Cryptography in the Post-Quantum Era

Rvail Naveed

***Abstract*—In the past decade, there has been extensive development in the quantum computing field. Quantum computers are a fundamentally new way of performing calculations and solving problems. Due to this, modern cryptography systems are put at risk. This report aims to review the concept of ”Post-Quantum Cryptography”, and what can be done to mitigate the risk to cryptosystems presented by quantum computers.**

***Index Terms*—Quantum Computing, Cryptography, Public-Key Encryption**

I. Introduction

SINCE the creation of the internet in the 1990’s there has been an ever growing need for cryptography. It has become a major component of the security and integrity of data. Modern encryption algorithms rely on the hardness of complex mathematical problems such as *Integer Factorization* and *Discrete Logarithm Problem*. These problems serve as the basis for widely used cryptosystems such as RSA. For classical computers, these problems are very hard problems to solve and require immense amounts of computing power and time to break. This is why they are said to be secure by today’s standards. However, a phenomenon known as Quantum Computing threatens this security. The concept of quantum computing was first put forward by a physicist named Paul Benioff when he proposed a quantum mechanical model of the Turing machine. Benioff was the first to show that quantum computing was theoretically possible. Many others built upon his work and it was then that it became known that a quantum computer could have the possibility to solve problems in a fundamentally new way that would allow for extreme gains in speed and computing power, that would be unparalleled by the classical computers of today.

The rest of this paper aims to review Quantum Coputers, how they operate, what makes current encryption schemes vulnerable, how quantum computers threaten their security and post-quantum alternatives for cryptosystems.

II. Quantum Computers

Unlike classical computers that depend on values being confirmed and definite in order to perform calculations with them, quantum computers can perform calculations on variables before they have ”settled” into a state. This allows quantum computers to perform the calculations with variables who’s states are undetermined. The common example used to illustrate this effect is a spinning coin. A classical computer only knows the value of the coin when it lands, either heads or tails. A quantum computer interprets the spinning coin as being both in the state of heads and tails at the same time. This phenomenon is called superposition and is one of the main ideas that makes these new computers so powerful. Quantum computers perform operations with *qubits*. Qubits are undefined properties of a system and they have the ability to be in a state of superposition, much like the spinning coin. These qubits are then used in special quantum algorithms such as *Shor’s Algorithm* discussed below, to perform multiple probabilistic calculations simultaneously, cutting down on the time it would take a classical computer to do the same task.

Another fundamental concept that quantum computers take advantage of is *Quantum Entanglement*. This refers to when 2 or more (n ¿= 2) qubits become an n-tuple. When this happens, a change in one of the qubits in the tuple will result in a direct change in the other, in some deterministic way. Entanglement also allows for the ”daisy-chaining” of multiple entangled qubits for exponential computing gain.

Despite the promising nature of quantum computers, there are some challenges that need to be worked on in order to make it a significant threat to cryptography. Quantum computers are much more error prone than their classical counterparts due to *decoherence*. This happens because of random noise in the environment such as heat and vibrations which make the superposition of the qubits decay over time, leading to less reliable functionality. However, there is extensive research being done on this subject and it won’t be long before a fully functional quantum computer is a reality. According to the American National Institute of Standards and Technology (NIST), it is a probable scenario that a quantum computer c ould be built for a budget of one billion dollars by 2030 that could break RSA-2048, a feat that is impossible by classical computers of the current age.

III. Current Cryptography

Current cryptography techniques can be divided into 2 distinct types: *Symmetric* and *Asymmetric*. These cryptography techniques rely heavily on the hardness of solving problems such as Integer Factorization and the Discrete Logarithm problem.

A. Symmetric

In symmetric-key cryptography there is only one key that is used to encrypt and decrypt messages between parties. The plaintext x is entered into an algorithm called a ”cipher” that encrypts the plaintext using the specified key and outputs it as ”scrambled” ciphertext. This ciphertext is now encrypted and can only be converted back to its original plaintext form by using the specified key that it was encrypted with. Symmetric-key cryptography allows for a respectable amount of security and efficiency. However the benefits carry a risk as there are concerns of the keys being intercepted when they are being transmitted/distributed between parties.

B. Asymmetric

Asymmetric cryptography is commonly referred to as public-key cryptography. This is because it uses a 2-key pair to encrypt and decrypt messages. Public-key cryptography uses a *public key* that can be shared over any channel and a *private key* that is kept secret by the intended sender/recipient. The sender uses the receivers public key to encrypt a message before transmission, and the receiver uses their own private key to decrypt the message and view it in its plaintext form. Public-key algorithms have seen wide adoption and serve as a backbone to many services today such as the Secure Socket Layer and HTTPS technology. Digital signatures are also commonly verified with public-key techniques.

