Quantum Cryptography: An Outlook on Improving IOT Security

Curtis Davis
Department of Computer Science and Engineering
Univeristy of South Florida
Tampa, FL
ctd@mail.usf.edu

***Abstract*— A prevalent issue is how fast the Internet of Things (IoT) is quickly encompassing various aspects of our lives. The IoT exists in numerous systems, including consumer product usage and military applications. Many of these and other IoT applications handle sensitive information and open privacy and data security issues. Some of these issues are concerned with how such a fast-growing sector of technology, IoT, is engraining itself into data sensitive areas before it has the chance to be regulated. Lack of a strong cryptography system can open a slew of problems for everyone, which is why IoT security is in dire need of a better implementation of cryptography. Quantum cryptography is a way to securely encrypt information transferred between parties, while being able to detect attackers attempting to eavesdrop on the conversation. Quantum cryptography is a promising solution to these problems and more.**

Keywords—quantum cryptography, Internet of Things (IoT), quantum cryptography for IoT, IoT security

I. INTRODUCTION

While proving to be quite practical, the constantly evolving technology of the Internet of Things (IoT) can create many security concerns if not properly managed. IoT is described as a system of interconnected computers, machines, and other objects that can collect transfer data and information over a network [2]. IoT presently finds itself connecting everyone and handling tasks that were never meant for computers to handle. While the quickly expanding IoT is found to be quite useful in optimizing these tasks, society has let looming security issues pass it by. The purpose of fixing these issues in IoT systems is because they deal with sensitive information and have the potential to be easily hacked in the future when quantum computers are slated to become more prevalent in the world. This paper summarizes current trends in quantum cryptography and how they can benefit security issues of IoT. This paper also provides an analysis of the referenced works where the impact of their proposed implementation was measured.

The material in [1] explains how IoT is in need of a security system to combat the future of quantum computing used as a hacking tool for current encryption methods. The paper also proposes a hybrid quantum cryptographic network infrastructure to improve security in IoT devices. In [2], a perspective is given on the current state and needs for quantum cryptography in IoT. It gives a general rundown on quantum cryptography and typical security scenarios for IoT. A new scheme 'InvRBLWE', an optimized variation of Ring-BinLWE, is presented in [3]. This paper explains how utilizing and improving upon how Ring-BinLWE uses ring theory can allow for more efficient implementations on hardware in cryptosystems. An explanation and related information for Ring-BinLWE and lattice based encryption is given in [5]. The team in [4] provides an experiment that exploits a vulnerability in quantum cryptography and possible solutions for the issue.

The following material of this paper is organized into 5 separate sections. Section 2 gives background information relevant to the Internet of Things and its security concerns. Section 3 contains the fundamental information of quantum cryptography. Section 4 describes approaches to solving IoT concerns. Section 5 provides an evaluation and analysis of the work done by Rahman and Hossam-E-Haider in [1] and Ebrahimi et al. in [3]. Section 6 concludes this paper by summarizing the findings of the paper and proposed future work.

II. IOT SECURITY

IoT is the result of the convergence of many different technologies, ranging from machine learning to embedded systems. The devices of IoT transmit a lot of data in many different environments, which can often include networks that handle sensitive information. Modern security measures for IoT are not as good as they need to be. Between the sensitive data it handles, lack of insight, and openness of the systems, IoT security is quite vulnerable and prone to problems as stated by Routray et al. in [2]. Current encryption methods are also vulnerable to eavesdropping during data transmissions. Ideally for IoT there would be a system which could sense attacks on the system and dispatch countermeasures to avert the attack. Routray et al. [2] and Ebrahimi et al. [3] all bring up a similar, glaring fact: IoT devices are often of low capacity and power. Current mainframe security solution operations include cumbersome computations to deal with security attacks, which also requires a large amount of memory and power [2]. This is not an ideal or realistic solution for IoT devices, which is why current research trends look for a way to optimize IoT security without relying on a large amount of resources.

III. QUANTUM CRYPTOGRAPHY

A. Preliminaries

This section describes the background information required to understand the rest of this paper. The section includes the fundamentals of entanglement-based quantum cryptography and how wave-functions can help detect intruders of a transmission for the system.

The basis of quantum cryptography lies in the properties of quantum mechanics. Entanglement is a property of at least two qubits which states though they are two separate objects and can vary greatly in distances, they are observed to be linked and exhibit the same characteristics as well as the same value [1]. These entangled objects can be linked in a way that a combined quantum state could describe them. This is a keystone in quantum cryptography, as entanglement allows the system to detect any intruding or unintended recipients of a transmission.

