MATH 5347: APPLIED ALGEBRA WITH CRYPTOLOGY

Quantum Cryptography

Jordan Klumper, Kimberly Mandery

DUE 1600 26 November 2018

Abstract

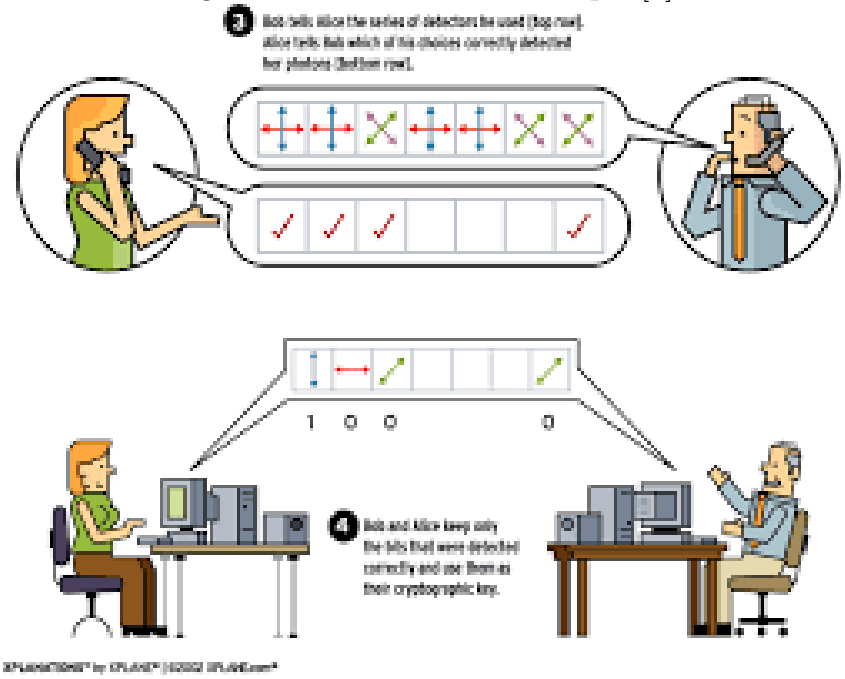
In this paper, we will introduce the roots of the quantum computing field and address it's ties with cryptography. The majority of quantum cryptography is theoretical at this point, thus the basics of the field and the ways in which quantum computing has affected the most commonly used cryptosystems will be discussed. For this paper, we will provide how RSA, ECC, and AES currently operate and how these common systems can be manipulated so that they are resistant to quantum computing attacks. The goal of quantum cryptography is to create a system that is nearly unbreakable with the influx of next-gen computing power.

Quantum Computing

To fully understand quantum computing, foundational knowledge of quantum theory is needed. Quantum theory is defined as the theoretical foundation of modern physics that explains the nature and behavior of matter and energy on the atomic and subatomic level [2]. Evermore, particles have guiding principles: they act like both a wave and a particle, they act in ways that defy the speed of light (and thus defy classical physics), and can be in more than one place at the same time. One of the more interesting aspects of this field is that a particle behaves like a wave in every instance except for when it is observed. This is akin to stating that we cannot know all there is about the state of a quantum system, called the Heisenberg Uncertainty Principle.

