CSEC-472 Authentication Paper

Quantum Cryptography and Research Trends

Mehul Sen[1], Alok Murthy[1], Chris Heine[1], Jacob Davis[1], and Alex Grant[1]

[1]Golisano College of Computing and Information Sciences, Rochester Institute of Technology

May 13, 2021

1 Abstract

Quantum Computers offer large memory, long storage times and improved capabilities. The currently used security encryptions are no longer effective when it comes to securing data. For example, a 2048-bit RSA key that would have taken billions of years to crack using a traditional computer could be broken in a matter of seconds using Quantum computers. However, researchers have already started implementing designs for the future; designs that make encryption algorithms resilient against the strongest quantum computers. This gives rise to a new field of cryptography; Quantum Cryptography.

Keywords

quantum computers, public key cryptography, Shor's algorithm, quantum cryptography, quantum cryptosystems, post-quantum algorithms, quantum effect, qubit

2 Introduction

The approaching shift towards quantum supremacy has created a need for quantum safe and quantum resistant cryptography. Research into the field takes a broad approach, looking into the numerous fields impacted by quantum computing. This approach has generated some trends as each team of researchers distills concepts down to something more actionable/effective. Our group determined that it will be critical to gather the research of more well equipped and qualified researchers by exploring research trends in quantum cryptography and trying to determine the current state and direction of the field. To this end we had three goals. First we endeavored to conduct a literary review of a number of journal articles to determine their contents and viability for the field. Next we attempted to synthesize some trends in the research we found. This involved developing an understanding of the common trends across the research we viewed. Finally we attempted to quantify these trends and document some recommendations for future research in the field. We hypothesize that necessary future research into this field will be guided by trend based analysis such as what follows.

3 Background & Significance

Quantum computers open up new possibilities when it comes to computing because of how much more powerful they are. This can create many different problems that will need to be solved. One of the key problems is making a secure cryptosystem that is able to prevent attacks done by quantum computers. Modern encryption methods that can not be broken currently can be broken "... with a complexity O(n2), i.e. in polynomial time." [1]. This means they can be broken easily. Cryptographers knew they needed to come up with a solution to this problem or else in the future quantum computers would be able to access encrypted information and data.

Our early research focused around quantum cryptography testing and implementation in real world applications. We delved into researching what cryptosystems would work against quantum computing. More specifically we read papers on simulated attacks on current cryptosystems as well as attacks on possible quantum resistant encryption methods[2]. Early simulation of quantum computers is a useful tool in creating a working encryption. Other papers also talked about modifications to current cryptosystems to make them more flexible in their uses[3, 4]. Without proper encryption methods to prevent quantum attacks, the Internet

of Things (IoT) will be vulnerable. There are an estimated 20.8 billion "things" connected to the IoT, which would all become vulnerable if quantum resistant encryption methods are not put into place to protect them [5]. Things like home security systems, connected cars, automated machines, and more could all be a security risk. Almost everyone has something connected to the IoT which means they all could be affected. The major issue is finding something that is fast and secure enough to protect against a quantum attack. We researched several different encryption schemes that will be talked about later.

Our philosophy regarding research methods was to start small and build on top of that. Getting a basic idea of quantum computing is essential in understanding quantum cryptography. Once we had an understanding of that we were able to focus our research on encryption and finally the specifics of different encryption methods. It is important that all research articles used are peer reviewed and we checked the conference metrics as well as the publishing date. The three major places we looked for our articles were the RIT Library, Google Scholar, and Microsoft Academic. Some key sources in our paper are [6] which focuses on cybersecurity regarding quantum computing and [7, 8] which are about quantum-resistant cryptosystems for IoT.

Our findings from our research discussed in our paper will be about implementing quantum resilient encryptions and how the IoT is affected by quantum computing. We will not be going into specific details about how quantum computing works. A qubit is different from a bit by the fact it can be a one or a zero or any combination of a one and zero together [9]. These play an important part in quantum computing and cryptography.

