IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 13, Issue 6 Ver. III (Nov. - Dec. 2017), PP 18-21
www.iosrjournals.org

An Overview of Quantum Cryptography with Lattice Based Cryptography

Chuck Easttom[1]
[1](CEC-Security, United States)
Corresponding Author: Chuck Easttom1

Abstract: *Many researchers believe quantum computing will be a practical reality within the next 10 years. Quantum based algorithms will be able to render current number theoretic asymmetric cryptography algorithms obsolete. This means that other algorithms must be discovered, prior to quantum computers becoming a practical reality. Lattice based cryptosystems are a viable candidate for post-quantum computing.*

Keywords: *quantum computing, cryptography, quantum physics, post-quantum cryptography, lattice based cryptography*

Date of Submission: 21-11-2017 Date of acceptance: 30-11-2017

I. Introduction

Innovations in quantum computing promise to significantly increase computing power. This will provide advances in numerous aspects of computing including data mining, artificial intelligence, and other applications [1]. However, the increase in computing power will also present a challenge for cryptography. Most experts agree that when quantum computing becomes a practical reality, that current cryptographic systems will be obsolete. Finding a cryptographic systems that would be resistant to quantum computing is an important research topic [2]. Quantum computing was first proposed by Paul Benioff at Argonne National Labs [3]. Work by Yuri Manin in 1980 and Richard Feyman in 1982, has also been useful in developing the concept of quantum computing. Research has progressed since that time, and there are limited quantum computers in research labs. Classical computing relies on individual bits to store information. Quantum computing relies on qubits.

The essential issue with quantum computing is the ability to represent more than two states. Current computing technology, using classical bits, can only represent binary values. Qubits, or quantum bits, store data via the polarization of a single photon[4]. The two basic states are horizontal or vertical polarization. However, quantum mechanics allows for a superposition of the two states at the same time. This is something simply not possible in a classical bit. The two states of a qubit are represented with quantum notation as |0> or |1>. These represent horizontal or vertical polarization. A qubit is the superposition of these two basis states. This superposition is represented as $|\psi> = \alpha|0> + \beta|1>$ [5][6]. Essentially a classical bit can represent a one or a zero. A qubit can represent a one, a zero, or any quantum superposition of those two qubit states. This superposition allows for much more powerful computing. The superposition allows the qubit to store a one, a zero, both a one and a zero, or an range of values between one and zero [7]. This significantly increases data storage and data processing power. This increase in computing power has important ramifications for cryptography (Broadbent & Schaffner). There are already quantum based algorithms that are far superior at factoring large numbers than are classical algorithms [8][9]. That is a critical issue because the widely used RSA algorithm is based on the difficulty of factoring a large number into its prime factors [10][11]. When quantum computers become a reality, that factoring problem will no longer be difficult, and RSA will be obsolete [12]. Various key exchange algorithms such as Diffie-Hellman depend on the difficulty in solving the discrete logarithm problem (Easttom, 2017). The two most significant improvements to Diffie-Hellman, ElGamal and MQV (Menezes–Qu–Vanstone), also depend on the discrete logarithm problem [13]. Elliptic curve cryptography, is based on the difficulty of solving the discrete logarithm problem with respect to an elliptic curve [14]. Quantum algorithms will also make the discrete logarithm problem quite solvable, thus rendering these algorithms obsolete as well.

II. Discussion

Essentially all current asymmetric cryptography is based on one of these two general classes of number theoretic problems: factoring or solving the discrete logarithm problem [15]. Essentially, when quantum computers become a practical reality, rather than just a research interest, all modern asymmetric algorithms will become obsolete [16]. This is a significant concern for cybersecurity because all modern e-commerce, encrypted

email, and secure communications over a network, depend on these algorithms. Currently, the NIST is working on a multi-year study to determine standards for post-quantum cryptography [17].

Current quantum computing is not at a stage to be useful in practical applications. Cutting edge quantum systems of today only have 20 to 50 qubits and can only maintain data for a very short time [18]. However, advances in quantum computing indicate that practical quantum computers could be a reality within 10 years [19]. Whether this estimate is accurate or not, it is clear that quantum computing will eventually be a practical reality, and thus existing asymmetric cryptographic algorithms will become obsolete. Fortunately, researchers are already exploring algorithms that would be resistant to quantum computing [20]. There are primarily two areas of research: multi-variate cryptography and lattice based cryptography. The focus of this current paper, is on the application of lattice based cryptography. Lattice based mathematics promises to provide a range of cryptographic solutions [21]. Lattice based cryptography involves the construction of cryptographic primitives based on lattices. A cryptographic primitive is an algorithm such as a symmetric cipher, asymmetric cipher, cryptographic hash, or message authentication code that is part of a cryptographic application. Essentially, a complete cryptographic system has to account for both confidentiality and integrity of the message. This often involves encrypting the message for confidentiality, exchanging symmetric cryptographic keys via some asymmetric algorithm, ensuring integrity with a cryptographic hash function, and digitally signing the message. Each of these aspects of security is accomplished via a different algorithm, a specific cryptographic primitive. The cryptographic primitives are combined to provide a complete cryptographic system.

