# Distributed Web Systems Leading to Hardware Oriented Cryptography and Post-Quantum Cryptologic Methodologies

*Andrew M. K. Nassief*

*The Lonero Foundation*

*andrew@etherstone.org*

December 14, 2019

**Abstract**

Distributed computational networks allow for effective hardware encryption systems and the rise of Quantum level encryption as well for Qubit based processing. Part of the reason distributed architecture can lead to Qubit level encryption is similar mechanisms applied to cryptographic hashing. In the work presented in this paper, we will look at the decentralized-internet SDK[1] and protocol, grid computing architecture, and mathematical approaches to parallel Qubit-based processing. The utilization for hardware oriented cryptography, modeled around distributed computing, will allow for an even more secure approach to Quantum authentication. The importance of works such as these, are due to the lack of security classical computing has in relation to encryption. Once mathematical formalities surpass NP-hardness, classical encryption mechanisms can be easily surpassed. However, a latent model for increased complexity in post-quantum level encryption likely forbids this trade-off. Given that Quantum Algorithms speed up superpolynomially[2], than deterministic NP-hardness would likely pose less harm to quantum encryption networks. Furthermore, with Qubit-based parallel processing, complexity models for encryption can harden in difficulty over time.

**Keywords:** Quantum Computing, Qubits, Distributed Computing, Post-Classical Computing, Cryptography, Quantum Cryptography, Parallel Processing, Grid Computing, Decentralization, Decentralized Computing Networks

# 1.0 Introduction

The decentralized-internet sdk is a software development kit that allows people to build distributed web or grid computing projects. The idea is to evidently allow for a suite of tools that one can use to offset data through parallel processing of an interconnected stream of computers. Applying the same

technique to cryptography allows one to build a decentralized node of systems. These computers can be interconnected to encrypt data through a hashing algorithm that increases in difficulty target. This can also be used as a counter-defense measure where multi-path layer security is supplied. Things such as higher and longer “pathwall layers” can be put into place where a much larger hash greets those who try breaking into the system[3]. One can also shut down a vulnerable node and automate the monitoring process.

Quantum level encryption can implement similar techniques through a Qubit-based processing mechanism. Quantum cryptography can implement Quantum Recursiveness in its hashing that would allow for recursive hashing in parallel Qubit-based processing systems that can be interconnected. Three simple equations I found are:  4n!/(2!)^n, (4^n^2)+n!, or the expanded (4n!/(2!)^n*2)^n. They are all similar, but extremely different sequences, that can be applied to Quantum Cryptography. This is because as a base 4n, applies as an original Qubit encryption layer[4]. The encryption over time becomes more and more complex.

Because of Quantum recursion, even things in classical computing such as the halting problem wouldn’t be of much effect. This is because the halting problem if solved, or one makes a metric for when computational processes should halt, the solution in itself is an assumption once you have computational unknowns such as continuous recursion or layers of uncertainty when introducing quantum computing. This has been stated well in K. Svozil’s Quantum recursion theory paper[5]. Uncertainty, even after the undecidable becomes decidable, is an important part of Quantum Computing.

## 2.0 Classical Computing and Cryptography

Classical Cryptography traditionally relies on public key and secret key style encryption. This means one has a key that can be used to decrypt the encrypted data[6]. A fundamental part of the security of these keys are the generation of the keys, as well as the cipher technique. Historically, earlier less complex style of encryption methods existed, such as Symmetric Key Encryption[7], where encryption keys and decryption keys were exactly the same. Many modern encryption styles also rely on a symmetric key pattern[8]. However a complexity to cryptography, is recursiveness. Advancements such as multiple keys for decryption, randomized block ciphers, or flash mechanism changes the key authentication style and layers.

With the rise of classical cryptography, comes authentication methods as well. Authentication comes in many different forms. There is Oauth systems in place, two-step authentication, MAC, and hardware key authentication based systems, (amongst others). The MAC algorithms or Message Authentication Code is a symmetric key cryptographic technique[9]. Due to its symmetric nature however, for message-key sender, it isn’t as reliable or as secure as some of the other options available. There are also symmetric key symmetric block cipher techniques as well such as AES[10]. Besides AES, you have hash function algorithms[11], its pre-successor the old DES, and other forms of cryptography methods.

Classical computing as opposed to Quantum Computing, is more limited in terms of the vulnerabilities one can face. This is because one may try figuring out certainty. In the event that the halting problem or even the P vs. NP (NP Hardness) has been solved, cryptography is no longer the same. Classical Computing is vulnerable even with large key sizes such as the dreaded 8096. This is because, there may still be technology out there that can break certain ciphers, it is just a case of time. Besides mathematical vulnerabilities, comes the social complexities of some of these systems as well. One can end up with centralized systems taking a work laptop home or accidentally slipping up through phishing, and carelessly wreck an entire system. This is rare to happen with a cybersecurity professional, but social engineering is still more of a vulnerability in centralized systems than a decentralized system. One can't shut an entire node down and the entire system is secure, given how a server is centralized. Even with decentralized classical computing systems where the difficulty target becomes more and more complex, given the speed of quantum computers in comparison to classical computing, it is still vulnerable security-wise.