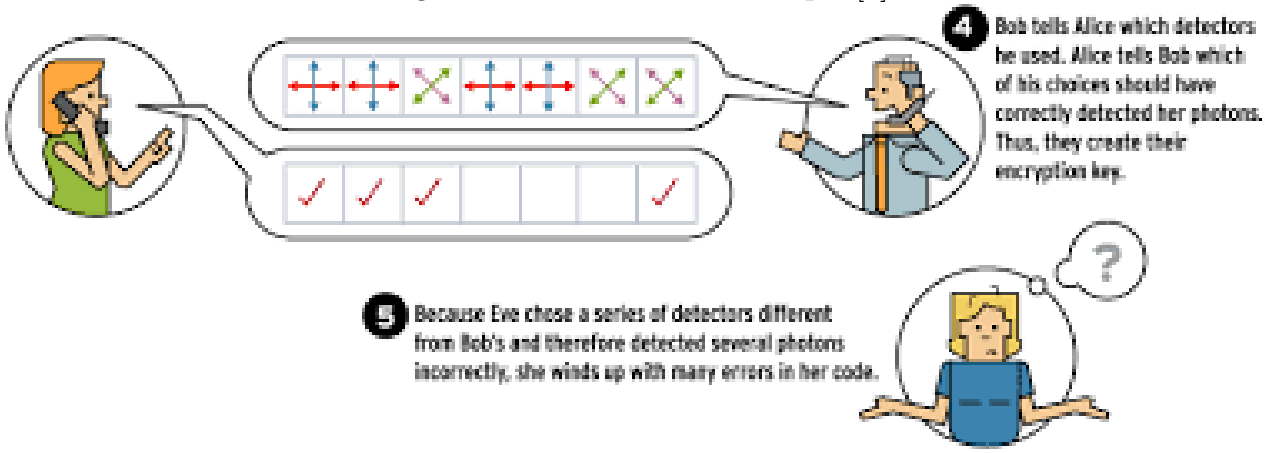
Applying quantum physics to computing, scientists were able to construct quantum versions of classical bits called qubits. These qubits are able to retain information of the classical two-state computations, as well as extending computation to probabilistic states where the qubit is neither a zero nor a one. Rather, these states are linear combination of probabilities of being both zero and one called superposition [5]. Superposition was first realized during the 1887 double-slit experiment by Michelson and Morley and later added upon by the metaphorical Schrodinger-Cat thought experiment in 1926 [5]. These experiments laid the groundwork for work on quantum entanglement, where measuring certain properties of linked particles affects all the particles that are connected. An analogy would be that of several baited hooks on the same fishing line, where the pull of one of the hooks by a fish affects the position of the other hooks. This linkage of entanglement is what makes quantum computing for cryptography so intriguing. To see these concepts in play, the following example is given using our two cryptologists Alice and Bob.

Figure 1: Alice and Bob Example [6]



In creating a random key for use on an encryption, Alice sends Bob a string of polarized photons. These photons can be of two types: rectilinear (either vertical or horizontal) and diagonal (either of the diagonals, i.e. D, D' $\in D_3$). Bob uses two filters, one for each scheme, and at random decodes the

Figure 2: Alice and Bob Example [6]



photons into binary. The rectilinear scheme would output the vertical as a one and the horizontal as a zero, and similarly for the diagonal scheme. He then sends the order of filters used to Alice. Alice sends back which filters are incorrectly used and they both get rid of the binary bit associated with the position of the wrongly identified photon. They now have a randomly generated key to use on any system.

In order for this to work properly, short travel distances and large enough strings of photons are necessary. The focus of enough photons is because Bob will choose filters at random, and as such will have a fifty-fifty chance of using the correct filter. In addition, if Bob uses the wrong filter, the photon would change (see Figure 1). This is called the Observer Effect and it indicates if Bob used the incorrect filter upon comparison with Alice. The Observer Effect is impactful for protection against attacks; if someone were to try to hack in, say Eve, it would influence the charge of the photon (see Figure 2). Bob and Alice would both know an intruder came in since they compare filters. Since each filter is used at random it would be nearly impossible for Eve. to correctly identify every filter 100 percent of the time.

When it comes to the positives and negatives of quantum computing, most are the by-product of how the quantum system is built. As alluded to in the example of Alice and Bob, it is important to understand the Observer Effect concept. When a system is measured it is altered, thus this concept is integral to both Alice and Bob in ascertaing when a hacker is interfering. This can also be a setback in computing as it is impossible to replicate quantum states without measurement. This theory, appropriately called the No-cloning Theory [2], prevents scientists from using classical error correction techniques. However, by storing the information of a singular qubit onto an entangled state of several qubits, scientists are able to circumvent classical error correction. QEC, or quantum error correction [3], is able to use this entangled system to not only find faulty qubits, but also effectively determine the various ways qubits can be affected using a metric called the syndrome measurement. Syndrome measurement allows researchers to create a superposition of basic operations and have each qubit "decide" [3] the state it should be in.