4 Related Work

Looking into journals about Quantum Cryptosystems, we found a range of varying articles that covered different aspects of quantum cryptography. Literature reviews mostly focused on explaining basic concepts of Quantum cryptography [6, 10, 11], the different perspectives of quantum cryptography, and definitions of different concepts [12, 13, 14]. Our paper heavily relied on these to integrate basic concepts of quantum cryptography with research trends and our perception of what the future will look like. Other works that gave us the idea of our paper focused on how the technologies in place will need to be modified to adapt to quantum technologies [15, 5, 16, 17] as well as the possible changes that can be made to the current quantum cryptosystems [18, 19]. Other works that influenced our paper were ones on the impact of quantum cryptography [**?**]. Quantum Cryptography's influence as well as usage in other fields. This includes Bitcoin [20], Quantum Signatures [21], Image Encryption and Decryption [22], Microgrids [23], Wireless Communications [24], IoT devices [7],and Network Deployment [25].

5 Research Questions

5.1 High level research

We began our exploration by looking into the level to which Quantum Cryptography and its theorized implementations has been tested and implemented in the real world. We sought to find out if the field has moved beyond basic proofs/theory? Specifically we looked into three theoretical pushes that we thought had potential to be simulated or tested.

1. Implementations of simulated quantum driven attacks on public key cryptosystems involving Shor's algorithm.

2. Testing of/attacks on current candidates for post quantum cryptosystems.

3. Modifications to existing cryptosystems to make them more cryptographically agile.

5.2 Impact on Specific Industries/Fields

In addition to a high level understanding of research trends in quantum security, we also wanted to know if there was additional research being done in specific fields. Our primary goals were to understand:

1. Impact on common usages of classical cryptography

2. Impact on future technologies that use cryptography

5.3 Quantum Crypto in the IoT space

To further our understanding of the space we also looked into deep diving one particularly affected industry/cryptographic application. IoT Cryptosystems were an excellent example because the IoT industry is growing massively and has little to no current protection from a quantum future. We sought to understand:

1. To what extent has it been possible to implement and test even simulated quantum safe/quantum ready cryptosystems for IoT?

2. How are Lightweight and fast encryption methods using Ring-LWE (lattices) or ECC being implemented?

6 Methods

6.1 Procedures

When conducting research for this paper, our group took the approach as stated in the Introductions section. To summarize our research for this paper we'll separate our research into three phases; Phases 1, 2, and 3. In our first phase, we learned the general aspects of quantum cryptography while trying to figure out what we wanted to focus on for our research. In our second phase, we began to have a better grasp on what we wanted to learn and focused more on specific cryptographic schemes and methods. Finally, in our third phase we focused even more while also starting to research more advanced aspects of quantum cryptography.

For our research, we used a mixture of search engines and terms to find the highest quality sources. Google Scholar was the main source used, as well as Microsoft Academics and the services offered by the RIT Libraries. In the first phase, we were searching for broad terms such as 'quantum cryptography' and 'quantum security', but as we focused in on our research, the search terms also began to be more specific. During phase 2, we searched for specific cryptography schemes, and for phase 3 we dialed in on specific hardware search terms and continued with cryptography scheme searches. The majority of the sources were published within the last 5 years to ensure the information was accurate and up to date, although there were a few exceptions.

6.1.1 Phase 1

In our first few weeks of research, we covered our first research question; "To what level has Quantum Cryptography and its theorized implementation been tested and implemented in the real world?" During this time, we were essentially surveying the land to see what the current state of quantum cryptographic research looked like and how far along it's come. Once we had a good grasp on this, we were able to decide what to focus on going forward.

