of cybersecurity, which is cryptography. While the U.S. National Institute of Standards and Technology (NIST), and other international organizations are working towards the standardization of Post Quantum Cryptography (PQC), there are compelling and low-cost solutions and steps available today that instantly strengthens standardized cryptography systems. Specifically, quantum technologies such as Quantum Random Number Generators (QRNGs), versus Random Number Generators (RNGs), and Quantum Key Generation (QKG), are Information-Theoretic Security (ITS) and not bound by mathematics, as most widely used standardized cryptography. Instead, the technologies use quantum mechanics and information theory, that ignores the computational power of the most sophisticated and well-resourced adversary. This exegesis links and discusses three prior peer review published research examining the complexities, hurdles, and gaps in migrating to PQC and quantum technologies such as QRNGs. Together, this work adds to the body of quantum technologies knowledge in understanding imminent quantum computing threats, and by offering practical, low-cost mitigation techniques and technologies.

Keywords: *QNRG, ECDSA, DLT, blockchain, quantum-resistant cryptography, lattice-based cryptography, entropy, digital signature algorithms, Hyperledger, PKI, cyber-resilience, critical infrastructure, Pseudo-Random Number Generator, OpenSSL*

DEDICATION

I would like to sincerely acknowledge essential people who have accompanied me on this journey to my Ph.D. Without hesitation, I owe an enormous debt of gratitude to Dr. Renee Bovelle, who has supported and pushed me through good times and hard times to succeed. Secondly, I would like to thank my advisor, Dr. Ian McAndrew, for his infinite patience and dedicated instruction, and who also conspired affectionately with Dr. Renee Bovelle to encourage me to complete this significant achievement. And last but by no means least to my sons, Robert Campbell, Jr., Kevin Campbell, and family and friends for all their understanding and encouragement.

Mitigating Quantum Computing Threats and Attacks

I. INTRODUCTION

In 2008, a paper entitled “Predictable PRNG in the vulnerable Debian OpenSSL,” revealed that the RNG in Debian’s OpenSSL package was predictable [1]. This vulnerability was caused by a software update in 2006 by a Debian developer. The developer removed a section of code used in the seed generation process of the RNG [2]. The research later revealed that the piece of code the developer removed was vital for the security of the cryptographic system because it was responsible for mixing in random data into the seed. In 2008 Debian patched the code and provoked a worldwide regeneration of all keys generated by the faulty RNG [3] [4].

In 2010, a hacker group reported that they recovered the Elliptic Curve Digital Signature Algorithm’s (ECDSA) private key that is used by Sony to sign software for their PlayStation 3 game console [5]. This vulnerability was caused when Sony failed to generate a new random nonce for each signature. Because they used the same nonce for multiple signatures, they revealed information about their private key, and eventually, the hacker group recovered the full key, which caused them to be able to sign any software for the PlayStation 3. Hackers used this exploit, copied, and downloaded unlicensed games at will. The exploit also allowed official malware showing as officially signed software by Sony, which could infect the systems of unsuspecting PlayStation 3 users.

In 2012, a flaw was discovered in TLS (Transport Layer Security) and SSH (Secure Shell) servers involving weak security keys [6]. The malfunctioning RNGs produced low-entropy randomness for the RSA (Rivest–Shamir–Adleman) and Digital Signature Algorithm (DSA) key generation process, which caused the private keys to be compromised. The vulnerabilities in the randomness generation caused many TLS certificates and SSH keys to be

easily factorable, and they were compromised. Obtaining these security keys compromised the entire TLS and SSH system.

In 2013, a vulnerability was revealed in the Java library java.security, in the class SecureRandom. This flaw caused SecureRandom to have colliding values, and as a result, it could generate the same output twice. The SecureRandom had a massive entropy flaw because the output had become predictable. Therefore, algorithms that depended on SecureRandom to generate keys or other cryptographic randomness were also compromised. One of these dependent algorithms was used in the Android Bitcoin wallet. The Android Bitcoin wallet uses the ECDSA algorithm to sign Bitcoin transactions, which was the same algorithm used by Sony to sign the PlayStation 3. The ECDSA signature algorithm was using the SecureRandom Java class on Android devices to generate a random number for each signature. Because of the security flaw, the same random number can be created for two different signatures. Using the equal random value for the ECDSA signature algorithm compromised security because an attacker can then quickly recover the private key [7]. Using the private key, an attacker can sign any transaction and therefore steal Bitcoins from the affected Bitcoin wallet. This vulnerability had a substantial impact because all Android users with Bitcoins stored on their Android devices were at risk of having their Bitcoins stolen by attackers. After this vulnerability was revealed, Google and Bitcoin have released a security update [7].

In 2013, the Taiwanese Citizen Digital Certificate flaw was discovered and presented a paper at Asiacrypt 2013 [4][8], where they showed that official citizen identification smartcards issued by the Taiwanese governments were flawed and had low entropy security keys. They attributed weak RSA keys to a fatal flaw in the hardware RNG. The randomness used for the RSA key generation contained insufficient entropy and created predictable patterns and shared

RSA primes. The smartcards were utilized for multiple security-sensitive processes, and the attackers could forge smartcard holders' digital signature and steal identities.

A. Motivation

Cryptographic core algorithms have been well studied and analyzed; however, other essential elements in organizational cryptographic systems, such as entropy and random numbers, are not well understood. And yet, random numbers support the security of every modern communications system, including the Internet. Random numbers are used for secret key creation, Transmission Control Protocol/Internet Protocol (TCP/IP) sequence numbers, TLS nonces, Address Space Layout Randomization (ASLR) offsets, password salts, and Domain Name System (DNS) source port numbers, and many more applications. There are many examples of cryptographic systems that are broken by an attack on their RNGs and their random seeds. The consequences of these attacks range anywhere between a minor security leak and a total security disaster [8]. It is important for developers and implementors to understand what interfaces to use, and how to handle random numbers correctly in their code. It is also crucial for users to understand the limitations of such code.

According to Forbes, the current global cybersecurity market is worth $173B in 2020, growing to $270B by 2026. Cybersecurity issues are now a significant economic, political health and safety, and national security issue for the entire planet. To successfully fight against malicious intent, organizations must make cybersecurity awareness, prevention, and security best practices a priority.

B. *Results*

Entropy

Cryptography defines the term “entropy” as a measure of the unpredictability of a secret or private key within cryptographic systems. We find entropy in entropy-based hash functions, mathematical and algorithmic foundations of applied cryptography, in advanced design and analysis of cryptographic algorithms, authentication, access control, privacy protection, trust computing, and entropy-based networks. RNGs are excellent starting points for hackers or security researchers to explore weaknesses in the most sophisticated and advanced encryption algorithms. The definition of entropy can also be stated as an expected value, $H(X) = E_X [- \log P_X(X)]$ [9](1). Similarly, H (X|Y) is the average number of bits required to describe X when Y is already known. Alternatively, the amount of entropy measured in bits that X is associated with and denoted by H(X) and $H(X) = - \sum_{i=1}^{n} i \; p_i \log_2 p_i$ [9] (2). An example of common sources on entropy is shown in Fig. 1. below:

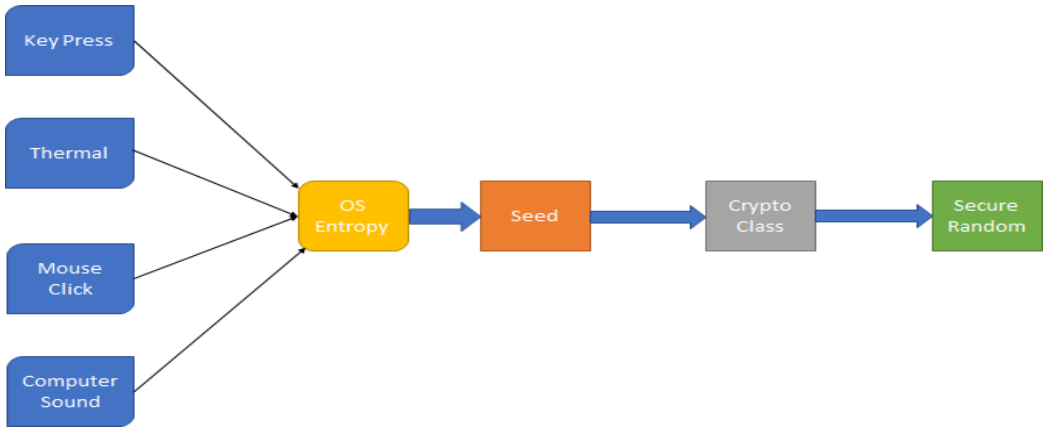

Figure 1. Common Sources of Entropy: Source Whitewood Encryption Systems

I. RNGs

The strength of the computational cryptographic system lies in its keys and the randomness of bits. The foundation of secure keys is the amount of randomness, or entropy, used in the generation of the keys. Low-entropy RNGs produce encryption keys that can be compromised, and it is possible for PRNGs that have been certified as "cryptographically secure" to be insufficiently random, once fault-tolerant quantum computers become commercially available. The RNGs provide entropy, which seeds the key generator that creates the key. The higher the degree of entropy, the more secure the key is. Most systems today use a process called PRNG. Classical computer systems cannot generate true randomness and sustained throughput rates necessary. Information from traditional inputs such as mouse movements, keyboard pressures, disc interrupts, system timers, or thermal is not sufficient to seed today's cryptography systems against the current and the future threat environment. (see Fig. 1 and Fig. 2). Security researchers found that these methods of entropy are not generating enough information to produce truly random numbers. Lack of entropy was also to blame for many reported security breach incidents; however, the source of the events are seldom reported as the lack of "entropy" as being the real source of the data breaches. Understanding entropy in its critical role of strong encryption schemes is not generally well recognized and not often addressed, but extremely important. The following is a high-level description of three distinct types of RNGs: PRNGs, True RNGs or TRNGs, and QRNGs. Some of the crucial parameters to look for in a random number generator are entropy density and throughput. Throughput is defined as sustained high-quality entropy at high rates sufficient for modern networks, communication systems, and cryptographic systems.

PRNGs

A PRNG uses computational algorithms to produce long sequences of pseudo-random numbers or symbols. A PRNG uses an algorithm into which an initial seed value is fed to define the generator's state. The algorithm then performs a series of operations using the seed value and generates a stream of data much longer than the seed itself. Depending on the implementation and application of the PRNG, the seed value might come from a physical RNG, a table of predetermined values, or another source. OpenSSL is an open-source software library used in Hyperledger Fabric and many other distributed ledgers, networks, and applications to secure communications (Fig. 2) [10].

In contrast to the other RNG types, a Pseudo-RNG is low cost and widely used. However, there is a lack of standardized origin of the random seed, and is not portable, and, hence, not suitable for high-quality cryptography. The NIST has certified some approaches as being "cryptographically secure" and acceptable for use in high-security settings. However, it is essential to note the limitations of PRNGs in general:

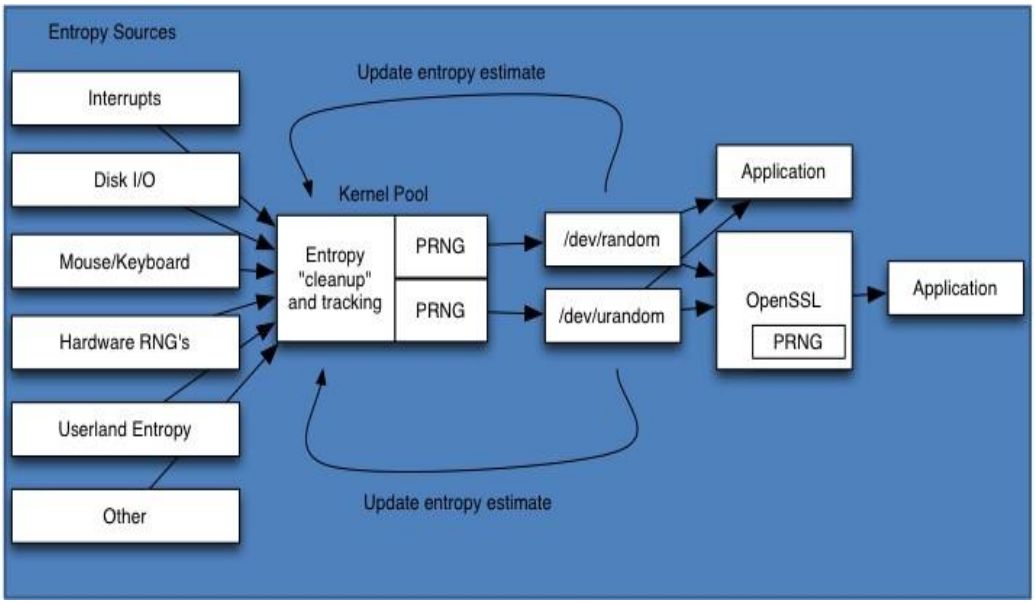

Figure. 2. Entropy Lifecycle

1. Deterministic design: A pseudo-random number generator has no intrinsic entropy and can never produce truly random data. The algorithms used are deterministic by nature, so a given seed value; it will always produce the same output.
2. Potential for hidden defects: PRNGs using outdated or poorly designed algorithms generate predictable data. However, flawed algorithms are often difficult to identify until it's too late when the weakness has been exploited.
3. Implementation issues: Even cryptographically secure PRNGs are dependent on the proper configuration and implementation to function correctly. As with flawed algorithms, improper implementations are often difficult to identify until after a vulnerability has been used in an attack.