C. Integer Factorization Problem

RSA first proposed by Rivest, Shamir and Adleman in the 1970's, is one of the world's first public key cryptosystems. RSA is often used in combination with symmetric key algorithms for maximum security and speed. RSA encryption is designed to be easy to compute in one direction and difficult to compute in the opposite direction. Such functions are often called *trapdoor* or *one-way* functions. RSA relies on the integer factorization problem via prime numbers.
The operation of RSA is as follow:

- Two large primes are generated p, q such that they are far away from each other, otherwise it would be easier to crack.
- The product of the two primes is then found $n = p * q$ and $\phi = (p-1) * (q-1)$
- A random number $1 < e < \phi$ is selected such that the greatest common divisor (gcd) = $gcd(e, \phi) = 1$
- Compute a unique integer $1 < d < \phi$ such that $e * d = 1(mod\ \phi)$
- We then have (d, n) and (e, n) as the private and public key's respectively.
- Encrypt message *m* using $c = m^e * mod\ n$
- Decrypt: $m = c^d mod\ n$

D. Discrete Logarithm Problem

Given a finite cycle group Z^*p of order $p-1$ and a primitive element $\alpha \in Z^*p$ and another element $\beta \in Z^*p$, the DLP is determining an integer $1 \leq x \leq p-1$ such that $\alpha^x \equiv \beta modp$. x is called the discrete logarithm of β to the base α.

$$x = log_\alpha \beta modp$$

. The difficuly of solving DLP relies in finding an x that satisfies the equation. DLP can prove to be a very hard problem to solve, if the parameters are large.

E. Security

Both symmetric and public-key cryprography are considered to be very secure by today's standards. However this security is threatened as we move towards a reality where Quantum Computers are more powerful. The inherent security of symmetric cryptography is based on the length of the keys used for encryption/decryption. A 128 bit key length would take billions of years to crack on classical hardware. NIST recommends a move to 256 bit key lengths, which are thought to be theoreticallly resistant to Quantum attacks. The same cannot be said for public-key algorithms such as RSA and Elliptic Curve Crptography as quantum algorithms such as *Shor's Algorithm* and *Grover's Algorithm* aim to drastically reduce the amount of time it takes to crack them. With classical hardware, prime factorization is extremely time consuming and unimaginable, with the best time being $O(exp(\sqrt[n]{\frac{64}{9}n(logn)^2}))$. However, with Shor's algorithm this time is significantly reduced to $O(n^3 logn)$, where n the bits of the product $p * q$.

IV. Shor's Algorithm - This defo needs to be better

In 1994, Peter Shor developed a quantum polynomial-time quantum algorithm for integer factorization. This algorithm described a process for finding factors of a number, even a very large one in a very short amount of time. Integer Factorization serves as the basis for many of the worlds currently most secure crpytography algorithms, such as RSA. In Layman's terms, Shor's algorithm takes a guess at a number that could share factors with N (but most likely doesn't) and transforms that guess into a much better one that is very likely to be a number that shares factors with N. Understanding how algorithms like RSA operate is fundamental to understanding why Shor's Algorithm works. Shor's algorithm leverages the concept of quantum superposition mentioned earlier to compute factors of these very large numbers at a scale that is unmatched by modern classical computers. In order to compute factors of N

- Consider N, a very large number (eg: An RSA public key)
- In order to crack RSA, we neeed to find factors of N such that $f(x) = (x^r) mod N$.
- Shor's Algorithm shifts the focus to finding period r i.e: $f(x) = f(x+r)$.
- The algorithm uses something known as a *Quantum Fourier Transform*(QFT).
- A quantum computer can be in many states simultaneously, which leads to very fast computing.
- This allows the computer to calculate the period r for all points simultaneously.
- Then the QFT essentially takes these values, transforms them into waves in such a way that they destructively interfere with each other, leaving only the correct value of r.
- This r can then directly be used to solve for a factor of N, thus breaking the encryption.

Shor's algorithm also applies to cryptography schemes that depend on the *Discrete Logarithm Problem.*

V. Quantum Key Distribution

Quantum Key distribution or QKD, first proposed in 1970, is a means of secure communication over a channel. This is achieved via a crytographic protocol based on the fundamentals of quantum mechanincs. QKD enables 2 or more people to share messages using a shared random key, much like traditional cryptpgraphy. In QKD , information is encoded in single photons of light which require special hardware to create and transmit. QKD's use lies in generating secure cryptographic keys for use in conjunction with other cryptograpghy schemes such as RSA, it would be too unreliable and inefficient at directly sending information. QKD in essence, works as follows; Two users Alice and Bob wish to communicate with each other but are unsure if someone is eavesdropping on theier conversation. Alice tries to send a message to Bob using a "bitstream" that is encoded in a base of her choosing. If Bob also chooses the same base to decode the message, then their results correlate, otherwise they are random and are discarded. If someone tried to intercept the communication, they would introduce errors into the bitstream, this is discussed further below. This approach to key distribution comes with a number of advantages, namely that a secret key can be created in a provably secure way to prevent any any eavesdropping of private information, eavesdropping is easily detectable and perhaps most importantly, QKD has the ability to wasily integrate with current cryptography to provide additional security. In this scenario, the interceptor would not only have to break the quantum key but also the classical one.