Initially, a wave function represents the quantum state of the quantum system. This wave function is at first in a 'superposition' of many eigenvalues. If a malicious person was to try and interact with the system, to listen into the transmission of qubits, that person interrupts the quantum state of these qubits and would reduce the many possibilities of a qubit to a single eigenvalue in an event called 'wave function collapse' [2]. In the QKD process, these interruptions would appear as the security key being different than expected. If Alice or Bob detects an interruption, the key is thrown out and the process is tried again repeatedly until a secure key is received. This is a crucial step in protecting information in IoT with quantum cryptography as it identifies when an intruder has attempted to intercept a transmission and shows that the transmission is not secure.

It is important to know that quantum cryptography does not transmit any information, it is simply a means of producing and distributing a key used for encryption [2]. Quantum cryptography starts by using a process known as Quantum Key Distribution (QKD) to produce a key which will later be used for encryption. QKD is different from classic encryption techniques as it uses properties of quantum mechanics to randomly produce such a secure key. There are two main approaches of QKD, but this will focus on one of the entanglement-based protocols, BB84. An entanglement-based protocol works by linking the quantum states of two or more separate objects in such a way that they will be described as a single combined quantum state. This process can be explained by proposing a hypothetical instance where an information sending party, Alice, is trying to send an encrypted message receiving second party, Bob. Another goal is to also prove the security of quantum cryptography in this instance by also including a malicious third-party eavesdropper, Eve, who will attempt to listen in on the two other parties exchanged information.

B. *The BB84 Protocol*

The following is of the entanglement based QKD protocol BB84. BB84 was invented by Charles Bennett and Gilles Brassard in 1984 but is still the standard for quantum cryptography protocols today. In this protocol, the polarization state of a photon represents a qubit, which can be either of the 2 bases: vertical or horizontal. Firstly, in this protocol, Alice sends Bob a series of randomly polarized photons, qubits, through a quantum communication channel, usually fiber or open space. Bob then guesses a random order of polarization bases for the incoming photons. Bob now has a randomly polarized number of photons, which results in a binary string of 1's and 0's where each 1 and 0 represents the polarization state of the photon and where half on average are correct [2]. Secondly, Alice and Bob 'sift' this raw key by exchanging information over an authenticated public classical channel, such as the internet. During this exchange of information, Alice and Bob search their key for differences. This is done through the property of entanglement which allows the system to transmit information of a quantum state and learn about the qubits by the combined quantum state. This is also the reason why it is very hard for an eavesdropper to listen in to a quantum encrypted transmission without 'collapsing the wave function' being detected. Once theses differing bits are found to be have different polarizations and values through the entanglement observation, said bits are discarded and the process leaves Alice and Bob with the correctly sifted key. During this sifting process, the eavesdropper would receive no useful information towards cracking the actual secure key. It is important to realize here that the information transferred publicly between Alice and Bob does not matter, because an eavesdropper would still not know the bases Bob had randomly generated, which are necessary to encode any messages Alice and Bob send after establishing such a secure connection. This is the process illustrated in Figure 1.

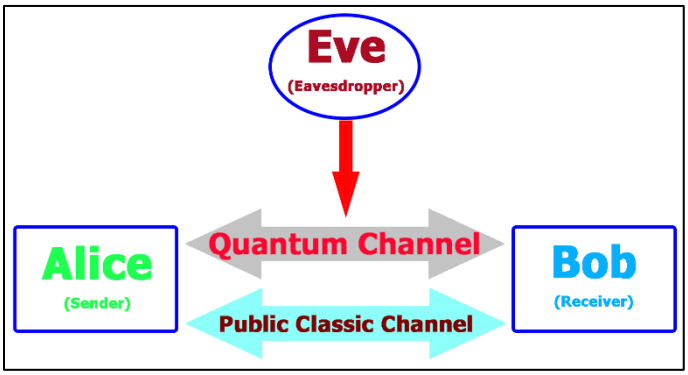

Fig. 1. The BB84 protocol [1]

IV. Approaches to the Problem

A. *A Hybrid IoT Network Infrastructure*

TABLE I. Proposed Hybrid IoT Architecture [1]

Layer	Elements
Perception Layer	Perception Network
	Perception Node
Network Layer	Local Area Network
	Access Network
	Core Network
Proposed Quantum Security Layer	Quantum Communication Channel
	Qubit Node
Application Layer	IoT Application
	IoT Application Layer