A. Potential Attacks

Due to the limitations of pseudo-random number generators and traditional physical RNGs, information encrypted using these technologies may be vulnerable to a variety of attacks. Attacks can take many forms, but they typically follow one of the strategies listed below:

1. Analysis of PRNG output: Attackers can evaluate the data stream produced by a PRNG and look for patterns, which can be analyzed and used to decrypt protected information. This is generally unfeasible against a cryptographically secure PRNG but is a significant concern with weaker algorithms or flawed implementations.
2. Knowledge of PRNG inputs: Since all PRNGs are deterministic, knowledge of the seed will allow an attacker to reproduce the generator's output. When a PRNG is seeded from a low entropy source, hackers may be able to guess the seed value with relative ease. This vulnerability gained attention in the early days of the Internet when a low-entropy PRNG

allowed hackers to decrypt Netscape's SSL-encrypted traffic using only consumer-grade technology [11].

B. TRNG

TRNGs take their random numbers from classical physical processes, which, for all practical purposes, are unpredictable. TRNGs produce random data by "collecting entropy," meaning that they measure events that are expected to be random. Entropy can be collected from the external environment (using phenomena such as ambient sounds or even cosmic background radiation), or from within a computer (using events such as hard drive activity, voltage fluctuations, or keyboard and mouse interactions). One area of concern regarding TRNGs is the possibility that the events being measured could be manipulated to produce predictable output. This scenario, while unlikely in most environments, cannot be ruled out entirely when extremely sensitive data is in question. A more practical concern is that most TRNGs produce data at unacceptably low throughput (number of bits generated per second) due to limitations in the phenomena measured. Organizations relying on these devices must compromise on either the level of entropy in their data or the speed at which cryptographic functions can be completed, either one of which can put sensitive information at risk. TRNGs based on noise in electronic circuits are very cheap and small. The difficulty is that the quality of the random numbers produced by TRNGs is questionable and challenging to assess. It is a considerable task to construct a good TRNG and practically impossible to certify it. For that reason, TRNGs often involve complicated post-processing of the random numbers, which makes them like PRNGs.

C. QRNG

While some TRNG technology was able to provide full entropy, it could not deliver the throughput needed for enterprise-scale and grade applications. Organizations were forced to

accept the tradeoff of lower entropy to gain the volume of random data they required. Today, however, developments in the field of QRNG have made this compromise unnecessary. Quantum random number generators can produce full-entropy random data at speeds of up to Gbits/second, equivalent to the output of the highest-capacity PNRGs and enough to meet the needs of even the largest organization. QRNGs detect random quantum effects and convert those fluctuations into a stream of binary digits. As quantum phenomena are random, the data generated by a QRNG has full entropy and cannot be predicted by any means. The output from a QRNG can be used for the key generation or any other cryptographic use, without the need for an external seed or different potential vulnerability. Together with robust encryption algorithms and secure key management practices, random data is a foundational element of cryptography. This approach eliminates the tradeoffs associated with other random data sources and provides the highest possible security against potential key attacks.

D. OpenSSL 3.0.0

Keys can be generated from many sources of entropy, through a key management system, hardware security module (HSM), or by a trusted third party (TTP), which should use a cryptographically secure QRNG for seeds. Computer applications can pull directly from /dev/random or /dev/urandom to get random numbers as needed (see Fig. 3) [12]. OpenSSL is one of the largest consumers of random numbers and is strong, enterprise-grade, a toolkit for TLS and SSL protocols, and it is also a general-purpose cryptography library [10]. OpenSSL is licensed under an Apache-style license, for commercial and non-commercial purposes subject to license conditions. OpenSSL is also equipped with its own PRNG that it uses to perform its cryptographic library operations. In OpenSSL 3.0.0 the PRNG is seeded by a call to BCryptGenRandom, and CryptGenRandom for Windows*, getentropy, getrandom, /dev/random,

/dev/srandom, and /dev/hwrandom for Unix-like, and SecRandomCopyBytes for iOS (see fig. 3)[10] . OpenSSL 3.0.0 provides cryptographic capabilities both through a command-line interface and through a library that is linked to a wide variety of software packages. OpenSSL is also used by Hyperledger Fabric and is often used as a source of entropy. OpenSSL 3.0.0 is the latest version and has made some architectural changes [10]. The biggest single change is the introduction of a concept called "Providers." In OpenSSL 3.0, all cryptographic algorithms will be implemented in a provider [10].

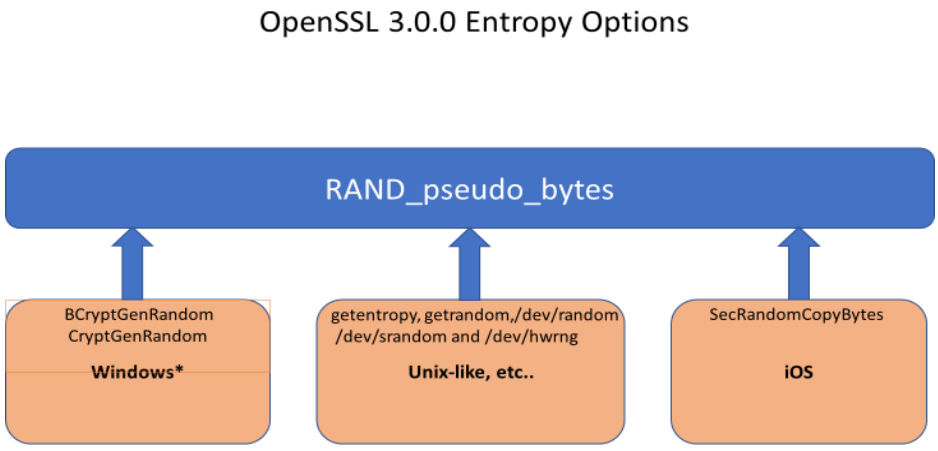

Figure 3. Abstraction of OpenSSL 3.0.0 Architecture

Random data for cryptographic applications is obtained from a physical RNG, a software-based PRNG, or a combination of the two. These technologies, when properly implemented, can pass standard tests for randomness and cryptographic security. However, most of today's conventional approaches to random number generation have limitations which can leave sensitive data vulnerable to attack. It is highly recommended that these sources be replaced with QRNGs, which exploit physical processes that are fundamentally random and have the

supreme advantage over classical RNGs. QRNGs always produce high-quality entropy, and today the, throughput levels are commercial-grade and are relatively low cost to implement.

Hyperledger 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) [13]. Fabrics' distributed ledger depends upon the security and reliability of Public Key Infrastructure (PKI) cryptography (Root-of-Trust), as depicted in the diagram labeled (Fig. 4). Encryption and digital signature algorithms are used to ensure confidentiality, integrity, and authenticity of messages, data. PKI is used to attach identities and public keys while Hyperledger Fabric's Certificate Authority (CA), is the primary trusted party which uses digital signature algorithms to sign certificates of trust. The MSP distributes X.509 certificates that can be used to identify components tied to an organization. X.509 certificates are used in client transaction proposals and self-executing contracts with the terms of the agreement or smart contract transactions. The member's public key is distributed within and contained in the certificate, while the private or secret key is not. Digital identities are validated digital certificates that comply with X.509 standards and are issued by a Certificate Authority (CA). Hyperledger Fabric uses self-signed (X.509) certificates to create the root of trust and a list of self-signed (X.509). A CA dispenses certificates that are digitally signed by the CA and bind together the actor with the actor's public-key [13].

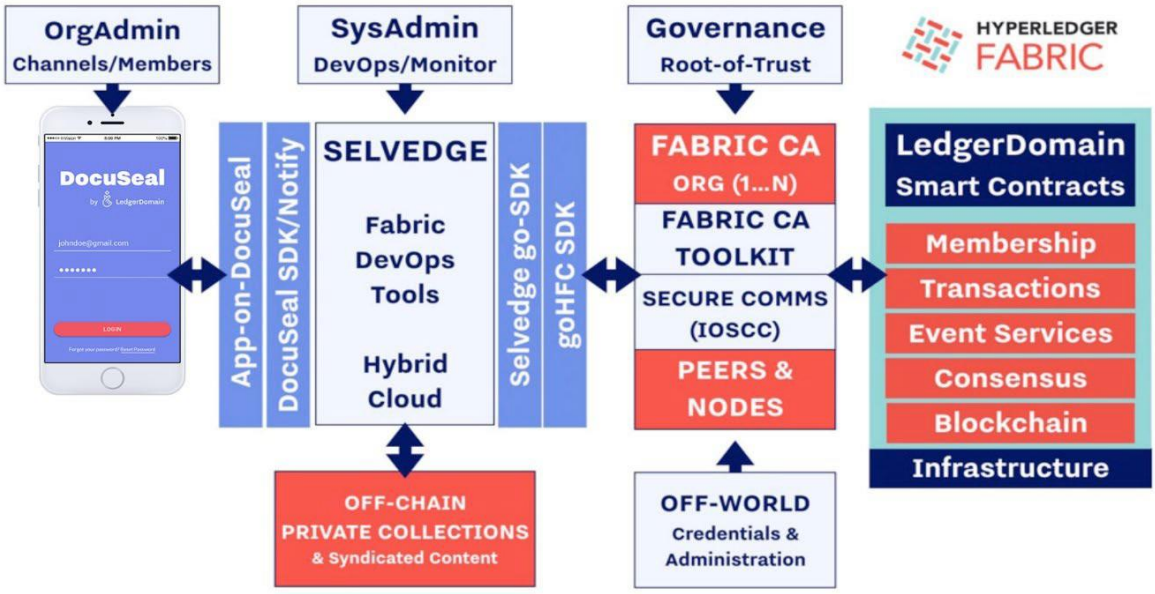

Figure 4. Hyperledger Fabric Architecture Overview. Source: Fabric Web

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. 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 the amount of entropy. Unfortunately, there has been little progress in updating or replacing the standard RNGs, in which most cryptographic systems depend. The quality and throughput levels of the random numbers are used directly to determine the security strength of the system. The high-level diagram below (see Fig. 5) illustrates how the Hyperledger Fabric CA server fits into the overall Hyperledger Fabric architecture [14].

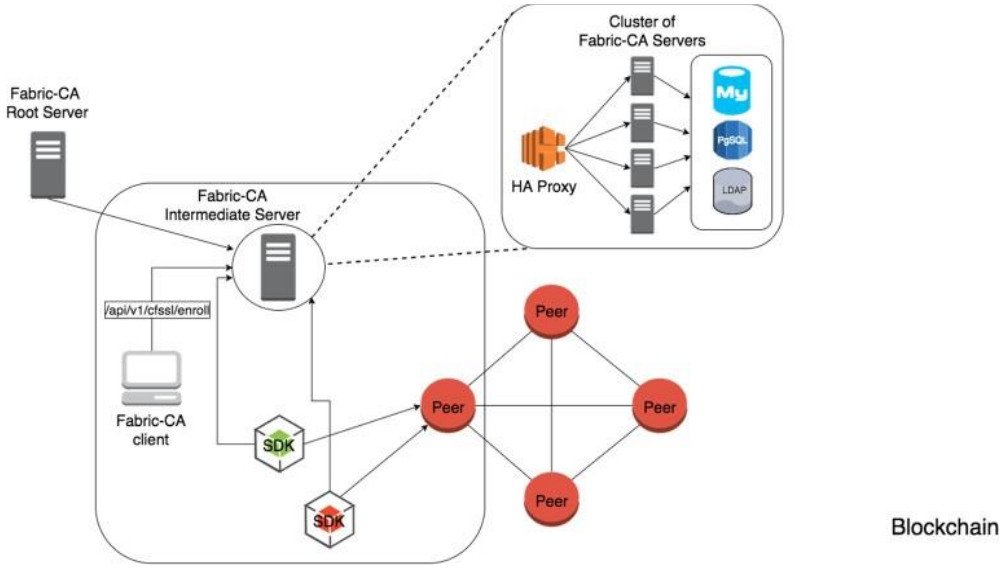

Figure 5. Hyperledger Fabric CA Architecture.

Hyperledger Fabric offers two options to access the CA server: via the Hyperledger Fabric CA client or through one of the Fabric Software Development Kits (SDKs). The Fabric CA client or SDK may link to a server in a group of Fabric CA servers. Fabric's server configuration file contains a Certificate Signing Request (CSR) section that can be configured [14]. The CSR can be configured to generate X.509 certificates and keys that support ECDSA. These algorithms are also a crucial component in the security properties of many protocols, standards, and services. The ECDSA is a prolific algorithm and is used in many other instances such as, in Bitcoin, Internet Key Exchange (IKE), Pretty Good Privacy/Gnu Privacy Guard (PGP/GPG), Secure/Multipurpose Internet Mail Extensions (S/MIME), digitally signed portable document formats [PDFs]), Z and Real-Time Transport Protocol (ZRTP), and Secure Internet Live Conferencing (SILC) all rely on asymmetric encryption and decryption [15]. The choice of algorithms and key sizes are based on security needs. Hyperledger Fabric offers standard ECDSAs in the following key size options [14] (see Table 1):

ECDSAs in the following key size options [14] (see Table 1):

Table 1. Hyperledger Fabric ECDSA Options

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

Some Known Attacks Against ECDSA

Physical attacks are potent tools that can be used against vulnerabilities of elliptic curves, such as side-channel attacks and twist-security attacks [15]. Side-channel attacks consist of passive attacks that attempt to recover secret information from the physical leakage of cryptographic computations, such as the timing of operations or device power consumption. While, fault analysis consists of active attacks that seek to learn secrets by deliberately tampering with the device to cause a malfunction or otherwise unexpected behavior, by modifying the voltage source at carefully chosen points in time or causing sudden changes in the device to cause information leaks. Twist-security attacks can be broken down into categories including small-subgroup attacks, invalid-curve attacks, and invalid-curve attacks against Montgomery ladders. During timing attacks, the malicious user measures the difference in time between observed peaks in power consumption. When different operations or input values have a significant time variance, the attacker can deduce the secret key.