There are two main types of QKD protocols: *Prepare and Measure* and *Entanglement Based*.

A. Prepare and Measure

Measurement one of the fundamental concepts of quantum mechanics. Measurement of a quantum state changes that state in some way. This fact of quantum mechanics can be taken advantage of to detect eavesdropping, as the very act of eavesdropping requires some level of measurement. Prepare and Measure techniques also allow us to see *how much* information has been intercepted. The most common prepare and measure protocol is BB84 which is discussed further below.

B. Entanglement Based

Entanglement based protocols exploit the quantum concept of entanglement which was explained earlier. Two or more qubits states become dependant on each other and they are in a joint state of superposition. Trying to determine the state of one of those qubits will directly result in a change in the other, making it very easy to detect eavesdropping. Theoretically, entanglement based protocols are much more secure than their prepare and measure counterparts, however it is currently unfeasible as managing and creating entangled qubits is very difficult.

C. BB84 Protocol

BB84 was the worlds first Quantum Key Distribution protocol. It was created in 1984 by Bennet and Brassard. BB84's operation can be divided into three layers:

1) Physical Layer: This layer is the most hardware intensive portion of BB84. This is where communication between two parties, Alice and Bob, takes place. Alice chooses random photons to send to Bob, these can either be encoded with a 1 with 50% probability or a 0 with 50% probability. She can then encode the photons in either "base" X or Y, each with equal probability. These encoded photons are then sent over a quantum channel to Bob. Bob does not know what base Alice used or any information about how the qubits were encoded. He measures each bit on a random basis in either X or Y each with 50% probability. This leads to Bob having 75% of the correct bases for the qubits.

2) Key-Extraction: In the next layer BB84 becomes classical to etract the key from the qubits that were sent by Alice. This layer consists of 4 sublevels. In the first sublevel called *sifting*, Alice and Bob reveal which bases they used and compare them over a public channel. They then proceed to discard the bits that do not correlate with each other.

In the 2nd sublevel *authentication*, Alice and Bob compare a subset of their bits to determine if their communication channel was compromised. If there is a higher error than can be accounted for by random noise, then the channel is believed to have been intercepted by a third party. This is because in order for an attacker to intercept the qubits, they must also guess the base wrong 50% of the time, leading them to forward some incorrect bits to Bob.

Error correction algorithms are then applied to reduce the effect of random noise on the data.

In the final sublayer *Privacy amplification*, the key generated from BB84 is combined with classical cryptography algorithms to reduce the effects of any undetected, minor eavesdropping and to maximize the security of QKD. This is done by encrypting the key itself using a scheme such as RSA or AES. This will require two levels of decryption.

3) Key-Application: The key-application layer is then responsible for using this generated key to encode data.

D. E91 Protocol

The E91 protocol is similar in nature to BB84 except it operates on entangled qubits. Alice and Bob both possess half of an entangled state. In this scenario there is nothing for an eavesdropper to intercept as the state of a qubit only settles after it has been measuered. As before Alice and Bob choose 1 iut of 2 bases to measure in, each with 50% probaility of getting chosen. After the qubits have been measured, they both share what bases they used over a public channel. If the qubits that were measured in different bases violate Bell inequalities, then states of the qubits remain entangled and it can be concluded that to eavesdropping has occured and the channel is secure. This is again, much more secure in theory than BB84 but it is impractical of the aforementioned decoherence problem of entangled qubits.

VI. Post Quantum Public-Key Algorithms

Along with the proposed methods of quantum key distribution, there has also been extensive research done into cryptography schemes that would be suitably secure for use in an age where quantum computers become powerful enough to bypass tranditional cryptography. There are three main areas of interest:

- Lattice-Based Cryptography
- Code-Based Cryptography
- Multivariate Polynomial Cryptography

These methods do not rely on the integer factorization and discrete logarithm problems used by so many cryptosystems today. Making them theoretically, viable candidates to replace these schemes.

A. Lattice Based

A lattice can be described as a grid of evenly spaces points stretching out to infinity in all directions. Lattice based cryptography has seen promising development in recent years. Instead of basing the algorithm on multiplying primes, lattice based solutions focus on multiplying matrices/vectors. The security proofs are related to hard math problems that involve lattice structures.