A lattice is a construct from algebraic group theory. A lattice is represented by a standard matrix, familiar to anyone who has taken an introductory course in linear algebra. The vectors that constitute the lattice are known as the basis vectors for the lattice [22]. A matrix is shown in the figure below.

$$A = \begin{bmatrix} 2 & 0 \\ -1 & 4 \end{bmatrix},$$

Figure 1. A basic matrix

The matrices used in lattice based cryptography can be of any number of dimensions, though for ease of presentation, most books demonstrate two dimensional matrices. Each column represents a vector. The matrices used in lattice based cryptography are much larger than the one shown in figure 1, or else solving mathematical problems based on a lattice would be a trivial task to solve; and encryption based on lattices would be easily broken. Lattice based cryptography is simply cryptographic systems based on some problem in lattice based mathematics [23]. One of the most commonly used problems for lattice based cryptography is the Shortest Vector Problem (SVP). Essentially this problem is that given a particular lattice, how do you find the shortest vector within the lattice? More specifically, the SVP problem involves finding the shortest non-zero vector in the vector space V, as measured by a norm, N. A norm is a function that assigns a strictly positive length or size to each vector in a vector space. The SVP problem is a good choice for post-quantum computing. Micciancio and Regeve (2009) state: "There are currently no known quantum algorithms for solving lattice problems that perform significantly better than the best known classical (i.e. non-quantum) algorithms."

There are a variety of mathematical problems based on lattices that can form the basis for cryptographic systems, SVP is only one choice. Another such problem is the Learning With Errors (LWE) problem. This is a problem from the field of machine learning. It has been proven that this problem is as difficult to solve as several worst-case lattice problems [24]. Algorithms are often measured by best-case, average-case, and worst-case solutions. Put simply, this means that the LWE problem is very difficult to solve. As has already been stated in this paper, asymmetric cryptography is based on mathematical problems that are difficult to solve. In fact, the problems are so difficult to solve that no solution can be found within a practical period of time. The LWE problem has been expanded to use algebraic rings with Ring-LWE.

There are currently several fully functional lattice based cryptosystems. The GGH algorithm, named after its inventors Glodreich, Goldwasser, and Halevi [25], is one such cryptosystem. It is a robust asymmetric/public key algorithm that has been proven to be resistant to cryptanalysis. This algorithm was first published in 1997 and uses the closest vector problem (CVP). This problem is summarized as: given a vector space V, and a metric M for a lattice L and a vector v that is in the vector space V, but not necessarily in the lattice L, find the vector in the lattice L that is closest to the vector v [26]. This problem is related to the previously discussed SVP problem and is also difficult to solve. Another lattice based cryptosystem is NTRU. It was invented by Hoffstien, Pipher and Sillverman. It is the most well-known and widely studied lattice based cryptographic system. NTRU is a cryptosystem that provides both encryption and digital signatures. It has been shown to be resistant to Shor's algorithm [27], unlike many other asymmetric cryptographic systems. Shor's

algorithm is named after the inventor, Peter Shor, and it is a quantum algorithm for integer factorization [28]. It is effective at factoring large numbers, thus breaking cryptography based on factorization problems. Another important fact about NTRU, is that even without concern about quantum computers, NTRU is more efficient than RSA. That makes it a viable option for classical computing.

With each of these cryptosystems, research is showing that these are not only applicable for use in asymmetric cryptography, but also in cryptographic hashes. These systems have also been applied to digital signature solutions, as well as encryption solutions. That means that a range of cryptographic primitives can be created from lattice based mathematics, yielding a complete cryptosystem from lattices.Bernstein and Lange (2017), also demonstrate that lattice based cryptography is resistant against current cryptanalytical attacks. This means that lattice based cryptography is a preferable solution, even when considering only classical computing. There have been advances in number sieves that are improving even classical computing's ability to break RSA [29][30]. This demonstrates that there is a need for improved asymmetric cryptographic primitives, even before quantum computing becomes a reality.

III. Conclusion

While the current state of quantum computers is nascent, still only applicable for research purposes, it seems clear that quantum computers will become a practical reality. When that will occur is not clear. However, what is clear, is that when quantum computers become a practical reality, current asymmetric cryptography, based on specific number theoretic problems, will be obsolete. There is an extensive body of research that indicates that lattice based cryptography is a viable solution for post-quantum computing. Furthermore, lattice based cryptography is more resistant to cryptanalysis with classical computing. However, further research is needed. While there have been numerous, disjointed studies, there has not been a single study that performs an extensive analysis of multiple lattice based algorithms against current number theoretic based algorithms.