The following setting is an example of the implementation of Elliptic Curve Digital Signature Algorithm (ECDSA) with curve prime256v1 and signature algorithm ECDSA-with-SHA256: Normal computations needed for ECDSA authentication are the generation of a key pair (secret key, public key), the generation of a signature, and signature verification.[15][16]. The hardness of ECDSA comes from solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) [5]. ECDSA algorithm descriptions:

ECDSA Key Pair Generation

A random number generator is started and seeded, and when its operation is completed, it delivers the numeric value that becomes the secret key d (a scalar). Next, the public key Q (x, y) is computed according to Equation 1 through point multiplication:

$$Q(x, y) = d \times G(x, y) \qquad (1)$$

(see Fig. 6 below) [17].

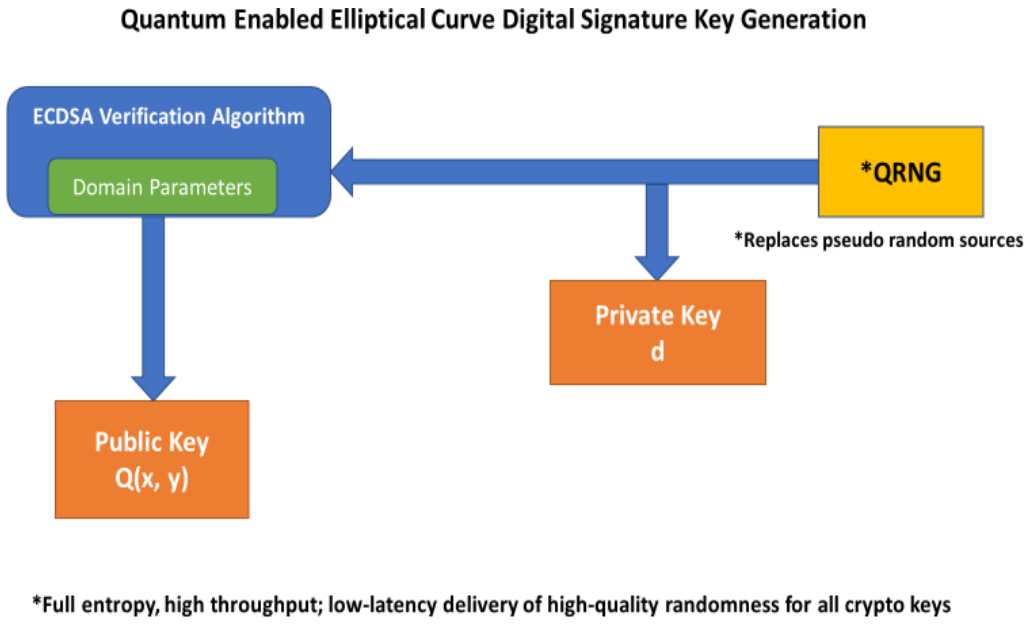

Figure 6. QRNG Enabled Hyperledger ECDSA

Signature Computation

The first operation consists of converting the variable-length message to a fixed-length message digest h(m) using a secure hash algorithm [17]. Once the message digest is computed, a random number generator is activated to provide a value k for the elliptic curve computations. The resulting signature contains two scalar integers, r, and s. Equation 4 shows the calculation of r from the indiscriminate number k and the base point

$$G(x, y): (x_1, y_1) = k \times G(x, y) \bmod p \quad (3)$$

$$r = x_1 \bmod n \quad (4)$$

The integer r cannot be zero, and when r is 0, a new random number, k, must be created. When r is computed, s is calculated corresponding to Equation 5 using scalar operations. The process then accepts inputs as the message digest h(m); the private key d; r; and the random number k: $s = (k^{-1} (h(m) + d * r) \bmod n$ [18] (see Fig 7). (5)

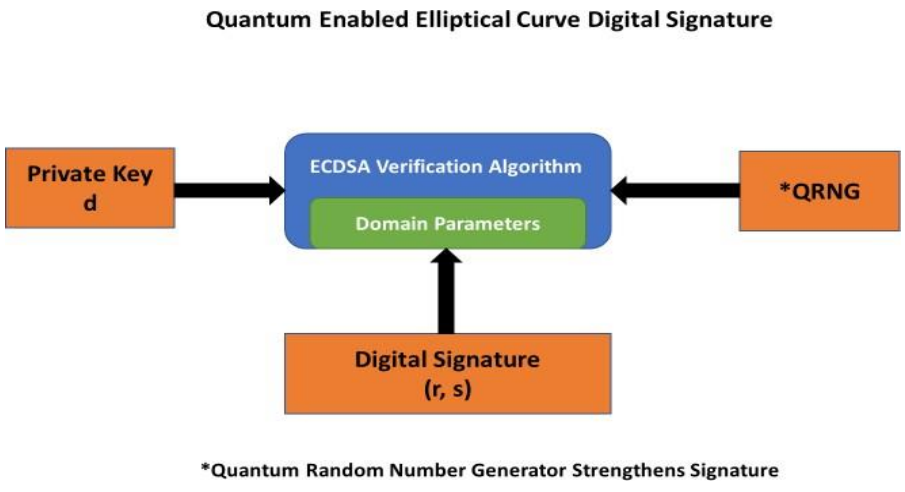

Figure 7. QRNG

Contributions to the collected knowledge from this research

The contributions of this dissertation include assisting in Independent Evaluation, Verification, and Testing (IV&V) of NIST PQC candidate cryptography algorithms. The standardization, migration, and transition to new PQC is an enormous task with significant implications and many uncertainties. PQC is unlikely to be a simple plug-in-play transition into days enterprise networks and requires an understanding of an entirely new class of algorithms with parameters and security models not solidly established and studied. Given the nature and intricacy of PQC, it will take years of planning for a successful migration. The U.S. and the international community will require reliable plans for transition, and it must begin now. The contributions to the collected knowledge are contained in three published articles located in the appendix. Briefly, the contributions are as follows;

Appendix: The first published paper titled "**Evaluation of Post-Quantum Distributed Ledger Cryptography**," the author evaluates the current cybersecurity vulnerability of the prolific use of Elliptical Curve Digital Signature Algorithm (ECDSA) cryptography in use by the Bitcoin Core, Ethereum, Bitcoin Cash, and enterprise blockchains such as Multi-Chain and Hyperledger projects Fabric and Sawtooth Lake. The author's original contribution includes making recommendations for improvements and documenting cybersecurity vulnerabilities in blockchains that are being used in media, health, finance, transportation, and government. Information produced in this study can be used as part of a plan and strategy for mitigation and migration to safer public-key cryptography. The author also discovered; currently, there is not an explicit agreement on the best way to measure quantum attacks. It is, nevertheless, fundamental that work continues with alternatives that will produce smaller key sizes, less memory, and less CPU time for the signing, key generation, and verification times. The second contribution is the proposal of the most practical PQC lattice-based cryptography that can be implemented near-term and provide a basis for industry-wide coordination.

The time to test and validate new post-quantum cryptology is now, given it takes at least ten years to build and deliver a new public key infrastructure. The pace at which quantum computing advancements can be anticipated is uncertain. The ability to transition to post-quantum cryptology appears to be very complicated, and there are many unknowns concerning establishing, standardizing, and deploying post-quantum cryptography systems. All of this must be completed before the arrival of large-scale quantum computers because the cybersecurity of many vital services will be severely degraded.

Appendix: The second paper published titled " **Transitioning to a Hyperledger Fabric Hybrid Quantum Resistant-Classical Public Key Infrastructure**," the author contribution includes 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 author discovered, 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 PKI. 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. This work also proposes that qTESLA’s public keys be used to create a quantum-resistant-classical hybrid PKI near-term replacement.

Appendix: The third paper titled "**The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework**," the author evaluated critical infrastructure sectors that are increasingly adopting enterprise distributed ledgers to host long-term assets, systems, and information that is considered vital to an organization’s ability to operate without clear or public plans and strategies to migrate safely and timely to PQC. The author's contributions included scenarios and sequences of possible attacks by a quantum computer compromised distributed ledger.

Global enterprises are increasingly adopting distributed ledgers and are hosting critical assets and infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. This study explored the attack surfaces in open-source permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. The author clearly illustrated how eavesdropping, unauthorized client authentication, signed malware, cloak-in encrypted session, a man-in-the-middle attack (MITM), forged documents, and emails attacks could be executed. These attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. This research also discusses, examined single points of failure, multiple security risks in enterprise distributed ledger PKI, areas that can be compromised, and provides an idea of what should be in a PKI distributed Risk Management Framework plan. There is a pressing need to strengthen the critical infrastructures and enterprise sectors further and adopted blockchain information systems, component products, and services. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise.

Recommendations

Technologies such as quantum computing and distributed ledgers are transforming theoretical applications in enterprise networks and critical infrastructure. Additionally, quantum computing requires an understanding of topics and complexities, such as quantum mechanics, optics, and Information-Theoretic Security (ITS). Many years of study and analysis are required to understand the practical strengths and weaknesses of PQC algorithms. The effective transition to PQC will require many months of preparation planning to reduce enterprise and critical infrastructure disruption.

Additional research is needed on approaches to introducing new PQC algorithms (e.g., hybrids) within live systems that must remain interoperable with other systems during the period of industry migration. This includes such areas as penetration testing, formal testing, formal modeling, automated tools, and approaching transition in complex infrastructures. Further research is required on policy, process, and people. We will need a sufficiently trained workforce and coordinated strategies between private industry and government to meet the challenges ahead.

Conclusion

Finally, the author's combined work in this paper investigated essential concepts such as entropy and its use in modern cryptography. Cryptographic systems depend on access to high-quality entropy or random numbers. The problem of high-quality entropy is especially significant in virtual machines, clouds, and containers where there is no direct user activity and, so, the expected sources of randomness are not present. It must be emphasized that random numbers support the security of every modern network and communications system. Cryptographers and research security professionals are well versed in cryptographic algorithm design and theoretical bit security, but not many know how the actual keys are generated, or how entropy is accumulated or its source. Random numbers are the source of long-term key creation, ephemeral key creation, and nonces. QRNG is one of the most mature and commercially available quantum technologies. The innate randomness at the core of quantum mechanics makes quantum systems a perfect source of entropy. It is important for developers and implementors to understand what interfaces to use, and how to handle random numbers correctly in their code. Collectively, in three papers, the author has presented compelling evidence that the explosion of science, engineering, and technology has created an educational, experience, knowledge, and skill gaps. The impact is that practitioners do not have a sufficient understanding of complex topics such as distributed ledger technologies and quantum computing. Mitigating quantum threats require a firm understanding of the fundamentals of cryptography, fault tolerance, distributed consensus, computer science, and quantum mechanics.

References

[1] Luciano Bello and Maximiliano Bertacchini. package: The What and The How. DEFCON16, Las Vegas, Nevada. 2008. https://www.researchgate.net/publication/255569058_Predictable_PRNG_In_The_Vulnerable_Debian_OpenSSL_Package. Accessed, 5/3/2020

[2] Bruce Schneier. Random Number Bug in Debian Linux https://www.schneier.com/blog/archives/2008/05/random_number_b.html. Accessed, 5/3/2020

[3] Debian Security Advisory. Debian. DSA-1571-1 openssl – predictable random number generator, 2008. https://www.debian.org/security/2008/dsa-1571.
Accessed, 5/3/2020

[4] US-CERT/NIST. CVE-2008-0166 Detail. 2008. https://nvd.nist.gov/vuln/detail/CVE-2008-0166.
Accessed, 5/3/2020

[5] Bushing, Marcan, Segher, Sven. 27th Chaos Communication CongressConsole Hacking 2010 - PS3 Epic Fail. 2010. https://fahrplan.events.ccc.de/congress/2010/Fahrplan/attachments/1780_27c3_console_hacking_2010.pdf

[6] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J Alex Halderman. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices https://factorable.net/weakkeys12.extended.pdf.

[7] Android Security Vulnerability 2013 https://bitcoin.org/en/alert/2013-08-11-android. Accessed, 5/3/2020

[8] Daniel J Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko Van Someren. Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild https://link.springer.com/chapter/10.1007%2F978-3-642-42045-0_18. Accessed, 5/3/2020

[9] Information Theory: Entropy, Markov Chains, and Huffman Coding.
https://math.nd.edu/assets/275279/leblanc_thesis.pdf
Accessed, 5/3/2020

[10] OpenSSL 3.0.0 Design. OpenSSL Management Committee (OMC). January 2019.
https://www.openssl.org/docs/OpenSSL300Design.html.
Accessed, 5/4/2020

[11] Random number generation failures from Netscape to DUHK. Nadia Heninger. University of Pennsylvania 2018 https://suri.epfl.ch/slides/2018/nadia-heninger.pdf

Accessed, 5/4/2020

[12] Understanding and Managing Entropy - Black Hat. https://www.blackhat.com/docs/us-15/materials/us-15-Potter-Understanding-And-Managing-Entropy-Usage-wp.pdf

Accessed, 5/4/2020

[13] Building Quantum REsistant Blockchains. The Journal of The..... https://www.slideshare.net/eraser/building-quantum-resistant-blockchains-the-journal-of-the-british-blockchain-association.

Accessed, 5/4/2020

[14] Fabric CA User's Guide — hyperledger-fabric-cadocs master.....https://hyperledger-fabric-ca.readthedocs.io/en/release-1.4/users-guide.html.

Accessed, 5/4/2020

[15] Can Elliptic Curve Cryptography be Trusted? A Brief ..... https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/can-elliptic-curve-cryptography-be-trusted-a-brief-analysis-of-the-security-of-a-popular-cryptosyste.

Accessed, 5/4/2020

[16] Degenerate Fault Attacks on Elliptic Curve Parameters in OpenSSL. Akira Takahashi. Mehdi Tibouchi https://eprint.iacr.org/2019/400.pdf.

Accessed, 5/5/2020

[17] The Elliptic Curve Digital Signature Algorithm (ECDSA).