6.1.2 Phase 2

From our first phase of research, we came to the conclusion that quantum cryptography would come into play much sooner than we thought [26]. Because of this, we decided to look into the cryptographic schemes that are currently being worked on. Currently, there are six main classes; isogeny-based, lattice-based, multivariate, hash-based, code-based schemes, and discrete mathematics-based schemes. When conducting our research, we tried to get a sample of each of the schemes to weigh their strengths and weaknesses. Some schemes give up speed in order to be more light-weight, while others compromise on speed to have increased security [19]. In the table below, you can see how many papers we gathered that cover various schemes. These papers were all written in the past 5 years and were published in reputable journals as rated by the Core Conference Journal and Scimago Journal Rankings.

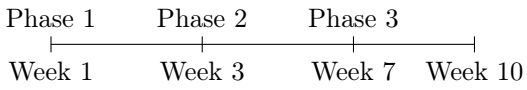
Frequency of Various Cryptographic Schemes	
Scheme	Number of Articles
Isogeny-based	6
Lattice-based	8
Hash-based	5
Code-based	3
Multivariate	4
Discrete-based	6
Shor's	5

This phase of our research is where we spent the majority of our time as it's important to understand the various schemes and what they're capable of. We also delved into our second research question on the various applications of quantum cryptography. We investigated the application on cryptocurrencies [20], the IoT [8], 5G networks [27], and more. We picked this variety as they had both the highest quality papers as well as the fact that the technologies are increasingly relevant in today's society. Cryptocurrency is an evolving technology similar to quantum cryptography, 5G networks are modern technology that will continue to develop in the coming years, and the IoT will need to be secured to protect against quantum attacks.

6.1.3 Phase 3

In the final phase of our research, we continue to look into the various cryptographic schemes while also going more in-depth on the mechanics behind both the schemes and quantum computing itself. We gathered several articles explaining the logic behind qubits [28], as well as articles covering the hardware rather than the software [29].

6.2 Timeline



This timeline shows what weeks we were gathering sources for our various phases (described in Procedures) in.

7 Findings

From the provided sources and related works, we were able to find information answering most of our proposed questions. We found the high-level explanation of the quantum cryptographic implementations as of 2021, the different fields in which quantum cryptosystems will play an essential part along with their implementations. The current state of IoT as well as ways in which we can use this information to prepare ourselves for a future with quantum computation. Quantum Cryptography is rapidly evolving, discoveries and better implementations are being discovered as we speak. Quantum Technology will certainly have massive implications for the current cryptographic landscape. Our current classical cryptographic algorithms stand no chance against quantum attacks and Shor's algorithm. Due to this, researchers have been looking into methods to counteract quantum attacks using quantum cryptography. Potential candidates like Quantum Key Distribution show promising results and might shape how we perceive quantum cryptosystems going forward. Although quantum computation ability is not readily available as of yet, we can analyze the potential candidates and their impacts on the current cryptographic playing field. We can make educated assumptions about how quantum technologies will influence the future based on current theoretical analysis. Future researchers that have access to quantum technology can use these studies and build upon theoretical analysis by building working practical models to test them out. Subsequent research into quantum cryptography could build further on the following three aspects:

7.1 Post-Quantum Cryptographic Algorithm Candidates

Some of the cryptosystems that have shown promising outcomes are the QC-LDPC and QC-MDPC Code-Based McEliece cryptosystem which can outperform Goppa code-based cryptosystem [1]. Another post-quantum candidate which is most likely to succeed is the lattice-based cryptography schemes, specifically the Ring–LWE schemes [30]. However, the most prominent post-quantum cryptography candidate is Quantum Key Distribution. Quantum Key Distribution, known as QKD [10], is based on the principles of quantum information theory and allows the establishment of information-secure cryptographic keys that belong to the group of theoretically breakable computational security solutions [31]. However, A wide range of research, ranging from fundamental to applied, still needs to be done to take QKD from its current state to one where it is a widely deployed global solution that can be reliably certified and be a part of major standards.