References

[1]. Imre, S., & Balazs, F. (2013). Quantum computing and communications: An engineering approach. Hoboken, New Jersey: John Wiley & Sons.
[2]. Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78(1), 351-382
[3]. Moret-Bonillo, V. (2017). Adventures in computer science: From classical bits to quantum bits. New York City, New York: Springer.
[4]. Neilson, M., Chuang, I. (2011).Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge, United Kingdom: Cambridge University Press.
[5]. Fano, G., Blinder, S. (2017). Twenty-First century quantum mechanics: Hilbert space to quantum computers: Mathematical methods and conceptual foundations. New York City, New York: Springer.
[6]. Rieffel, E., Polak, W. (2011). Quantum computing: A Gentle introduction. Boston, Massachusetts: MIT Press.
[7]. Stanescu, T. (2016). Introduction to quantum matter & quantum computation. Boca Raton, Florida: CRC Press.
[8]. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
[9]. Kollmitzer, C., Pivk, M. (2010). Applied quantum cryptography. New York City, New York: Springer.
[10]. Easttom, C. (2015). Modern cryptography: Applied mathematics for encryption and information security. New York City, New York: McGraw-Hill Publishing.
[11]. Stanoyavich, A. (2010). Introduction to cryptography with mathematical foundations and computer implementations. London, England: Chapman and Hall.
[12]. Trabesinger, A. (2017). Quantum computing: towards reality. Nature, 543(7646), S1-S1.
[13]. Kraft, J., Washington, L. (2013). An Introduction to Number Theory with Cryptography. London, England: Chapman and Hall.
[14]. Shermanske, T. (2017). Modern cryptography and elliptic curves: A beginner's guide. Providence, Rhode Island: American Mathematical Society.
[15]. Stallings, W. (2016). Cryptography and network security: Principles and practice. New York City, New York: Pearson Press.
[16]. Curty, M. (2014). Quantum cryptography: Know your enemy. Nature Physics, 10(7), 479-480.
[17]. Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology.
[18]. Knight, W. (2017). IBM Raises the Bar with a 50-Qubit Quantum Computer. MIT Technology Review. November 2017. Retrieved from https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer.
[19]. Kelly, D. (2015). Microsoft lab predicts we'll have a working 'hybrid' quantum computer in 10 years. Business Insider. October 2015. Retrieved from http://www.businessinsider.com/microsoft-hybrid-quantum-computer-2015-10.
[20]. Shenoy-Hejamadi, A., Pathak, A., & Radhakrishna, S. (2017). Quantum cryptography: Key distribution and beyond. Quanta, 6(1), 1-47.
[21]. Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). An Introduction to
[22]. Axler, S. (2015). Linear algebra done right. Berlin, Germany: Springer.
[23]. Pöppelmann, T., & Güneysu, T. (2013). Towards practical lattice-based public-key encryption on reconfigurable hardware. International Conference on Selected Areas in Cryptography. Berlin, Germany: Springer
[24]. Bogdanov, A., Guo, S., Masny, D., Richelson, S., & Rosen, A. (2016). On the hardness of learning with rounding over small modulus. In Theory of Cryptography Conference. Heidelberg Germany: Springer.
[25]. Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), 283-424.
[26]. Lay, D., Ray, S. (2015). Linear algebra and its applications. New York City, New York: Pearson.
[27]. Monteiro, R. T. (2016). Post-quantum cryptography: lattice-based cryptography and analysis of NTRU public-key cryptosystem (Doctoral dissertation). University of Lisbon, Portugal.

[28]. Wang, D. S., Hill, C. D., & Hollenberg, L. C. (2017). Simulations of Shor's algorithm using matrix product states. Quantum Information Processing, 16(7), 176-183.
[29]. Abubakar, A., Jabaka, S., Tijjani, B. I., Zeki, A., Chiroma, H., Usman, M. J., ... & Mahmud, M. (2014). Cryptanalytic attacks on Rivest, Shamir, and Adleman (RSA) cryptosystem: Issues and challenges. Journal of Theoretical & Applied Information Technology, 61(1).
[30]. Vuicik, E. J., Šešok, D., & Ramanauskaitė, S. (2017). Efficiency of RSA key factorization by open-source libraries and distributed system architecture. Baltic Journal of Modern Computing, 5(3), 269-274.

Chuck Easttom An Overview of Quantum Cryptography with Lattice Based Cryptography. IOSR Journal of Mathematics (IOSR-JM) , vol. 13, no. 6, 2017, pp. 18-21.