Dept. of Combinatorics & Optimization, University of Waterloo,

Canda.https://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf.

Accessed, 5/5/2020

[18] ECDSA Authentication System | EEWeb Community. https://www.eeweb.com/profile/maxim/articles/ecdsa-authentication-system

THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-1-(4)2019

Evaluation of Post-Quantum Distributed Ledger Cryptography

Robert E. Campbell, Sr.
Capitol Technology University, USA

Correspondence: rc@medcybersecurity.com
Received: 08 January 2019 **Accepted**: 26 February 2019 **Published**: 16 March 2019

Abstract

This paper evaluates the current cybersecurity vulnerability of the prolific use of Elliptical Curve Digital Signature Algorithm (ECDSA) cryptography in use by the Bitcoin Core, Ethereum, Bitcoin Cash, and enterprise blockchains such as Multi-Chain and Hyperledger projects Fabric, and Sawtooth Lake. These blockchains are being used in media, health, finance, transportation and government with little understanding, acknowledgment of the risk and no known plans for mitigation and migration to safer public-key cryptography. The second aim is to evaluate ECDSA against the threat of Quantum Computing and propose the most practical National Institute of Standards and Technology (NIST) Post-Quantum Cryptography candidate algorithm lattice-based cryptography countermeasure that can be implemented near-term and provide a basis for a coordinated industry-wide lattice-based public-key implementation. Commercial quantum computing research and development is rapid and unpredictable, and it is difficult to predict the arrival of fault-tolerant quantum computing. The current state of covert and classified quantum computing research and advancement is unknown and therefore, it would be a significant risk to blockchain and Internet technologies to delay or wait for the publication of draft standards. Since there are many hurdles Post-Quantum Cryptography (PQC) must overcome for standardisation, coordinated large-scale testing and evaluation should commence promptly.

Keywords: *ECDSA, blockchain, post-quantum, lattice-based cryptography, cybersecurity, distributed ledger, qTESLA, Ring Learning with Errors, critical infrastructure*

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

Competing Interests:
None declared.

Ethical approval:
Not applicable.

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

Funding:
None declared.

Acknowledgments:
RC would like to acknowledge Dr. Ian McAndrew for his supervision and guidance in preparing this research.

1. Introduction

Rapid advances on a global scale in Quantum Computing technologies and the threat it poses to most standardized encryption prompted NIST to put out an international call for candidate quantum-resistant public-key cryptographic algorithms to evaluate for standardization. NIST will conduct efficiency analysis on their reference platform delineated in the *Call for Proposals*; NIST invites the public to perform similar tests and compare results on additional platforms (e.g., 8-bit processors, digital signal processors, dedicated complementary metal-oxide-semiconductor (CMOS), etc.) and provide comments regarding the efficiency of the submitted algorithms when implemented in hardware.

This research has two goals; the first is to examine the vulnerabilities in current Asymmetric Digital Signature Cryptography (ASDC) as used in private key generation in Bitcoin Blockchain technology in the PQC era. The second goal is to independently test and evaluate candidate NIST algorithms to assist in the process of selection of acceptable candidate cryptosystems for standardisation and the proposal of potential replacement of ADSC in private key generation in blockchain and distributed ledger technology. Most blockchain and distributed ledger technologies use an asymmetric digital signature scheme for private key generation such as ECDSA, which has been cloned often from the Bitcoin Blockchain. These digital signature schemes are being implemented in critical sectors of government and the economy. Evaluations will include cryptographic strengths and weaknesses of NIST candidate pool of submitted algorithms. It is expected that the analysis will consist of required performance parameters that include;

Public Key, Ciphertext, and Signature Size, Computational Efficiency of Public and Private Key Operations, Computational Efficiency of Key Generation, and Decryption Failures against NIST provided Known Answer Test values (KAT).

Blockchain and Distributed Ledger cryptography private key generation cyber-security concepts are poorly understood and often misrepresented. There is a misconception that Blockchain technology can't "be hacked," resulting in a general endorsement for critical sectors and industries [1]. The author believes that technology offers excellent cyber-security promise for many areas, but the limitations and strengths must be defined. This work examines the weakness of the ECDSA and its current vulnerability and uses in the Bitcoin Blockchain or Distributed Ledger Technology (DLT). Many industries are rapidly adopting versions or mutations of the first of the Bitcoin Blockchain technology in essential sectors such as information technology, financial services, government facilities, healthcare, and the Public Health Sector seemingly, without cybersecurity due diligence, a proper comprehension of the cryptography vulnerabilities or plans for addressing quantum computing threats [2]. The ECDSA is the foundation of Public Key Infrastructure (PKI) for many Internet applications and open source projects, and it's the primary source for public-key cryptography. The second part of this paper offers the most practical and near-term first-round candidate NIST Lattice-Based Post-Quantum Cryptography solution with a recommendation for immediate coordinated (academia, the private sector, government) independent testing, verification, and validation (IV&V) and test framework for sharing results [3]. This framework aids in speeding the approval of PQC standards that are vital to global cybersecurity. The scope of this work evaluates the lattice-based digital signature scheme qTESLA, based on the verifiable hardness of the decisional Ring Learning With Errors (R-LWE) [4]. Quantum computing's threat adversely affects the cybersecurity of financial services such as payment systems, general network communications systems, business functions including cloud computing, Internet of Things (IoT) and critical infrastructure. Further, the author believes that currently estimated timelines for the availability of large-scale fault-tolerant quantum computers are underestimated due to unpredicted global progress and the veil of secrecy surrounding classified research programs led by organizations and governments around the globe. It is, therefore, essential to begin work and testing the most likely candidate algorithms for normalization.

2. Implications in this work

Current encryption systems and standards such as Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Digital Signature Algorithm (DSA), and ECDSA impact everything from defense, banking, healthcare, energy, telecommunications, intelligence, Internet and the Blockchain. The compromise, disruption or non-availability of one of these sectors would severely impact the health and safety of U.S. national security, public health, safety or its economy.

Blockchain technology is a revolutionary technology that has great potential in many applications. This technology has gained global interest in all industry sectors based on cryptography-based algorithms that are considered vulnerable today but will be increasingly threatened by accelerated advances in quantum computing.

3. Significance of the findings

The time to test and validate new post-quantum cryptology is now, given it takes at least ten years to build and deliver a new public key infrastructure. The pace at which quantum computing advancements can be anticipated is uncertain. The ability to transition to post-quantum cryptology appears to be very complicated, and there are many unknowns concerning establishing, standardizing, and deploying post-quantum cryptography systems. All of this must be completed before the arrival of large-scale quantum computers because the cybersecurity of many vital services will be severely degraded.

4. Bitcoin and Distributed Ledger Technology

The Bitcoin Cryptocurrency (BTC) is the first widespread application of blockchain technology. The critical elements of Blockchain and DLT have been in existence for decades, and they include fault-tolerance, distributed computing, and cryptography. Succinctly, the first iteration of this technology is a decentralized distributed database that keeps records of transactions relatively secure and in an append-only mode, where all peers eventually come to a consensus regarding the state of a transaction. The Bitcoin Blockchain like others operates in an open peer-to-peer (P2P) network, where each node can function as a client and a server at the same time. The nodes in the system are connected over TCP/ IP and once a new node is connected that node broadcast peer IP addresses via Bitcoin address messages. Each address maps to a unique public and private key; these keys are used to exchange ownership of BTCs among addresses. A Bitcoin address is an identifier of 26 to 35 alphanumeric characters [5] . Since the advent of BTC along with its choice of a data structure, called a block, modified blockchain technologies, makes use of different data structures such as Directed Acyclic Graph (DAGs). Therefore, recent versions of the newest blockchains can longer accurately be called blockchains, and it is more appropriate to use the term Distributed Ledger (DL) that applies to all version of the blockchain. Presently, according to Crypto-Currency Market Capitalizations [6], there are more than 2000 alternate cryptocurrencies, and most make use of the Bitcoin Blockchain or are clones with minor differences in the private key generation cryptography and structure. The primary configuration changes include the underlying hash function, block generation times, data structures and method of distributed consensus. However; the critical task of generating private keys in blockchains remains unchanged across most blockchain adaptions, and this work asserts that the foundation of the current cryptocurrency markets and all the private and public sectors using this technology are vulnerable to the same cybersecurity weaknesses.

5. ECDSA, libsecp256k1 and OpenSSL

The ECDSA algorithm is part of public-key cryptography and is also the cryptography the Bitcoin blockchain uses to generate the public and private keys. The ECDSA is used in critical infrastructure, secure communications over the Internet, cellular and Wi-Fi, and in many blockchain forks in use today. Specifically, the Bitcoin blockchain uses the ECDSA and the Koblitz curve *secp256k1* [7], which have significant weaknesses which include general algorithm structure, side-channel attacks, and threats from quantum computers. The Koblitz Curve was not adopted for standardisation by NIST due to the non-random structure of the algorithm. The Bitcoin creator selected a non-NIST P-256 approved curve to serve as a source of entropy. Entropy is defined in this case as the randomness inserted by an operating system or application for use in cryptography that requires random data. OpenSSL is an open-source software library used in BTC technology and ECDSA applications to secure communications and many critical infrastructures. OpenSSL [8] provides software Pseudo-Random Number Generator (PNRG) based on a variety and type of hardware and software sources. Its core library is written in the C programming language. The process starts once the Bitcoin Core client is installed, and the user receives a set of ECDSA key pairs, called Addresses. The PRNG starts in the state unseeded, and this state; it has zero entropy. A call to RAND bytes is made, and it will transfer automatically into the state seeded with a presumed entropy of 256 bits and is feed to the PRNG through a call to RAND add. The keys generated from this process are necessary to transfer BTC from one address to the other. Next, the client needs to sign a specific message (called Transaction) with the private key of the user. The public key is used to check if the given user has rights to BTC [9].

The ECDSA algorithm relies 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.

The Koblitz curve secp256k1 is non-verifiable random and is defined by Standards for Efficient Cryptography Group (SECG), instead of the NIST 186-3 DSS Standard using the elliptic curve secp256r1. The security of the ECDSA algorithm and protocols relies on a source of distributed random bits.

6. Fault Attack on Bitcoin's Elliptic Curve with Montgomery Ladder Implementation.

This Montgomery Ladder Fault Attack method is a fault attack on elliptic curve scalar product algorithms and can be used when the (y-coordinate) is not used. The bit security of the elliptic curve parameters in most cases can be significantly reduced. The Fault attack is a robust side-channel technique that is used to break ECDSA cryptographic schemes. The idea is to inject a fault during the computations of implementation and to use the faulty outputs to deduce information on the secret key stored in the secure component [10]. Table 1 gives the resultant bit security after the Montgomery Ladder Fault Attack.

Table 1: Curve parameter security according to Montgomery Ladder Fault Attack [10]

Values *secp*	P1363 IPSEC	X9.62 X9.63	NIST	Strength	Security
256k1	c/c	c/r		128	**50**
256r1	c/c	r/r	r	128	121

The bold font indicates the scep256k1 security is below 2^{60} since these computations can be easily performed with classical computers. The mention 'r' denotes parameters explicitly recommended in the standard, while the mention 'c' denotes parameters in conformance with the standard. The column "Strength" refers to the standard. Clearly, implementations without protections, the attacker can compute the discrete logarithm in the twist with a cost of 2^{50} operations and retrieve the secret scalar for n = 256.

7. Algorithm Security Strength

Breaking a cryptographic algorithm can be defined as defeating some aspect of the protection that the algorithm is intended to provide. For example, a block cipher encryption algorithm that is used to protect the confidentiality of data is broken if, with an acceptable amount of work, it is possible to determine the value of its key or to recover the plaintext from the ciphertext without knowledge of the key.

The approved security strengths for 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. NIST Special Publication 800-57 Part 1 Revision 4: Recommended for Key Management, as shown in Table 2 [11]. The Fault Attack on Bitcoin's Elliptic Curve with Montgomery Ladder Implementation yields a security strength of only 50 bits, as shown in Table 1.

8. NIST and Post-Quantum Cryptography

In December 2016, NIST formally announced its Call for Proposals (Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms), [12]. This call solicited

Table 2: Comparison of conventional and quantum security levels of typical ciphers [12].

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

proposals for post-quantum digital signature as well as public-key encryption and Key Encapsulation Mechanism (KEM)/Encryption for evaluation. In response, there were 82 total submissions, and 69 were accepted, and five withdrew. The results and categories included 19 Signatures and 45 KEM Encryption. The Signature category, which produces private keys, included five Lattice-based submissions, and this work focuses on qTESLA's submission, which is based on the verifiable hardness of the decisional Ring Learning With Errors (R-LWE) problem [4]. Public Key Systems based on R-LWE is computationally superior over LWE systems because of reduced overhead, greater capacity for message space, and smaller public key sizes.

9. Selected algorithm for test and evaluation: qTESLA

The author's considerations for the selection qTESLA are "reasonable" key and ciphertext sizes, and to a lesser extent, the number of CPU cycles required for encryption, decryption, and verification, and potential incorporation into constrained devices such as smartphones and emerging IoT devices. Additional considerations included trust, metrics, parameters, migration, compatibility, and efficient and secure implementation. This submission utilizes two approaches for parameter generation. The first approach is called "heuristic qTESLA," and it uses heuristic method parameter generation, and the second approach is called "provably-secure qTESLA,"

Table 3: Adapted from The NIST Post-Quantum Crypto "Competition" [13].

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

and its parameter generation is provably-secure. qTESLA includes five parameter sets that correspond to two security levels located in Table 3.

Security levels:

A. Heuristic qTESLA:
   - qTESLA-I: NIST's security category 1.
   - qTESLA-III-speed: NIST's security level 3 (option for speed).
   - qTESLA-III-size: NIST's security level 3 (option for size).