A *basis* of a lattice is a small subset of vectors from the original lattice that can be used to reproduce the original grid of points. Basis' are derived to conserve computer memory, as lattices tend to be very storage heavy. The basis of a lattice is *short* when it contains short vectors, likewise when the basis is long. Some lattice problems are described below as well what a public-key system based on lattice problems would look like. Pursuing a public-key cryptosystem has many advantages, lattice problems are some of the most well understood and researched types of hard math problems, dating back to the 1800's.

1) Short vector problem: In this problem a long basis is constructed from a lattice L. The task is then to find a point somewhere in the lattice's grid as close as possible to the point of origin. The hardness of this problem lies in the relative difficulty of finding a short point in a long basis. Furthermore, a lattice can be very large consisting of thousands of points, so finding a combination of basis vectors that concurrently leads to those thousands of points small turns into an extrenuous task.

2) Short Basis Problem:

- Given a long basis for a lattice L.
- Find a short basis in L.

3) Closest Vector Problem:

- Given a long basis for a lattice L.
- A randomly chosen challenge point P is also selected.
- Find the closest point in L to challenge P.

4) Public-Key Scheme: Encryption is done by selecting a vector v as plaintext. This vector would then be hidden by adding some error vector to it such that $c = v + e$. Decryption of the ciphertext would then involve solving the shortest vector problem mentioned aboce using c as the input. However this approach does not lead to secure schemes. When worst-to-average reduction schemes are applied, lattice based solutions also tend to lose their efficency. However NTRU, an open source lattice based cryptosystem seems promising. NTRU is very fast and efficient, but there could be unknown security flaws and no security proof exists for NTRU.

B. Code-Based

Code-based solutions make use off error correcting codes. They are based on the inherent difficulty of decoding linear codes. Code bases solutions are thought to be resilient against quantum attacks if their key size is increased by a factor of 4. The McEliece Goppa Code cryptosystem (MECS) is one of the most prominent code based solutions. In MECS encryption and decryption have quadratic complexity, which is on par with RSA. The main downside to MECS is the very large key size compared to other crypto algorithms. Common key sizes can be as big as 0.5Mb, vs 0.1Mb for RSA and just 0.02Mb for Elliptic Curve Cryptography (ECC). There is also no known polynomial time algorithm for decoding liner block codes and the problem is said to be NP hard, which further increases it's merit as a replacement for current encryption schemes. However, work needs to be done to improve the security of this system.

There are many known attacks against MECS, one of them was proposed by McEliece himself and is based on *information set decoding*. In this attack k co-ordinates are selected from n of the code in a way that no errors affect the selected co-ordinates. This can be done with probability of $(1 - \frac{t}{n})^k$. The plaintext message can then be extracted using simple algebra and the running time of the attack is an unbearable $k^3(1 - \frac{t}{n})^k$. This requires MECS to be combined with a semantically secure conversion to increase its security. Despite these vulnerabilites, MECS still remains a prime candidate for a drop-in replacement for algorithms such as RSA, should the need arise.

C. Multivariate Polynomial

A multivariate polynomial is a polynomial with multiple variables such as $-3x^7 - v^5y^4 + 5 + 6yx^3v^2$. Solving multivariate polynomials are also proven to be NP hard problems. Currently no encryption schemes based on multivariate polynomials exist, however there are some signature schemes implemented based on the concept such as Unbalanced Oil and Vinegar(UOV) and Rainbow. The most promising encryption scheme is called SimpleMatrix or ABC. ABC allows for very fast encryption and decryption, however decryption fails with high probabilities and the key size for the scheme is also fairly large. It is also worth noting that many proposed signature schemes have been broken in the past such as the aforementioned UOV. Multivariate polynomial cryptography is also very young, and it has not been thoroughly tested by cryptanalytic techniques to consider it a feasible option for post-quantum cryptography.

VII. Conclusion

Cryptography plays an ever growing role in our society. It is used to secure the transmission and storage of billions of peoples data. Quantum Computers propose a significant threat to the security of current cryptosystems that we have come to rely on. There are many promising post-quantum alternatives such as the code based McEliece cryptosystem and Lattice Based cryptography. It is unclear if any of the currently known algorithms will have the capability to serve as drop-in replacements when powerful quantum computers become a reality. Post-quantum cryptography faces many challenges in order to make it viable and there needs to be extensive research done to improve efficiency and usability. Development requires a collective, community effort to improve these problems and to build confidence in the security of any schemes proposed. However, the future looks bright as there are breakthroughs being made regularly, and it is improbable that the world will be completely unprepared by the time a sufficently powerful and usable quantum computer is developed.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

[2] My guy, *The New Codebreakers*