After demystifying quantum cryptography, it is clear how it offers a great solution to the prevalent concerns with IoT. IoT systems have 3 layers in them: a perception layer, a network layer, and an application layer. Rahman and Hossam-E-Haider in [1] suggest a hybrid IoT network infrastructure to ensure the security of all layers by implementing an additional 'Quantum Security layer'. This layer includes a qubit node and a quantum communication channel and houses the management of the quantum cryptography part of the system. The quantum security layer would be added between the network and application layers of the IoT system to protect the security key that is used

for transmitting information. Rahman and Hossam-E-Haider also suggest managing qubit nodes through a virtual cloud quantum computer management system. The physical side, the application layer, would use the classical encryption process of using a One Time Pad (OTP). The intention of this hybrid IoT system is to bring more security to communications of IoT users and prevent modern issues of hacking as it is nearly impossible to hack into a quantum channel as mentioned in [1]. The layout of this hybrid infrastructure is represented in Table 1.

B. The Optimized InvRBLWE Scheme

One paper, namely [3], offers a solution to cryptography in various types of IoT devices. Ebrahimi et al. are concerned with the optimization of cryptosystems and their cryptoprocessors in edge and resource-constrained devices. They propose InvRBLWE, which is an optimized variant of the proven Ring-BinLWE process, for securing information against quantum attacks and providing a resource efficient scheme for hardware implementations. InvRBLWE is mentioned to have two proposed optimized architectures: 1) a 'high-speed' architecture for the more high-performance edge devices in IoT and 2) an 'ultralightweight' power saving architecture for the nodes in IoT which have a lack of resources; this ultralightweight architecture targets devices that run on batteries or 'energy harvesting' units in IoT [3]. These architectures are also platform independent, broadening the scope of applicable devices with cryptoprocessors in IoT.

Ring-BinLWE operates as a lattice-based cryptosystem, which relies on the hardness of the Learning With Errors (LWE) problem and ring theory [3]. Ring-BinLWE utilizes the hardness of this problem and the efficiency ring theory provides to implement a strong method of key generation, encryption, and decryption. Ring-BinLWE is an improvement over the simpler Ring-LWE by using binary error distribution [5]. The scheme has smaller key sizes and does not require any complex operations [3].

InvRBLWE is an optimized scheme of binary learning with errors over the ring, transformed from Ring-BLWE by reconsidering how the ring on which operations are performed. The changes and optimizations made for InvRBLWE are intending to make a more efficient hardware implementation. One of the crucial parts of implementation of ring-related schemes is the reduction performed after each operation. In relation to ring theory, the set of coefficients of polynomials in the ring are now selected from the inverted range when compared to Ring-BLWE [3]. This change now allows the coefficients of InvRBLWE to match the range of the 2's-complement notation range of log2-bit integer [3]. This improves the past scheme because now any modular operation is performed automatically by typical underflow and overflow that is in 2's-complement notation [3]. The reduction performed over the ring are now easier to handle in hardware implementations due to these improvements. Despite the differences, InvRBLWE has the same operations and parameters as Ring-BinLWE, thus the correctness and security claims of InvRBLWE are also the same as Ring-BinLWE [3].

V. Analysis

A. The Hybrid IoT Network Implementation

Rahman and Hossam-E-Haider's proposal in [1] has beneficial intentions. Mass user information and communication would be vastly secure, and the proposers of the hybrid system also intend to inspire more applications of quantum computing in the future. However, it is also important to mention there are drawbacks. For one, while the idea is sound, this is a hypothetical situation that hasn't been tested for implementation or accuracy. Also, quantum computers are still in the lab, where commercially available ones are presently very expensive [1]. Another issue is quite major, being that if the eavesdropping party is another quantum computer, it can computer reversible computation and render the system compromised [1]. This issue may arise when quantum computers are more mainstream.

B. InvRBLWE Results

The work of Ebrahimi et al. in [3] was tested by implementing their highspeed InvRBLWE architecture on both FPGA and AISC platforms and comparing the results against other encryption schemes. The team implemented their architecture on high-performance Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC) platforms. The high-speed architecture implementation on FPGA performed better against other previous architectures in their referenced works, by improving the commonly used Area × Time complexity measurement in encrypt/decrypt operations by at least 52%. The results also show highspeed architecture performs faster than ECC on ASIC platforms while consuming less power, making it a very viable option for battery powered IoT devices. The comparison of these and other post-quantum architectures is represented in Table 2, which is an excerpt from the results in [3].