B. Provably-secure qTESLA:
   - qTESLA-p-I: NIST's security category 1.
   - qTESLA-p-III: NIST's security category 3 [4].

The security of lattice-based systems is provably secure under worst-case hardness assumptions. In the author's view, it is not

Table 4: Description and bounds of all the system parameters [4]

Parameter	Description	Requirement
λ	security parameter	-
q_h, q_s	number of hash and sign queries	-
n	dimension (n – 1 is the poly. degree)	power of two
σ, ξ	standard deviation of centered discrete Gaussian distribution	$\sigma = \xi/\sqrt{2\ln 2}$
k	#R-LWE samples	-
q	modulus	$q = 1 \bmod 2n$, $q > 4B$ For provably secure parameters $q^{nk} \geq \lvert\Delta S\rvert \cdot \lvert\Delta L\rvert \cdot \lvert\Delta H\rvert$ $q^{nk} \geq 2^{4\lambda+nkd}\, 4q_s^3 (q_s + q_h)^2$
h	# of nonzero entries of output elements of Enc	$2^h \cdot \binom{n}{h} \geq 2^{2\lambda}$
L_E, η_E L_S, η_S	bound in checkE bound in checkS	$\eta_E \cdot h \cdot \sigma$ $\eta_S \cdot h \cdot \sigma$
B	interval of randomness is chosen during signing	$B \geq \frac{\sqrt{\cdot}}{\sqrt{\cdot}}$, near a power of two
d	number of rounded bits	$\binom{78}{56} \geq 0.3$, $d > \log_+(B)$
b_{GenA}	number of blocks requested to SHAKE128 for GenA	$b_{GenA}\, \varepsilon\mathbb{Z} > 0$
$\lvert\Delta H\rvert$ $\lvert\Delta S\rvert$ $\lvert\Delta L\rvert$		$\binom{D}{EFG} \binom{DOE}{JFG} (4(-B - L_S) + 1)^8 (2^v + 1)^{87}$
δz δw δ_{keygen}	acceptance probability of z acceptance probability of w acceptance probability of key pairs	experimentally experimentally experimentally
sig size pk size sk size	theoretical size of signature theoretical size of public key theoretical size of secret key	experimentally experimentally experimentally
$\varkappa$	output length of hash function H and input length of GenA, PRF_1, PRF_2, Enc and ySampler	$\varkappa \geq \lambda$

Table 5: Parameters for each of the proposed heuristic and provably-secure parameter sets with $q_b = 2^{128}$ and $q_s = 2^{64}$; $M = 0.3$ [4]

Parameter	qTESLA-I	qTESLA-III-speed	qTESLA-III-size	qTESLA-p-I	qTESLA-p-III
λ	95	160	160	95	160
$\varkappa$	256	256	256	256	256
n	512	1024	1024	1024	1024
σ, ξ	23.78, 27.9988	10.2, 12	8.49, 9.9962	8.5, 10	8.5, 10
k	1	1	1	4	5
q	4205569 $\approx 2^{22}$	8404993 $\approx 2^{22}$	4206593 $\approx 2^{22}$	485978113 $\approx 2^{29}$	1129725953 $\approx 2^{30}$
h	30	48	48	25	40
L_E, η_E	1586, 2.223	1147, 2.34	910, 2.23	554, 2.61	901, 2.65
L_S, η_S	1586, 2.223	1233, 2.52	910, 2.23	554, 2.61	901, 2.65
B	2^{20} -1	$2^{21} - 1$	2^{20} - 1	$2^{21} - 1$	2^{23} - 1
d	21	22	21	22	24
b_{GenA}	19	38	38	108	180
|ΔH|				$\approx 2^{435.8}$	$\approx 2^{750.9}$
|ΔS|				$\approx 2^{23551.6}$	$\approx 2^{51199.7}$
|ΔL|				$\approx 2^{94208.0}$	$\approx 2^{2560000}$
δ_w	0.31	0.38	0.25	0.33	0.34
δz	0.44	0.56	0.37	0.78	0.81
δ_{sign}	0.14	0.21	0.09	0.26	0.28
δ_{keygen}	0.45	0.60	0.39	0.59	0.44
sig size	1376	2848	2720	2848	6176
pk size	1504	3104	2976	14880	39712
sk size	1216	2112	2112	4576	12320
classical bit hardness	104	178	188	132	247
quantum bit hardness	97	164	169	123	270

likely that current PQC will be direct replacements for current standards and will likely impact the entire category of Internet protocols, such as Transport Layer Security (TLS) and Internet Key Exchange (IKE).

System parameters can be viewed in Table 4 and Table 5.

10. Informal 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, and d be system parameters that denote the modulus, the bound constant for error polynomials, the bound constant for the secret polynomial, 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 is w well-rounded if w is $([q/2] - L_E)$-short and $[w]_L$ is $(2^{d-1} - L_E)$-short, where $[w]_L$ denotes the unique integer in $(-2^{d-1}, 2^{d-1}] \subset Z$ such that $w = [w]_L$ modulo 2^d. Also, $[w]_M$ is the value represented by all but the d least significant bits of $(w - [w]_L)$. Let $R = Z[x]/(x^n + 1)$ and $R_q = Z_q[x]/(x^n + 1)$. The hash oracle H(·) maps from {0, 1}* to H, where H denotes the set of polynomials $c \in R$ with coefficients in {-1, 0, 1} with exactly h nonzero entries.

Algorithm 1: Informal description of the key generation.

Require - , n/a

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)

1. a_1, …, $a_k \leftarrow R_q$ invertible ringelements.
2. Choose $s \in R$ with entries from D_σ. Repeat step if the h largest entries of s sum to L_S.
3. For $i = 1, \ldots, k$: Choose $e_i \in R$ with entries from D_σ. Repeat step at iteration i if the h
4. largest entries of e_i sum to L_E.
5. For i = 1, …, k: Compute t_i $a_i s + e_i \in R_q$.
6. 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)

1. Choose y uniformly at random among B-short polynomials in R_q.
2. $c \leftarrow H([a_1 y]_M, ..., [a_k y]_M, m)$.
3. Compute $z \leftarrow y + sc$.
4. If z is not $(B - L_S)$-short then retry at step 1.
5. For $i = 1, ..., k$: If $a_i y - e_i c$ is not well-rounded then retry at step 1.
6. 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

1. If z is not (B - L_S)-short then return reject.
2. For $i = 1, \ldots, k$: Compute $w_i \leftarrow a_i z - t_i c \in R_q$.
3. If $c \neq H([w_1]_M, \ldots, [w_k]_M, m)$ then return reject.
4. Return accept [4].

Performance of post-quantum qTESLA algorithms analysis

To evaluate the performance of the provided implementations written in portable C, the author ran benchmarking suite on three machines powered by (i) an Intel® Core™ i7-6500 CPU @ 2.50 GHz x 4 (Skylake) processor (see table 4**)** (ii) an Intel® Core™ i5-6400T CPU @ 2.20GHz (VMWARE)(Haswell) processor (see table 5) (iii) an Intel® Core™ i7-2630QM CPU @ 2.00GHz × 8 (Haswell) (see table 6) all running Ubuntu 18.04.1 LTS. For compilation, GCC version 7.3.0 was used in all tests.

11. Analysis

The author argued that the uncertainties had not been appropriately addressed. For example, there is the possibility that additional quantum algorithms or techniques will be developed, which will lead to new and unanticipated attacks. Also, it is difficult to calculate the impact of those programs that are highly classified, and its performance characteristic is not public. Rapid and unpredictable advancements in quantum computing are endangering or making current encryption schemes obsolete. It has been established that the most significant threat posed by quantum computers is directed towards current RSA, ECC digital signature scheme systems on which Bitcoin, Distributed Ledger, and much of Internet-based technology uses.

It has been settled that the current RSA and ECC based public-key cryptography are broken, and the AES cryptography is adversely reduced in bit security by the quantum computing era. It is the author's view that recommendations such as doubling the AES key size need to be examined while considering the constraints of present systems. Current AES-128 is reduced to 64-bit security, and AES-256 would have 128-bit security.

An example of the impact of doubling the key size for AES-256 to AES-512 is not well documented and verified. This alternative algorithm (AES-512) would most likely use input block size and a key size of 512-bits. An increasing number of rounds and key schedule would adversely impact performance constraints, especially for constrained devices. The higher the key size, the more secure the ciphered data, but also the more rounds needed. In the hardware perspective, a bigger key size also means a larger area and power consumption due to more operations that need to be done. More focus and examination need to be done for AES in the PQC era, especially for constrained devices.

The author specifically examined the ECDSA that are in use in Bitcoin and Distributed Ledger technologies. Secondly, evaluated NIST Candidate PQC for standardisation and possible replacement in blockchain and other public key cryptography Internet-based technologies. Table 6 gives the ECDSA (P-256) parameters used as the benchmark for comparison regarding the number of quantum security bits, and the size of the public key, secret key, and signature key as an independently controlled variable. According to NIST, the use of schemes with less than 112-bit security is deprecated and will eventually be disallowed for use by U.S. government institutions to handle sensitive data. It is noted that the speed at which the encryption and decryption occurs is also an important parameter.

Table 6: ECDSA; signature and key sizes are given in bytes [4].

Software/ Scheme	Computation Assumption	Bit Security	Key Size (bytes)	Signature Size (bytes)
ECDSA (P-256)	Elliptic Curve Discrete Logarithm	128	pk: 64 sk: 96	64

Table 7: Intel® Core™ i7-6500 (Skylake) CPU @ 2.50 GHz x 4

Scheme	Keygen	Sign	Verify	Total (sign + verify) median
qTESLA-I	1321.3	402.4	82.6	485
qTESLA-III-speed	2987.6	551	168.8	719.8
qTESLA-III-size	5042.8	1035.8	170.4	1206.2
qTESLA-p-I	5370.1	1033.2	423.4	1456.6
qTESLA-p-III	25791.8	4223.2	2134	6357.2
Scheme	**Keygen**	**Sign**	**Verify**	**Total (sign + verify) average**
qTESLA-I	1501.7	557.3	87.1	644.4
qTESLA-III-speed	3349.9	747.2	172.9	920.1
qTESLA-III-size	5329.7	1448.6	171.8	1620.4
qTESLA-p-I	5545.3	1328.9	428	1756.9
qTESLA-p-III	27570.3	5254.8	2156.4	7411.2

Table 8: Intel® Core™ i5-6400T CPU @ 2.20GHz (VMWARE)

Scheme	Keygen	Sign	Verify	Total (sign + verify) median
qTESLA-I	1460	461	88.7	550.0
qTESLA-III-speed	3217	634.8	180.8	815.7
qTESLA-III-size	5367	1219.7	181.7	1401.4
qTESLA-p-I	6316	1187.2	446.5	1633.7
qTESLA-p-III	29961	4730.5	2260	6990.6
Scheme	**Keygen**	**Sign**	**Verify**	**Total (sign + verify) average**
qTESLA-I	1786	664	107	772
qTESLA-III-speed	3998	898	212	1110
qTESLA-III-size	618	1718	206	1925
qTESLA-p-I	6898	1595	520	2116
qTESLA-p-III	31280	5952	2412	8364

Table 9: Intel® Core™ i7-2630QM CPU @ 2.00GHz × 8

Scheme	Keygen	Sign	Verify	Total (sign + verify) median
qTESLA-I	1729.3	494	105.7	599.7
qTESLA-III-speed	3900.5	708.6	223.2	931.8
qTESLA-III-size	6047	1350.2	220.5	1570.7
qTESLA-p-I	6987.2	1328.2	563.8	1892
qTESLA-p-III	36254.2	5204.5	2858	8062.5
Scheme	**Keygen**	**Sign**	**Verify**	**Total (sign + verify) average**
qTESLA-I	1972	672	108	780
qTESLA-III-speed	4367.9	929	224.4	1153.4
qTESLA-III-size	6994.3	1858.8	225.2	2084
qTESLA-p-I	7343	1683	5689	2252
qTESLA-p-III	3739	6430	2882	9312

The following results cannot be compared directly with the vendor qTESLA's submitted results, but; specific observations can be made with alternative applications and platforms. It is the author's view that if the key sizes are not manageable and practical for use in conventional and constrained devices, then the time or speed becomes less critical metric compared to key size.

Table 7, Table 8, and Table 9 give the results of the independent tests on respective platforms, and performance is measured (in thousands of cycles) of the reference implementation. Results for the median and average (in the first and second table respectively) are rounded to the nearest 10^3 cycles. Signing is performed on a message of 59 bytes.

12. Recommendations

The PQC Standardisation process is complex, arduous, and requires coordinated involvement (academia, private and public sector) and requires significant IV&V before formalization. Successful PQC must be resistant to both classical and quantum attacks. Multiple tradeoffs will have to be considered, such as security, performance, key size, signature size, and side-channel resistance countermeasures. Other important considerations are the capability to migrate into new and existing applications such as TLS, IKE, code signing, PKI infrastructure.

It is necessary to begin a coordinated international campaign to mitigate the uncertainties of breakthroughs and the unknowns regarding classified programs. The aim should include information sharing between the academic, public, and private sectors toward the common goal.

It is critical to devise and initiate the incorporation of cutting edge yet practical PQC to prevent a disastrous impact on global privacy, security, and economy before the arrival of large-scale fault-tolerant quantum computing.

13. Conclusion

qTESLA's submission for NIST Security Categories I and III as tested on platforms described in this work is more than two orders of magnitude larger for the public-key for qTESLA-p-1 (128-bit security) and qTESLA-p-III (192-bit security). The qTESLA-p-1 secret key is 56 times the size of ECDSA's secret key, and qTESLA-p-III is two orders of magnitude larger.