7.2 Impact on Classical Cryptography

Quantum Computing (QC) algorithms like the Shor's algorithm places our modern-day public-key infrastructure (PKI) in jeopardy since PKI is based on the difficulty of factoring large prime numbers using RSA. Therefore, a 2,048-bit RSA key that was thought to take billions of years to break on a classical computer could be solved in a matter of seconds using a mature QC architecture [6]. Due to this researchers in the cryptographic world are increasingly focusing their attention on producing Post-Quantum cryptographic schemes [11]. Researchers have also considered the possibility that in the event of powerful QC architectures breaking all the existing cryptographic protocols, we can upgrade these existing cryptosystems such that they keep provable security guarantees in a universally composable way [15].

7.3 Future with Quantum Technologies

Harnessing the power of quantum mechanics and being able to use quantum computers will allow us to solve various different problems, taking humanity forward, however before we are able to develop useful quantum computers, researchers need to develop and deploy quantum-safe cryptographic tools such that it does not break our cybersecurity infrastructure [10]. In the future, researchers will be more informed on quantum cryptography and influence potential cryptography scholars to explore further mechanisms of quantum cryptography, quantum computation, and other principles of quantum theory.

8 Conclusion

Quantum Cryptography is an upcoming technology that can completely alter the current cryp-

tographic landscape. Our study focuses on three main aspects of quantum cryptography, the explanation of quantum cryptography itself, its impact on different fields, and further applications of this technology. We tied together different articles of varying complexity to conduct a literature review and were able to bring together common trends within quantum cryptosystems that we found as well as document recommendations to further improve the currently developing technologies. Quantum Cryptography is in its infancy and will play a massive role in cybersecurity going forward, the steps taken now in designing future cryptosystems will have a massive impact on how this technology ends up becoming decades from today.

9 Acknowledgement

We'd first like to thank RIT and the RIT Library for providing several resources and articles for us to use for our research paper. Without this, we wouldn't have such high-quality sources. We'd also like to thank Justin Pelletier for recommending us this topic, giving us valuable feedback and critique throughout the semester, and for his lectures on quantum cryptography. Just as we were starting to stall, his lecture gave us the information and push we needed to finish strong.

References

[1] M. Baldi, P. Santini, and G. Cancellieri. Post-quantum cryptography based on codes: State of the art and open challenges. *2017 AEIT International Annual Conference*, pages 1–6, 2017.

[2] Ashley Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(1), Jan 2016.

[3] Cong Peng, Jianhua Chen, Sherali Zeadally, and Debiao He. Isogeny-based cryptography: A promising post-quantum technique. *IT Professional*, 21(6):27–32, 2019.

[4] Changbin Lu, Fuyou Miao, Junpeng Hou, Zhaofeng Su, and Yan Xiong. Quantum multiparty cryptosystems based on a homomorphic random basis encryption. *Quantum Information Processing*, 19(9), Aug 2020.

[5] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi. Securing the internet of things in a quantum world. *IEEE Communications Magazine*, 55(2):116–120, 2017.

[6] L. Mailloux, Charlton D. Lewis, Casey Riggs, and M. Grimaila. Post-quantum cryptography: What advancements in quantum computing mean for it professionals. *IT Professional*, 18:42–47, 2016.

[7] T. Fernández-Caramés. From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things. *IEEE Internet of Things Journal*, 7:6457–6480, 2020.

[8] Yu-Long Gao, Xiu-Bo Chen, Yu-Ling Chen, Ying Sun, Xin-Xin Niu, and Yi-Xian Yang. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, 6:27205–27213, 2018.

[9] Ashish Nanda, Deepak Puthal, Saraju P Mohanty, and Uma Choppali. A computing perspective of quantum cryptography. *IEEE Consumer Electronics Magazine*, page 57–59.

[10] M. Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security Privacy*, 16:38–41, 2018.

[11] An overview of quantum cryptography and shor's algorithm. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5):7487–7495, 2020.