## 2.1 Hardware-Oriented Cryptography

Hardware-oriented cryptography is the process of using hardware keys in order to authenticate into a network or decrypt some sort of data. A series of different cryptographic hashing techniques come into play when developing a hardware-oriented cryptographic system[12]. Many hardware-oriented cryptographic systems are decentralized, and rely on some sort of USB key w/ bios or headless computer in order to authenticate into a network. Flashing mechanisms sometimes play a role into the original encryption of the hardware key. Some current use-cases for such technology depends on the level of communication being transferred, but a popular example is hospital networks[13]. Many hospital networks utilize centralized systems and outdated cryptography. If one has a USB, laptop or piece of technology taken home connected to the hospital network, they are extending the reach of vulnerability. If there is a leak on their piece of technology, the entire network can suffer.

Hardware-oriented cryptography can limit this vulnerability. You can have a hardware key that flashes the computer for authentication, and act as a "node" on the network. Nodes can interconnect, and they can also set some sort of randomized hashing algorithm for ciphering. One may even be able to store a larger key size on the hardware. If one of the pathwalls or security layers of one of these keys are leaked, it may still evidently be increasing in difficulty. Someone can also shut down a single node, and rest of the system remains stable. This is also better because given the rise of technological capabilities, it should require less infrastructure to manage and one is more secure than the outdated forms of encryption.

## 2.2 Distributed Computing Systems

Distributed computational systems allow for grid or distributed processing of networks and/or data. The ability to build a distributed system to offload data have already been done. Organizations such as BOINC[14] have been using classical computing to work on this for a very long time. The decentralized-internet sdk is also a critical use-case. One can use the decentralized-internet protocol to

build a system that offloads data through a shared network of computers. The ability to extend the range of data processing, synchronization, and syndication through a wide variety of computers (as well as extend the range of wireless transmission) without any extra hardware, allow for a new form of communication[15] among computers.

A cryptographic algorithm or distributed network of monitored, decentralized nodes can be built off of the decentralized-internet sdk. The process of offloading data and extending data transmission doesn't solely have to be applied to classical computers. Quantum computers can also do parallel Qubit-based processing. A network that recursively hashes extremely large ciphers and interconnects Quantum computers even with uncertainty, can allow for a system that isn't traditionally vulnerable to the same sort of mathematical limitations that classical computers have. Since Quantum recursion theory exists, and the way Qubits traditionally process data, one can have a set of Qubit-based processors processing shared data simultaneously, becoming more and more encrypted over time.

## 2.0 Quantum Computing and Traditional Quantum Encryption

Quantum Computing relies on principles of Quantum Mechanics in order to increase processing capabilities in comparison to classical computers[16]. Traditionally computers use bits, representing data being processed through 0 and 1s. Quantum Computers are based off of the phenomena known as superposition and entanglement. Data can be simultaneously processed through multiple states such as 0 and 1 at the same time, or multiple strings of data are being simultaneously processed or observed entangled in the same state. Qubit-based processing systems are what is set in a Quantum computer in order to process data in this manner. Sometimes Qubits are manipulated through high beam lasers, and super conductivity. Due to the sensitivity of these Qubits and the way it is designed to work, Quantum processing units or QPUs are usually stored in vacuum chambers, supercooled fridges and/or cryogenic chambers.

Given the technological capabilities Quantum computers are theorized to have, post-quantum cryptography is a set of cryptographic standards for encryption and security[17] for post-classical computing. Quantum cryptography doesn't fully need to replace traditional cryptography, but enhances it. A process known Quantum coding allows for the encoding and decoding for data with Quantum computing[18]. Through Quantum cryptography, the data can be converted back through 0s and 1s, and transferred through polarized photons.

## 3.0 Traditional Qubit-based Processing

There are a series of different architectures for Quantum Computing systems. Quantum Computers rely on a collection of Qubits and process information through a QPU (Qubit Processing Units). QPUs traditionally range at 4, 8, 16, 32, 64, and 128 Qubits[19]. However, likely you need thousands of Qubits in order to process information in a way that garnishes the fuller benefits that Quantum computing has to offer. That being said, scientist are developing different ways for Quantum

information to be processed such as spin-based quantum information, loop-based[20], etc. for the different Quantum states.