It is essential to come to a consensus on how to assess quantum security. Currently, there is not a clear agreement on the best way to measure quantum attacks. It is, nevertheless, fundamental that work continues with alternatives that will produce smaller key sizes, comparable to the current ECDSA algorithms. The major drawback with qTESLA is the large key sizes, which make it unlikely to be accepted in its current configuration. However, there is ongoing research being done to make it potentially a more viable candidate, both by reducing the key sizes and providing more efficient implementations (see tables 7, 8, 10).

The qTESLA's "Heuristic" submission for NIST Security Categories I and III are qTESLA-I, qTESLA-III-space, and qTESLA-III-size. The vendor claims that their heuristic approach is the security level of an instantiation of a scheme by the hardness level of the instance of the underlying lattice problem. Also, the claim is that it corresponds to these parameters regardless of the tightness gap of the provided security reduction if the corresponding R-LWE instance is intractable.

These claims and the necessary proof are beyond the scope of this work and cannot be independently verified and validated and is not the author's aim. It is important to note that; the results of qTESLA's heuristic algorithm were captured and are analyzed against its provably secure submissions. The heuristic algorithms were tested on the same platforms identified in the provably secure submission. qTESLA-I's public-key size vs. qTESLA-p-1's public-key size is a reduction of 90%. The secret key size at the same bit security level is reduced by 60%, and the signature size is reduced by 52%. Observations for public keys; qTESLA-III-size vs. qTESLA-p-III is reduced by 92%; secret key size reduction is 66%; signature size reduction is 56% (see Table 10).

The difference in the heuristic key sizes are dramatically reduced and compares more favorably to ECDSA (P-256) parameters. While the heuristic values are dramatically reduced compared to the provably secure values, the key sizes are still large compared to current standard ECDSA (P-256) sizes. For

Table 10: qTESLA Public-Key, Secret key, and Signature Size

Scheme (Bytes)	Public-key	Secret key	Signature Size
qTESLA-I	1504	2112	1376
qTESLA-III-speed	3104	4160	2848
qTESLA-III-size	2976	4160	2720
qTESLA-p-I	14880	5184	2848
qTESLA-p-III	39712	12352	6176

example; the best result for the secret key size for qTESLA-III-size (4160) vs. ECDSA (P-256) secret key size (96) is a 4233% increase and would prove problematic in existing systems.

14. Future Work

The author selected qTESLA's submission, which is 1 of 5 NIST Candidate PQC digital signature schemes. Additional work needs to be done in verifying and validating and testing the vendor's results. Concrete PQC parameters for testing and validation need to be created for the promotion of a baseline. The parameters should be modified to determine the best tradeoffs while maintaining the required security. Moreover, the organization of guidelines and standards are necessary for the wider cryptography community to aid in PQC standardisation create efficient, high-quality implementations.

Continued measurements of current PQC scheme implementations should be performed, such as performance and memory usage on the ARM and CMOS platforms. Many embedded devices have ARM and CMOS architecture and have limited computational and memory resources. NIST currently plans a Post-Quantum Cryptography Round 2 call tentatively schedule in 2019 and will offer additional opportunities for IV&V and research.

References:

[1] S. . M, A. H. D, M. . M, P. . P and S. . Balaji, "Decentralized digital voting application," *International Journal of Advance Research, Ideas and Innovations in Technology,* vol. 4, no. 3, pp. 1725-1728, 2018

[2] E. . Feig, "A Framework for Blockchain-Based Applications.," , 2018. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1803.html. [Accessed 7 1 2019]

[3] D. Moody, L. Feldman and G. Witte, "Securing Tomorrow's Information Through Post-Quantum Cryptography", *Csrc.nist.gov*, 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/itl-bulletin/2018/02/securing-information-through-post-quantum-cryptography/final. [Accessed 7 1 2019].

[4] E. Alkim, N. Bindel, J. Buchmann, Ö. Dagdelen, E. Eaton, G. Gutoski, J. Krämer, and F. Pawlega, "Revisiting TESLA in the Quantum Random Oracle Model," *Post-Quantum Cryptography Lecture Notes in Computer Science*, pp. 143–162, 2017. [Accessed 7 1 2019].

[5] G. O. Karame, "On the Security and Scalability of Bitcoin's Blockchain," , 2016. [Online]. Available: https://dl.acm.org/citation.cfm?id=2976756. [Accessed 7 1 2019].

[6] "Cryptocurrency Market Capitalizations," , . [Online]. Available: https://coinmarketcap.com/currencies/bitcoin-cash/. [Accessed 8 1 2019].

[7] N. T. Courtois, G. . Song and R. . Castellucci, "Speed Optimizations in Bitcoin Key Recovery Attacks," *Tatra mountains mathematical publications,* vol. 67, no. 1, p. 103, 2016.

[8] J. Ooms, "Toolkit for Encryption, Signatures and Certificates Based onOpenSSL," , 2016. [Online]. Available: https://cran.r-project.org/web/packages/openssl/index.html. [Accessed 7 1 2019].

[9] J. A. Dev, "Bitcoin mining acceleration and performance quantification," , 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6900989. [Accessed 30 12 2018]

[10] P.-A. R. L. D. R. F. V. Fouque, "Fault Attack on Elliptic Curve with Montgomery Ladder Implementation," 2008

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

[12] 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].

[13] D. Moody, "The NIST Post-Quantum Crypto "Competition" "The Ship Has Sailed"," in *Asiacrypt 2017*, Hong Kong, 2017.

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 confidentiality, 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 that run on classical computers and are considered 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 was 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 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 that 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 standards 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 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 the 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 that 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 a 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 the 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 a 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 are 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, business 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].

THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-1-(5)2020

The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework

Robert E. Campbell, Sr.
Capitol Technology University, USA

Correspondence: rc@medcybersecurity.com
Received: 24 February 2020 **Accepted**: 02 March 2020 **Published**: 16 March 2020

Abstract

Critical infrastructure sectors are increasingly adopting enterprise distributed ledgers (DLs) to host long-term assets, systems, and information that is considered vital to an organization's ability to operate without clear or public plans and strategies to migrate safely and timely to post-quantum cryptography (PQC). A quantum computer (QC) compromised DL would allow eavesdropping, unauthorized client authentication, signed malware, cloak-in encrypted session, a man-in-the-middle attack (MITM), forged documents, and emails. These attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. In 2018, Gartner revealed that a QC is a digital disruption that organizations may not be ready and prepared for, and CIOs may not see it coming.[1] On September 18, 2019, IBM announced that the largest universal QC for commercial use would be available in October 2019.[2] On October 23, 2019, Google officially announced "Quantum Supremacy," "by performing a calculation in 200 seconds that would take a classical supercomputer approximately 10,000 years."[3] DL cyber resilience requires "reasonable" measures, policies, procedures, strategies, and risk management before large-scale deployment. Cyber resilience implementations must be a critical component during the design and building phase, or during the initialization phase. The most significant existing attack vector for enterprise DLs is the public key infrastructure (PKI), which is fundamental in securing the Internet and enterprise DLs and is a core component of authentication, data confidentiality, and data and system integrity [1] [2]. Effectively implementing and managing a quantum-resistant PKI solution requires adherence to PKI standards, industry requirements, potential government mandates, certificate management policies, training personnel, and data recovery policies that currently do not exist. This research discusses security risks in enterprise DL PKI, areas that can be compromised, and provides an idea of what should be in a PKI DL Risk Management Framework plan.

Keywords: *cyber resilience, PKI, quantum computing, distributed ledger, cyberattack, risk management framework, hyperledger fabric*

[1] Gartner Reveals Seven Digital Disruptions CIOs May Not See Coming: https://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-reveals-seven-digital-disruptions-cios-may-not-see-coming

[2] IBM's new 53-qubit quantum computer is the most powerful machine you can use: https://www.technologyreview.com/f/614346/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/

[3] Quantum Supremacy Using a Programmable Superconducting Processor: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

Despite the vast opportunities distributed ledger technologies (DLT) offer, they suffer from challenges and limitations such as security and privacy, compliance, and governance issues that have not yet been thoroughly explored and addressed. There are many threats and numerous attack vectors, such as phishing, malware, implementation, and technology. While there are some studies on the security and privacy issues of DLT, they lack a systematic examination of the security of these systems at the fundamental level of digital signatures and public key infrastructure (PKI) vulnerabilities. Vulnerabilities and weaknesses lead to the execution of various security threats to the standard functionality of the distributed ledger (DL) platforms. The rapid development and progress of quantum computing technology are not considerations that CEOs and CIOs are correctly figuring in as a risk factor. Quantum computing poses global security concerns because the technology will be able to hack into and disrupt nearly all current information technologies. In this paper, the author explores the attack surfaces in the open-source permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. The attacks considered are insider threats, certificate authority (CA) attacks, and private-key attacks from quantum computers (QCs). The author will examine single points of failure in Hyperledger Fabric's membership service provider (MSP), or PKI, which proves to be a centralizing aspect of a decentralized system and a significant weakness of the permissioned blockchain network. Also, the author presents a cyber-resilient framework as possible use in a hybrid post-quantum-resistant enterprise PKI. Cyber resiliency is a feature that must be in systems of the future, which, when implemented, will enable the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, and/or attacks. Both the global security risks and the economic benefits necessitate building in cyber resilience.

Digital Currency and Blockchains under Attack

In 2018 alone, $1 billion in cryptocurrency was hacked from exchanges,[4] approximately $2.7 million stolen per day, or $1,860 each minute. Upbit is the seventh major crypto exchange hack of 2019 so far.[5] Upbit is the largest victim of hacking to date, after losing $49 million at 9:00 UTC on November 26, 2019. The exchange stated that an "abnormal transaction" resulted in a 342,000 ether loss in a few minutes. Some of the most notable attacks occurred in June 2011, when a hacker was able to exfiltrate Mt. Gox's auditor's credentials and transferred 2,609 bitcoins (BTCs) to an address for which Mt. Gox had no keys. The second attack occurred in 2014, resulting in 750,000 BTCs ($350 million) stolen from the exchange, and Mt. Gox halted operations and filed for bankruptcy. The Bitfloor bitcoin exchange was hacked in 2012 when hackers were able to retrieve unencrypted private keys that were kept online for backups. The amount stolen was 24,000 BTCs. Poloniex was hacked in 2014 and only stated it "has lost 12.3% of its total bitcoin supply in an attack." The exchange also explained that "the hacker found a flaw in his site's code that processes withdrawals, and made multiple simultaneous withdrawals," and the system did not respond to this error. The major problem was a coding error, and "the auditing and security features were not explicitly looking for negative balances."[6] On January 4, 2015, Bitstamp announced that an anonymous hacker hacked it, and 19,000 BTCs (worth $5 million) were lost. In 2016, Bitfinex breached and claimed 120,000 BTCs (worth $72 million) hacked. The attackers exploited a vulnerability in the multi-sig wallet architecture of Bitfinex and BitGo.[7] On May 7, 2019, Binance was hacked, losing more than 7,000 BTCs ($40 million). Binance announced that they discovered a large-scale security breach on May 7, 2019. The attackers were able to obtain user Application Programming Interface (API) keys and 2FA codes. The attackers used techniques such as phishing, viruses, and other attacks, and the hackers were able to withdraw 7,000 BTCs from this one transaction.

Distributed Ledger Growth in Critical Infrastructure

Recent forecasts indicate that global blockchain technology revenues will experience rapid growth in the coming years, with the market expected to rise to over $60 billion worldwide in size by 2024. The financial sector is currently the largest investor in blockchain, with over 60% of the technology's market value concentrated in this field.[8] However, global enterprises are increasingly adopting DLT and are hosting critical assets and critical infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. As an example, the Energy Web Foundation (EWF) is a global organization that uses

[4] How Hackers Stole $1B From Cryptocurrency Exchanges In 2018:
https://www.forbes.com/sites/daveywinder/2018/12/31/how-hackers-stole-1b-from-cryptocurrency-exchanges-in-2018/#7066025e4d87

[5] Upbit Is the Seventh Major Crypto Exchange Hack of 2019:
https://www.coindesk.com/upbit-is-the-sixth-major-crypto-exchange-hack-of-2019

[6] Yet another exchange hacked: Poloniex loses around $50,000 in bitcoin:
https://arstechnica.com/information-technology/2014/03/yet-another-exchange-hacked-poloniex-loses-around-50000-in-bitcoin/

[7] The Binance Hack:
https://medium.com/coinmonks/the-attack-on-binance-eba46700eef6

[8] Blockchain Market Shares, Market Strategies, and Market Forecasts, 2018–2024:
https://www.ibm.com/downloads/cas/PPRR983X

blockchain technology in the energy sector, with offices in Switzerland, Germany, and the United States. EWF launched the Energy Web Chain in June 2019 and advertised "the world's first public, open-source, enterprise-grade blockchain tailored to the energy sector."[9] On December 12, 2019, the U.S. President's National Infrastructure Advisory Council published draft findings on the urgent cyber risks in the most critical and highly targeted private infrastructures and called for bold action.[10] The report indicated that escalating cyber risks to critical infrastructures present an existential threat to the continuity of government, economic stability, social order, and national security. Global governments and enterprises adopting DL are on the front lines of a cyberwar; they are ill-equipped to win against organized cybercriminals and nation-states intent on hacking, robbing, disrupting, or destroying critical assets.

DLT Complexity

There are more than 30 known DL attack vectors in the categories of network, wallet, mining, double spending, and smart contracts, and these attack can be phishing and social engineering, DNS hijacking, exchange hacks, 51% attacks, software flaws, and other types that can be malware and crypto-jacking, and other traditional attacks that affect systems that connect to a blockchain [3]. The zero-day vulnerabilities cannot be quantified but must be considered as potential vulnerabilities that will be discovered and exploited. DLT consist of the integration of networked cryptography, fault-tolerance, and distributed consensus. Each of these topics is complicated, intricate, and has many known vulnerabilities and weaknesses that are not well-understood by those who lack the technical background in these topics. Also, as with any complicated technology, there are always zero-day vulnerabilities yet to be discovered and made public. The combined technologies used to form DLT dramatically increase the vulnerabilities, threats, and weaknesses. This complexity, along with the intricacies of its ecosystem (wallets, exchanges, sidechains, mining pools, enterprise consortiums), requires a formal and logical framework to address issues systematically and mitigate them to make DLT resilient.