[12] Alejandro Aguado, Victor Lopez, Diego Lopez, Momtchil Peev, Andreas Poppe, Antonio Pastor, Jesus Folgueira, and Vicente Martin. The engineering of software-defined quantum key distribution networks. *IEEE Communications Magazine*, 57(7):20–26, Jul 2019.

[13] C. Pradeep, M. Rao, and B. Vikas. Quantum cryptography protocols for ioe security: A perspective. 2019.

[14] V. Padamvathi, B. Vishnu Vardhan, and A.v.n. Krishna. Quantum cryptography and quantum key distribution protocols: A survey. *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, Aug 2016.

[15] I. Vajda. On classical cryptographic protocols in post-quantum world. *International Journal of Computer Network and Information Security*, 9:1–8, 2017.

[16] T. Zhou, Jian Shen, X. Li, Chen Wang, and Jun Shen. Quantum cryptography for the future internet and the security analysis. *Secur. Commun. Networks*, 2018:8214619:1–8214619:7, 2018.

[17] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations. *ACM Computing Surveys*, 51(6):1–41, 2019.

[18] Oscar M. Guillen, Thomas Poppelmann, Jose M. Bermudo Mera, Elena Fuentes Bongenaar, Georg Sigl, and Johanna Sepulveda. Towards post-quantum security for iot endpoints with ntru. *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*, Mar 2017.

[19] Fabio Borges, Paulo Ricardo Reis, and Diogo Pereira. A comparison of security and its performance for key agreements in post-quantum cryptography. *IEEE Access*, 8, Jul 2020.

[20] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt. Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack. *Royal Society Open Science*, 5(6):180410, May 2018.

[21] Panos Kampanakis and Dimitrios Sikeridis. Two post-quantum signature use-cases: Non-issues, challenges and potential solutions∗. 2019.

[22] Harshad R. Pawar and Dinesh G. Harkut. Classical and quantum cryptography for image encryption decryption. *2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)*, Oct 2018.

[23] Zefan Tang, Peng Zhang, and Walter O. Krawec. A quantum leap in microgrids security: The prospects of quantum-secure microgrids. *IEEE Electrification Magazine*, 9(1):66–73, Mar 2021.

[24] Panagiotis Botsinis, Soon Xin Ng, and Lajos Hanzo. Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design. *IEEE Access*, 1:94–122, Nov 2018.

[25] M. Li and T. Wang. Optimized coherent state based quantum cryptography with high robust for networks deployment. *IEEE Access*, 7:109628–109634, 2019.

[26] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, and et al. Status report on the first round of the nist post-quantum cryptography standardization process. 2019.

[27] T. Charles Clancy, Robert W. Mcgwier, and Lidong Chen. Post-quantum cryptography and 5g security. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[28] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. Brandão, David A. Buell, Brian J. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, Keith Guerin, Steve Habegger, M. Harrigan, M. Hartmann, Alan Ho, M. Hoffmann, T. Huang, T. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, Mike Lindmark, E. Lucero, D. Lyakh, Salvatore Mandrà, J. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Niu, E. Ostby, A. Petukhov, John C. Platt, C. Quintana, E. Rieffel, P. Roushan, N. Rubin, D. Sank, K. Satzinger, V. Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. Yao, P. Yeh, Adam Zalcman, H. Neven, and J. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505–510, 2019.

[29] Paulo Vinicius Pereira Pinheiro, Poompong Chaiwongkhot, Shihan Sajeed, Rolf T. Horn, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. Eavesdropping and countermeasures for backflash side channel in quantum cryptography. *Optics Express*, 26(16):21020, 2018.

[30] W. Buchanan and Alan Woodward. Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*, 1:1 – 22, 2017.

[31] Miralem Mehic, Marcin Niemiec, Stefan Rass, Jiajun Ma, Momtchil Peev, Alejandro Aguado, Vicente Martin, Stefan Schauer, Andreas Poppe, Christoph Pacher, and Miroslav Voznak. Quantum key distribution: A networking perspective. *ACM Comput. Surv.*, 53(5), September 2020.