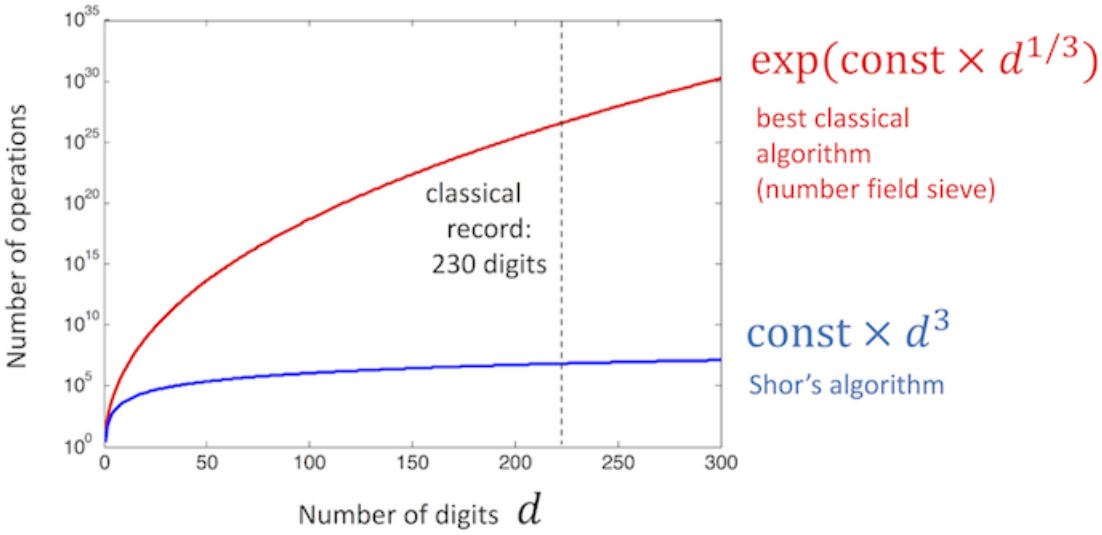
One drawback that is not dependent on the structure of the system, however, is the prevalence of quantum computing. Since quantum computing is in its infancy, it is difficult to effectively determine certain outcomes. The bright side to these drawbacks are that researchers can learn from mistakes and gain more information. As physicist Richard Feynman stated, "if you think you understand quantum mechanics, then you don't understand quantum mechanics" [4]. This does not counteract the previous

statement, but rather sheds light onto the vastness of what quantum computing could be. What researchers have found is that quantum computing is essential for safe-guarding current algorithms used in cryptography. The foundation for most of these advances in quantum cryptography includes incorporating Shor's Algorithm, a theoretical algorithm for finding prime factorization of incredibly large numbers. Shor's Algorithm [7] allows factorization to be completed in manageable computation time as seen in Figure 3. Shor's Algorithm is as follows:

1. Pick a number $a < N$ where a not a factor of N.
2. Find r, the period of a mod N where $a^r \equiv 1$ mod N
3. Check: r is even and $a^{1/2} + 1 \not\equiv 1$ mod N
4. Then $p = gcd(a^{1/2} - 1, N)$ and $q = gcd(a^{1/2} + 1, N)$

In Shor's Algorithm, finding Step 2 is akin to finding a global property of the function. This is where quantum computing comes in handy. To solve this, the Quantum Fourier Transform can be implemented. This transform uses resonances to amplify the basic state associated with the correct period and suppress amplitudes that incorrectly interfere [7]. Complex Analysis (i.e. complex roots of unity) can then be used in order to find most probabilistic space. As such, the algorithm can be continued after finding Step 2 in order to correctly solve for p and q.

Figure 3: Complexity Comparisons [7]