The Quantum Computer Threat

Google's "quantum supremacy" announcement means that QCs can process and solve massive computational problems that exceed the capabilities of current supercomputers and threatens DL cryptography. Complex mathematical problems are the foundation in which much of today's cryptography is based, including PKI and DL. DLT and PKI use asymmetric digital signature schemes for private and public-key generation, signing, verification of digital signatures, and QCs break and all of these functions. This public-key cryptography is in email, web browsing, encrypted storage, banking, virtual private networks, communications, critical infrastructures, and much of the Internet [2]. It would be exceptionally naive to think that covert research and development in "quantum supremacy" is not among the highest priorities of organized groups and nation-states around the planet. Further, it would follow that classified programs seek to protect actual capabilities, or there would not be a need for secrecy. Also, a QC attack could be difficult to detect because the attacker would derive the private key from the available public key, and with the private key, a hacker will have free and absolute access [4].

Impact of Compromised PKI Private Keys

PKI is the backbone of today's enterprise blockchain, DL, network, and internet security. Figure 1 is a depiction of Hyperledger Fabric's Managed Service Provider (MSP) services, which is essentially an abstraction of PKI for enterprise blockchains. Cyber resilience is methods and procedures that aid in preventing adversarial access to systems housing critical data while ensuring the integrity of data, despite the presence of the adversary on the network and being resilient to the adversary's efforts to manipulate data. DL must assume the existence of adversaries in the network and be capable of nullifying adversarial strategies by harnessing the computational capabilities of the honest nodes, and the information exchanged is resilient to manipulation and destruction [5].

Network DL private keys are the credentials and the means of authorizing transactions, which, if compromised, will make all assets controlled or secured by the keys freely available to an adversary. The private keys enable and allow the attacker(s) to capture information, passwords, compromise CAs, certificate forgeries, obtain other private keys, derive other private keys, hijack private keys, and forge validations. The attacks and risks associated with these malicious acts allow forged documents and emails, signed malware, unauthorized clients, eavesdropping, and man-in-the-middle (MITM) attacks. The impact of these activities can result in the loss of personally identifiable information (PII), protected health information (PHI), intellectual property (IP), reputation, assets, crippled operations, and human life.

Each MSP is in a folder with various subfolders containing the administrator certificate(s), root CA certificates, the node's private key, the node's X.509 certificate, and other optional inclusions. An X.509 PKI infrastructure is a security

[9] The Energy Web is unleashing blockchain's potential in the energy sector: https://www.energyweb.org/

[10] NIAC TRANSFORMING THE U.S. CYBER THREAT PARTNERSHIP DRAFT REPORT: https://www.cisa.gov/publication/niac-transforming-us-cyber-threat-partnership-draft-report

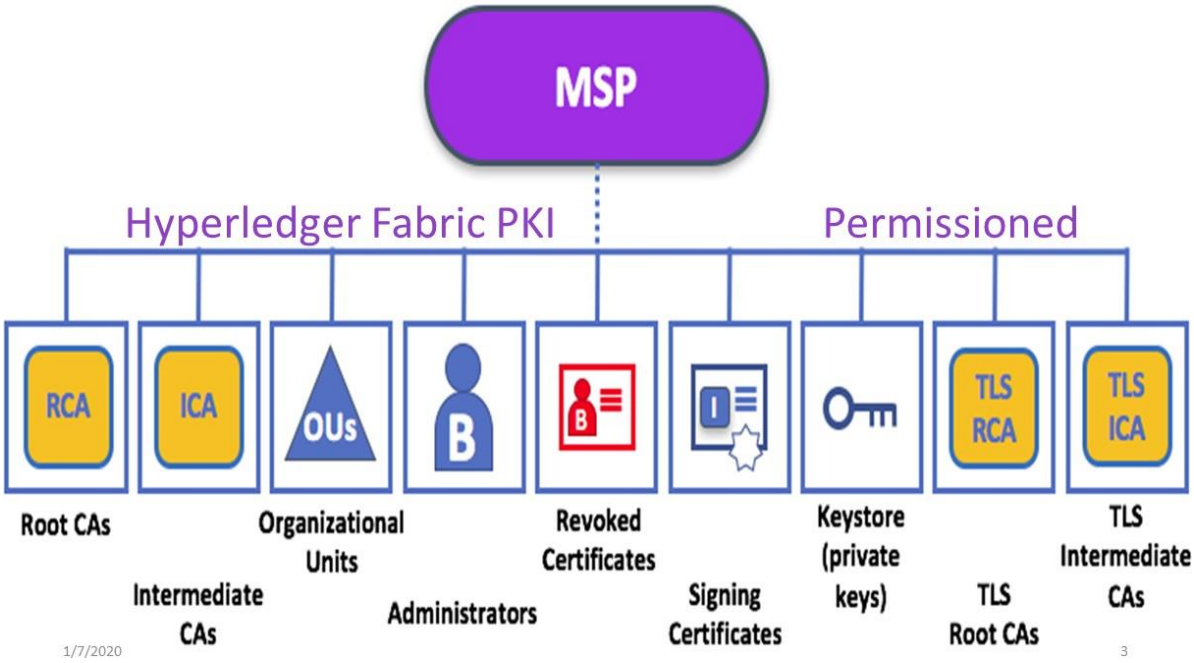

Figure 1. MSP Architecture. Source: Hyperledger Fabric.

architecture or format used in intranets, networks, and the Internet. Its cryptographic mechanisms support functions such as email, server authentication, signature generation, and validation. Specifications such as the secure multipurpose internet mail extensions (S/MIME) and transport layer security (TLS) also rely on this standard. The MSP is used to link identities, public-keys, and CAs; it acts as the primary trusted authority and uses digital signature algorithms to sign certificates of trust. Key security considerations include the ability of untrusted or unauthorized persons to participate in the network and the strength of the bit security of the encryption protocols [2].

Administrative duties include providing access and permissions for the entire blockchain network and are thus a single point of centralization. Each participant on the network is assigned a digital certificate that assures they are whom they say they are and defines the levels of access and permissions. These administrators set the permissions along with a digital certificate; each participant is assigned what Fabric labels a digital signature or the private key half of a public-/private-key pair. These keys sign off on transactions and endorsements to ensure and retain the integrity of the blockchain [6].

In the case of an insider threat such as a rogue administrator, the holder of the administrator certificate(s) is not to be trusted and has free rein over the blockchain. Administrative controls such as adding or revoking access, adding identities to the Certificate Revocation List (CRL), MSP validation of CAs, and manipulating the access a given identity has to the blockchain network are all managed solely by the administrator. Digital certificates and identities are crucial to the operation of the MSP. Cryptogen, a utility for generating Hyperledger Fabric key material, provides a means of preconfiguring a network for testing and produces all private keys in one centralized location, and it is then up to the user to adequately and safely copy them to appropriate hosts and containers. Allowing new users to decide key management best practices and the lack of standard procedures can easily lead to private-key leakage attacks. Private-key leakage is possible because each participant can choose to store and protect their private key in any way the member determines; there need to be key management best practices for all members [6].

An outside attacker obtaining private key(s) could lead to any number of attacks. As private-key leakage attacks provide potential unlimited access to the blockchain and open the possibility for any number of secondary attacks, they are one of the greatest threats to the MSP. The leakage of private keys or a successful quantum computing attack could further lead to more severe attacks, such as MITM attacks, replay attacks, message tampering attacks, and identity leakage attacks [6]. Figure 2 illustrates the weaknesses, threats, and risks of a compromised MSP or PKI in enterprise blockchains. A further shortcoming of CAs in Hyperledger Fabric is in the way it is implemented in the MSP. The MSP requires at least one root CA and can support as many root and intermediate CAs as desired. If the root CA certificate or implementation were attacked, all certificates leading back to the root certificate are compromised. Successful attacks on the MSP, which controls the membership of the blockchain runs on, would be detrimental to the security of the entire enterprise, resulting in falsified identities and more.

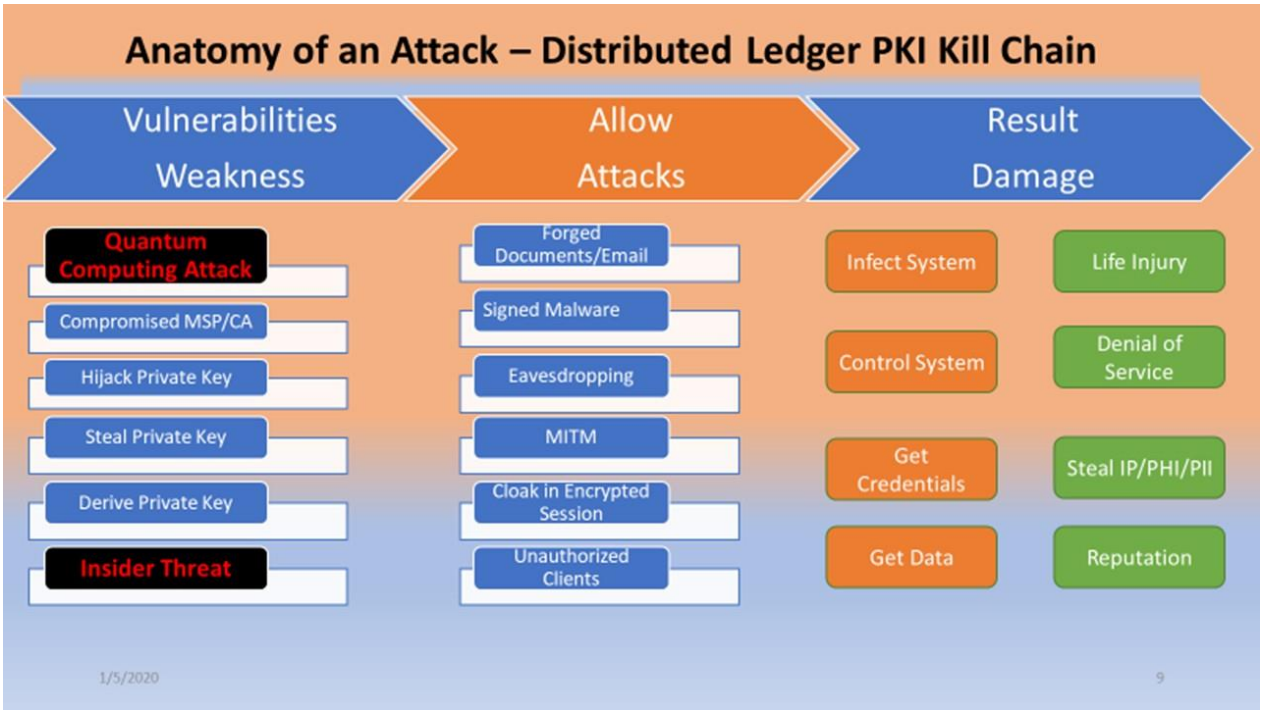

Figure 2. Distributed Ledger Kill Chain.

Anatomy of a Critical Infrastructure Attack Scenario Using Hyperledger Fabric

The following is a hypothetical critical infrastructure attack scenario on an energy plant X using enterprise blockchains such as Hyperledger Fabric and the newly discovered Russian-linked malware, which infects safety instrumented systems (SIS), called Triton. The SIS is automated safety defense systems for industrial facilities, responsible for stopping plant operations in the event of an emergency and are designed to prevent equipment failure and catastrophic incidents such as explosions or fire. FireEye has linked Triton to the Russian state-sponsored hackers.[11]

Quantum Computing Attack Scenario

The hackers are equipped with QCs capable of cracking today's standard PKI cryptography started by researching and gathering information about energy plant X. They looked for network ranges, IP addresses, and domain names. Furthermore, the hackers also searched for email addresses of key players in the organization, such as CFOs, IT professionals, and CTOs. After getting access to the network, the hackers proceeded to infiltrate the organization's network. Once the private keys were derived or obtained, the hackers accessed the entire network and went through the system silently. The attackers, armed with private keys, quickly gained remote access to an SIS engineering workstation and deployed the Triton attack framework. Immediately they started to reprogram the SIS controllers as the infection entered the SIS workstation and system via remote access. Also, the malware compromised the target system's logic controllers, exploiting "zero-day" vulnerabilities and software weaknesses that have not been identified by security experts.

The attackers reprogrammed the SIS to allow an unsafe condition while using the distributed control system (DCS), which allows attackers the ability to monitor and control an industrial process remotely and to cause fires and explosions. The result is that the attackers manipulated the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately and giving false feedback to panel safety controls until it is too late to react. The attackers were able to exploit the weaknesses, vulnerabilities, and risks contained in the current enterprise architecture PKI technology and caused explosions and fires that destroyed the plant and caused the release of lethal gas and radioactive clouds, causing massive injuries and loss of human life.

During the incident, none of the SIS controllers entered a visible failed safe state, which provided false safety readings and allowed the industrial process to continue under unsafe and dangerous conditions. The false readings prevented any investigation that would have alerted authorities and initiated an investigation. The attackers employed multiple techniques to conceal their activities and to deter digital forensic investigation of their tools and activities. They renamed the most typical and useful files to make them look legitimate like

[11] TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers: https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

Microsoft update files or a legitimate Schneider Electric application; they also used hacker tools to mimic legitimate administrator activities.[12] The attackers were able to derive the private keys of critical personnel, including safety monitors, and took total control of energy plant X. They gained complete control of SIS and caused dangerous processes to go unnoticed by sending false data to the safety control panels. The panels showed normal readings when the actual condition was increasingly hazardous. This control of the SIS and the extreme safety condition continued until it was too late, and it caused many explosions and the destruction of the plant and release of lethal and toxic clouds.