TABLE II. InvRBLWE ASIC Implementation Results [3]

Architecture	Work	Tech (*nm*)	Area (μm^2)	Power (*mW*)	Time Enc/Dec (μs)
ECC GF(2^{283})	[6]	65	49k	1.70	218 / 218
		65	72k	1.50	138 / 138
Isogeny	[7]	65	1.7m	-	- / 5140
InvRBLWE-Highspeed (n=512)	[3]	45	51k	1.5	102 / 51
		65	92k	2.5	
InvRBLWE-Ultra-lightweight (n=512)	[3]	45	7.9k	0.28	15.2k / 7.6k
		65	15k	0.7	

The ultralightweight architecture implementation of Ebrahimi et al. was tested on an ASIC platform where results showed the architecture outperformed Ecliptic Curve Cryptography by requiring less power and area, also represented in Table 2. The team also claimed this to be the first public key implementations which consumes so little power, it can run on energy supplied by electron magnetic energy harvesting units. In comparison to ECC, the ultralightweight implementation on an ASIC platform required 66% less power and 62% less area. The results of these InvRBLWE architecture implementations indicates the architecture is a promising and efficient alternative for both classical and other related proposed cryptosystem schemes [3].

VI. Conclusion

Quantum cryptography has proven to be a strong contender for solving security concerns in IoT. These papers give great insight to the current trends of quantum cryptography, especially in the field of IoT. IoT security is currently lacking while it handles very sensitive information. It is also engraining itself into society each passing day, thus it is seen how quantum cryptography currently the only comprehensible solution for such concerns against quantum computers in the future. Once quantum computers exit the lab and become a more mainstream method of computation, modern encryption methods will be immensely easy for malicious people to hack classically encrypted data transmissions. Unless quantum cryptography is realized before this happens, such attackers will easily harvest vast amounts of sensitive data.

There are avenues where quantum cryptography needs to explore and fix before it can truly be a perfect security system. There have also been instances found where the hardware of quantum computing can be compromised and invalidate the secure system it creates. In the past, quantum cryptography equipment was open to attacks by lasers and their reflections inside the system to affect the polarizers which encoded the outgoing photons; this has since been fixed by preventing such reflections [4]. There are many more instances that have yet to be thought of, which is why providing ideas of future work and improvements is so very important. The InvRBLWE architecture in [3] proves to be a robust and sturdy scheme for post-quantum cryptoprocessors in cryptosystems. However, Ebrahimi et al. also realize their architecture isn't without fault. They've tested InvRBLWE against certain attacks, but a malicious attacker can always take another path which is why extensive testing is needed on the architecture before any true implementations.

Xiao-Ling et al. [4] shows how a new way to disrupt quantum cryptography is by changing the frequency of the photon emitting laser through a process called 'injection locking'. This process can cause an output laser's frequency to resonate with some other injected photons. If this process is done correctly, frequency of the outgoing photons is exposed and thus one has a compromised system. Xiao-Ling's MDI-QKD hacking strategy through this process has been recorded to have a 60.0% success rate with an error rate as low as 6.1%. This is dangerously high for quantum cryptography, a security measure considered to be impenetrable.

Contrary to researchers finding issues with quantum cryptography, findings like these should not be treated as excessively worrisome and do not discredit quantum cryptology. Studies which find such relevant vulnerabilities makes pathways for quantum cryptography to become more robust. If it were not for these researchers discovering such issues, it is possible malicious attackers would use them against others. One can only hope that as quantum cryptography grows, so does its strength.

References

[1] M. S. Rahman and M. Hossam-E-Haider, "Quantum IoT: A Quantum Approach in IoT Security Maintenance," in 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019, pp. 269–272.

[2] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," in 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, 2017, pp. 1–4.

[3] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT," IEEE Internet Things J., vol. 6, no. 3, pp. 5500–5507, Jun. 2019.

[4] X.-L. Pang et al., "Hacking Quantum Key Distribution via Injection Locking," arXiv:1902.10423 [physics, physics:quant-ph], Feb. 2019.

[5] J. Buchmann, F. Göpfert, T. Güneysu, T. Oder, and T. Pöppelmann, "High-Performance and Lightweight Lattice-Based Public-Key Encryption," in Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security-IoTPTS 16, Xi'an, China, 2016, pp. 2-9.

[6] R. Salarifard, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "A Low-Latency and Low-Complexity Point-Multiplication in ECC," *IEEE Trans. Circuits Syst. I*, vol. 65, no. 9, pp. 2869–2877, Sep. 2018.

[7] D. Jao et al. *Supersingular Isogeny Key Encapsulation (SIKE).* Accessed: Nov. 2019. [Online]. Available: https://sike.org