## 3.1 Distributed Qubit-based Processing and Quantum Recursiveness

Processing information on a Quantum level through parallel based QPUs, similar to the loop-based architecture seems to be a viable option. Since, Quantum recursion theory exists, one can develop some sort of recursive hashing and data encoding algorithm that allows for multi-path layer cryptography on a hardware-oriented level. This means that one may able to flash QPUs and than be able to process information through a distributed mechanism through Quantum computing utilizing a distributed/grid computing architecture. This will allow for better cryptography. Since Quantum algorithms speed superpolynomially, one may not necessarily need to worry about certainty when processing Quantum information. This is true, (even given NP-hardness) because the way Qubits process information in comparison to the data processing mechanisms of classical computing. Since you have different polarization for photons, the mathematically vulnerabilities in observing data is far less then looking at bits of 0s and 1s. Even if one had a recursive algorithm based off a sequence such as  4n!/(2!)^n (amongst others), the state of security would be exponentially secure with a Qubit as the set base. A theorized algorithm and this distributed structure that would allow for Qubit-based processing, could further prove out Quantum advantage over classical computers. This is because if an architecture such as this was to be developed, than one may even have a series of QPUs interconnect in order to provide better algorithmic capabilities and act almost as a single system, but with separate nodes.

# References


[1] Kamal AM. decentralized-internet. npm. 2019 Oct [accessed 2019 Dec 15]. https://www.npmjs.com/package/decentralized-internet

[2] [accessed 2019 Dec 15]. https://quics.umd.edu/publications/super-polynomial-and-exeponential-improvements-quantum-enhanced-reinforcement-learning

[3] Kamal AM. MediSafe-Project-Demo. MediSafe Project Demo (HackingHealth Windsor). 2017 May 6 [accessed 2019 Dec 15]. https://mentors4edu.github.io/MediSafe-Project-Demo/

[4] Kamal AM. Mentors4EDU/New-Field. GitHub. 2019 Aug 11 [accessed 2019 Dec 15]. https://github.com/Mentors4EDU/New-Field

[5] Quantum recursion theory. CiteSeerX. 2009 [accessed 2019 Dec 15]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.263.9717

[6] Barber B. Traditional cryptography - Cryptography. Essay Papers. 2019 Nov 28 [accessed 2019 Dec 15]. https://benjaminbarber.org/traditional-cryptography/

[7] Traditional Ciphers. Tutorialspoint. [accessed 2019 Dec 15]. https://www.tutorialspoint.com/cryptography/traditional_ciphers.htm

[8] Modern Symmetric Key Encryption. Tutorialspoint. [accessed 2019 Dec 15]. https://www.tutorialspoint.com/cryptography/modern_symmetric_key_encryption.htm

[9] Message Authentication. Tutorialspoint. [accessed 2019 Dec 15]. https://www.tutorialspoint.com/cryptography/message_authentication.htm

[10] Advanced Encryption Standard. Tutorialspoint. [accessed 2019 Dec 15]. https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[11] Cryptography Hash functions. Tutorialspoint. [accessed 2019 Dec 15]. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

[12] Kamal AM. HIPPASafe 2.0. HIPPASafe 2.0. 2019 Aug 5 [accessed 2019 Dec 18]. http://hippasafe-20.launchrock.com/

[13] Kamal AM. P2P HIPPA-Compliant Hardware Key Cryptography Submission. HeroX. 2019 Jul [accessed 2019 Dec 18]. https://www.herox.com/DCx/round/516/entry/23251

[14] High-Throughput Computing with BOINC. BOINC. [accessed 2019 Dec 17]. https://boinc.berkeley.edu/

[15] What is Data Transmission? - Definition from Techopedia. Techopedia.com. [accessed 2019 Dec 17]. https://www.techopedia.com/definition/9756/data-transmission

[16] Giles M. Explainer: What is a quantum computer? MIT Technology Review. 2019 Jul 12 [accessed 2019 Dec 17]. https://www.technologyreview.com/s/612844/what-is-quantum-computing/

[17] Giles M. Explainer: What is post-quantum cryptography? MIT Technology Review. 2019 Jul 15 [accessed 2019 Dec 17]. https://www.technologyreview.com/s/613946/explainer-what-is-post-quantum-cryptography/

[18] Ortiz J, Sadovsky A, Russakovsky O. Modern Cryptography: Theory and Applications. [accessed 2019 Dec 18]. https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/cryptography/quantum.html

[19] r/science - Japanese scientists have invented a new loop-based quantum computing technique that renders a far larger number of calculations more efficiently than existing quantum computers, allowing a single circuit to process more than 1 million qubits theoretically, as reported in Physical Review Letters. reddit. 2017 Sep 25 [accessed 2019 Dec 18]. reddit.com/r/science/comments/72bnel/japanese_scientists_have_invented_a_new_loopbased/

[20] Takeda S, Furusawa A. Universal Quantum Computing with Measurement-Induced Continuous-Variable Gate Sequence in a Loop-Based Architecture. Physical Review Letters. 2017;119(12). doi:10.1103/physrevlett.119.120504