Urgent Need for Risk Management Framework for Distributed Ledger Systems

There is a pressing need to strengthen further the DL information systems, component products, and adopted services in critical infrastructures and enterprise sectors. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise. Cyber resiliency can be for system elements, systems, missions or business functions, and the system-of-systems which support those functions, organizations, sectors, or transnational missions/business functions. Nation-states and other well-resourced adversaries have intensified their efforts to infiltrate and gain control of enterprise networks and critical infrastructures, such as financial services and energy, and if successful, these could impact the continuity of government, public safety, economic stability, and national security. Global enterprises are on the front lines of a cyberwar; they are ill-equipped to fully understand, thwart, or counter against nation-states' intent upon disrupting and destroying critical infrastructure. Cyber resilient DL systems require developing an integrated approach to building trustworthy systems. The author has modified SP 800-37 Rev. 2 guidelines and recommended steps to help build a more defensible information technology infrastructure, including the component products, systems, and services [7]. Systems security engineers must apply the necessary security measures that assure the system can withstand cyber faults, failures, and attacks.

Mitigating Cyberattacks on Permissioned DLTs

While no known technology, method, or procedure can categorically prevent cyberattacks, some steps and procedures can be put in place to mitigate attacks. The architecture, deployment, and operation impact the network's cybersecurity risks and determine the controls that are best able to reduce those risks. Mitigating considerations include the number and types of participants in the system; unauthorized persons to access the network; the design and sturdiness of the consensus validation rules and processes; the strength of the encryption protocols, and the sensitivity of the data or transactions recorded in the ledger; and the ability to correct fraudulent, malicious, or erroneous files or data. At a high level, Figure 3 represents cybersecurity principles and controls of best practices that can be implemented on compromised CA, MSP, public keys, or private keys. These principles and controls include access controls, threat modeling, systems, and procedures to detect actual and attempted attacks or intrusions and risk management practices. The most important contribution this modified framework offers is the ability to adapt, survive, and continue operations with minimum disruption and loss. This framework can be used in building, deploying, and operating DL systems and outlines logical step-by-step procedures needed for cyber resiliency.

Resources Needed for Incident Response

Cyber resilient DL systems must have a business continuity planning (BCP) that delineates the organization's use of strategies, procedures, technical measures, and plans necessary for the recovery of lost data, operations, and systems in the event of a business disruption. The BCP includes a management plan, a data backup plan, a disaster recovery plan, and an emergency mode operation plan. The plans must consist of roles, responsibilities, and communication strategies in the event of a compromise or disaster, including notification of relevant external partners. A data backup plan is required to establish necessary procedures to ensure the maintenance and retrieval of exact copies of stored regulated data. The disaster recovery plan creates procedures and processes that will assist the restoration of any lost data in case of disaster, system failure, or cyberattacks. This plan is crucial, especially in the case of a cyberattack that may disrupt access to such data for an extended period. This will also require creating an inventory of all the sensitive data and systems that will be necessary for the restoration of an enterprise's activities. The emergency mode operation plan is used to ensure the continuity of an enterprise's operations while protecting critical assets and regulated data. This operation plan assists an organization in resuming its normal operations in the event of a disaster, emergency, system failure, or cyberattack. The plans should be tested and revised as necessary to ensure that the procedures put in place are effective. The main goal should be periodic testing of written contingency plans to identify weaknesses and making necessary revisions on the documentation. Figure 3 outlines the primary phase in the Distributed Ledger Risk Management Framework.

The Distributed Ledger Risk Management Framework starts with Step 1, analyzing the organizational architecture documents and reference materials external to the enterprise. This step is in the context of determining the criticality of the

[12] SAS 2019: Triton ICS Malware Hits A Second Victim: https://threatpost.com/triton-ics-malware-second-victim/143658/

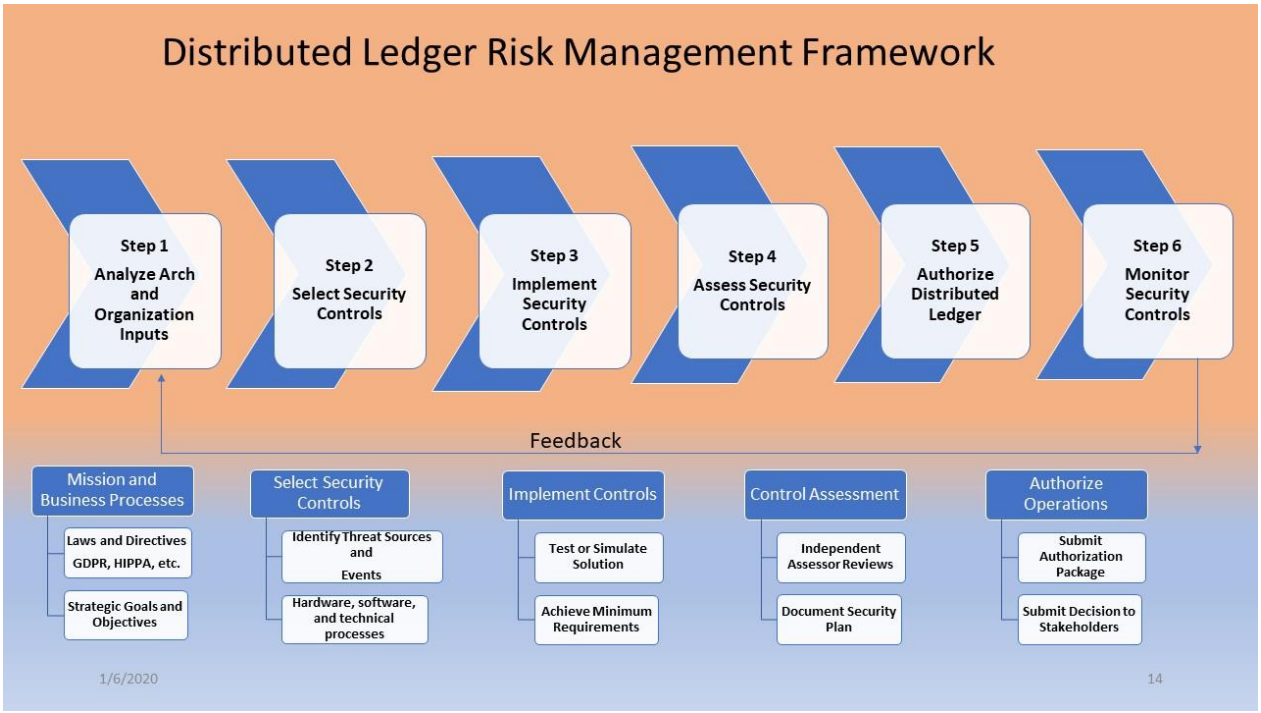

Figure 3. Distributed Ledger Risk Management Framework.

information and system according to potential worst-case, adverse impact on the organization, mission/business functions, and the system. These documents include policy and procedures, data regulating requirements, and laws for protected data such as the General Data Protection Regulation (GDPR) Health Insurance Portability and Accountability Act (HIPAA), Financial Industry Regulatory Authority (FINRA). In this phase, the business processes, objectives, and goals must align with the overall platform design and performance. Selecting security controls in Step 2 is based upon the output of step 1, which builds the baseline using categorization. Step 2 specifies a minimum baseline of security controls for countermeasures prescribed for the system designed to ensure the integrity, confidentiality, and availability of its information and to meet a set of defined requirements. Step 3 implements security controls within the enterprise architecture and systems using solid system security engineering practices. Step 4 determines security effectiveness—assessing whether the controls are implemented correctly, operating as intended, and meeting the security requirements for the system and environment of operation. Step 5 involves a documented independent assessment of security controls, and this information is promulgated to all stakeholders to ensure everyone understands the configuration changes and its potential impact on operations and business. The authorizing official (AO) examines the output of the security controls evaluation to determine whether or not the risk is acceptable. Step 6 monitors security controls for effectiveness and includes a communication or feedback loop that goes back to Step 1. Continually monitoring the controls applied for the system and its ecosystem of operation for changes, indications of attack, and so on may affect regulation and reassess control effectiveness.

Cyber Resilient Distributed Ledger Systems and NIST Post-quantum Project

Google's surprise announcement of quantum supremacy is a warning to all that quantum computing advances are not predictable. Cyber resiliency requires the ability to react quickly to cryptographic threats by implementing alternative methods of encryption. Specifically, it requires the ability to respond to incidents, has an inventory of all certification and cryptographic keys from all issuing authorities, and is capable of quickly migrating the PKI to new post-quantum resistant PKI algorithms. National Institute of Standards and Technology (NIST) is in the process of choosing one or more public-key cryptographic algorithms through a public competition-like process. The latest public-key cryptography standards will specify one or more additional digital signature and public-key encryption algorithms. These algorithms will likely be capable of protecting sensitive information well into the foreseeable future, including after the advent of QCs. NIST has down-selected a group of potential cryptographic algorithms—down to a bracket of 26. These algorithms are the ones that NIST mathematicians and computer scientists consider to be the strongest candidates. The 9 second-round candidates for digital signatures are CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, and SPHINCS+[13]. While NIST does not expect to formalize new post-quantum cryptography (PQC)

[13] PQC Standardization Process: Second Round Candidate Announcement: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

standards until the 2022–2024 time frame,[14] the enterprises cannot afford to wait. The time is now to begin independent testing and evaluation of the most promising NIST candidate algorithms toward migration and replacement. The path to a successful migration is lengthy and complicated.

Recommendations

It is of note that this research does not specify any of the NIST second-round candidate algorithms will be a straightforward "drop-in replacement"; it may need additional NIST rounds and years of follow-on research, analysis, and testing for a suitable "drop-in replacement" to be identified or developed. Therefore, the author believes that now is the time to test possible near-term "Hybrid Quantum Resistant Classical Public Key Infrastructure," a solution with the aim of seeking reductions in public-key size as one of the most significant parameters. 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 new PQC algorithms, which would only provide the public key that would be much more resistant to implementation and quantum computing attacks.

Additional research is needed on approaches to introducing new PQC algorithms (e.g., hybrids) within live systems that must remain interoperable with other systems during the period of industry migration. This includes such areas as penetration testing, formal testing, formal modeling, automated tools, and approaching transition in complex infrastructures. There is a critical need for research to understand and quantify the implications of replacing today's public cryptography algorithms.

Conclusion

Google's surprise announcement of quantum supremacy is a notice to all that quantum computing advances cannot be perfectly projected. Quantum computing attacks can lead to disruption of service, damage of reputation and trust, injury to human life, and the loss of intellectual property, assets, regulated data, and global economic security. PQC-safe algorithms generally have the higher computation, memory, storage, and communication requirements; research and prototyping are needed to understand performance, security, and implementation. In this paper, the author explored the attack surfaces in open-source permissioned blockchain project Hyperledger Fabric and its potential exploits through social engineering, malware, and cryptographic tactics. Despite the vast opportunities DLT offer, they suffer from challenges and limitations such as security and privacy, compliance, and governance issues.

The author examined single points of failure in Hyperledger Fabric's MSP, or PKI, which prove to be a centralizing aspect of a decentralized system and a significant weakness of the permissioned blockchain network. Further research is required on policy, process, and people. Global enterprises are increasingly adopting DLT and are hosting critical assets and infrastructure in a hostile, organized, sophisticated, and well-resourced cyber threat environment. As an example, EWF is a global organization that uses open-source blockchain technology in the energy sector without clear or public plans and strategies to migrate safely and timely to PQC. There is a pressing need to further strengthen the critical infrastructures and enterprise sectors and adopted DL information systems, component products, and services. It is essential that those systems, products, and services are sufficiently trustworthy throughout the system development life cycle and can provide the necessary resilience to support the economic and security interests of the enterprise.

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Robert E. Campbell, Sr. designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Robert E. Campbell, Sr. would like to thank Dr. Ian McAndrew, Dean of Doctoral Programs.

References

[1] R. Campbell, "Evaluation of Post-Quantum Distributed Ledger Cryptography," 2019. [Online]. Available: https://jbba.scholasticahq.com/article/7679-evaluation-of-post-quantum-distributed-ledger-cryptography. [Accessed 21 9 2019].

[2] R. Campbell, "Transitioning to a Hyperledger Fabric Quantum-Resistant Classical Hybrid Public Key Infrastructure," 31 July 2019. [Online]. Available: https://jbba.scholasticahq.com/article/9902-transitioning-to-a-hyperledger-fabric-quantum-resistant-classical-hybrid-public-key-infrastructure. [Accessed 21 September 2019].

[3] H. Chen, M. Pendleton, L. Njilla and S. Xu, "A Survey on Ethereum Systems Security" 13 August 2019. [Online]. Available: https://arxiv.org/pdf/1908.04507. [Accessed 7 1 2020].

[4] A. Majot and R. V. Yampolskiy, "Global catastrophic risk and security implications of quantum computers," Futures, vol. 72, no., pp. 17–26, 2015.

[14] Post-Quantum Cryptography: Workshops and Timeline: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

[5] S. Bagheri and G. Ridley, "Organisational cyber resilience: research opportunities," 2017. [Online]. Available: https://eprints.utas.edu.au/25820. [Accessed 7 9 2019].

[6] A. Davenport, X. Liang, and S. Shetty, "Attack Surface Analysis of Permissioned Blockchain Platforms," September 2018. [Online]. Available: https://par.nsf.gov/servlets/purl/10083311. [Accessed 8 1 2020].

[7] J. T. Force, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. [Accessed 8 1 2020].

[8] V. Lyubashevsky, T. Giineysu, T. Poppelmann, and D. Stehlé, "Post-Quantum Cryptography - Round 2 Submissions," 30 March 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. [Accessed 14 January 2020].