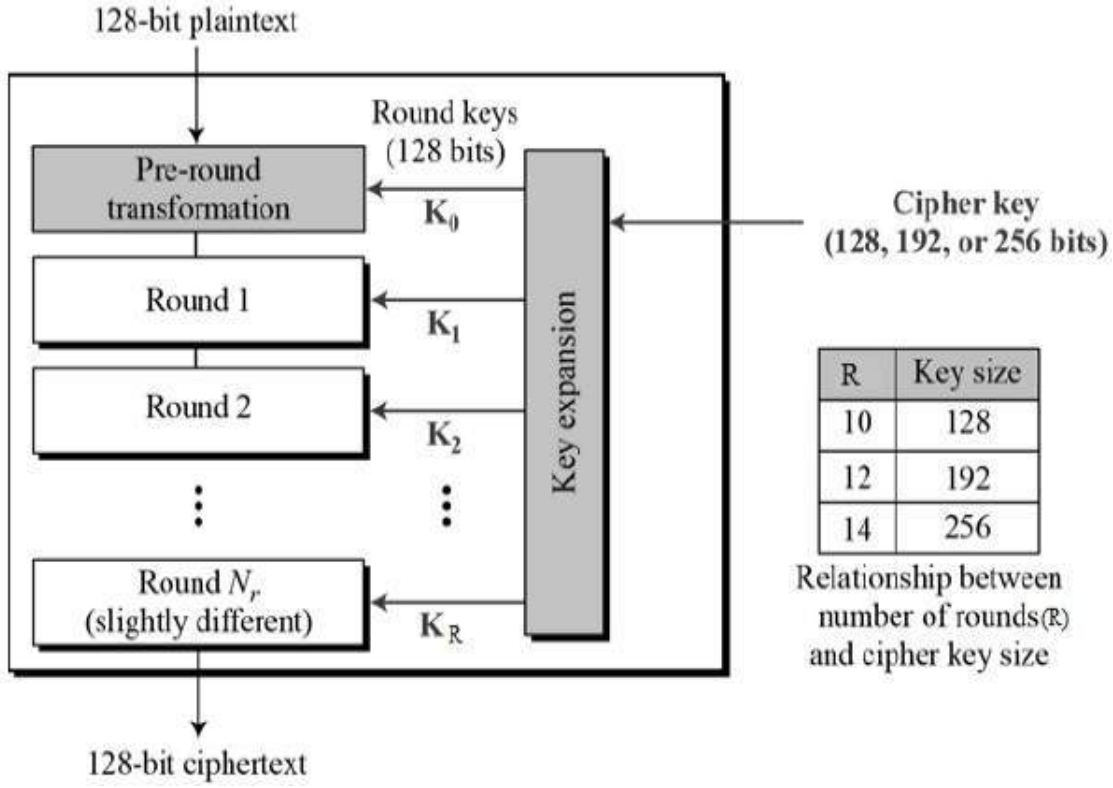


AES Methods and the Stability of 256

AES (Advanced Encryption Standard) is a single key cryptosystem first published in 1998 [10]. The same key is used both for encrypting and decrypting and the encryption occurs on blocks of bits, or matrices. It's a system that uses multiple operations on a block of 16-bits (a 4x4 matrix), these 16-bit blocks are created from 128 bits of plaint text.

In Figure 4, we begin with the 128-bit plaintext that gets converted to a 16-bit matrix. For each round, a different 128-bit round key (based on the overall key expansion) is used to perform an operation

Figure 4: AES Schematic [14]



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

on the message matrix. For different sizes of the overall key, a different number of rounds are used 10 rounds, 12 rounds, and 14 rounds for the 128-bit, 192-bit, and 256-bit keys, respectively.

Shor's algorithm is one method that would crack many common cryptosystems used today. AES is not based on the discrete logarithm problem. Therefore, Shor's algorithm isn't effective in breaking AES. There is a lesser known quantum algorithm published in 1996 [11], called Grover's algorithm, that allows one to crack AES in $\mathcal{O}(\sqrt{n})$ time as opposed to $\mathcal{O}(n)$ time in classical computing. While this is significant, it does not decrease the time it takes enough to viably crack AES-256 [17]. It does however render the 192-bit and 128-bit key unsecure [9]. Ultimately, AES can be improved by using a large key size and including it in authentication systems such as Kerberos (which verifies the authenticity of the users accessing information) [15].

RSA Methods and an Alternative

The RSA (Rivest-Shamir-Adleman) cryptosystem published in 1977 is an asymmetric system that relies on the discrete logarithm problem. This means that it relies on the difficulty of factoring the product of two very large primes. Here is the basic idea of the RSA key generation:

RSA Encryption: [8] [18]

1. Choose two large similar sized primes p and q.
2. Find $n = p \cdot q$ which is our modulus
3. Find $\phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$

4. Given e, the encryption key, find d where $d \equiv e^{-1} \pmod{n}$

5. We now have our public key: (n, e) and our private key: (d, p, q)

Unlike AES, the strength of this system is heavily reliant on the ability to factor numbers into their primes. Shor's algorithm is the perfect tool to utilize in order to break this cryptosystem; it would likely be able to factor the large numbers used in RSA in polynomial time which is a significant improvement and granting it the ability break our current RSA keys. Given the ability to use Shor's algorithm, we would be able to find $\phi(n)$ if we knew the prime factors of n. This would allow us to use the division algorithm to find our decryption key d mod n $\equiv e^{-1}$ and break the system.

As a substitute for RSA, a method that could be used is called XMSS (Extended Merkle Signature Scheme) published in 2011 [12]. This method is a hash-based signature scheme which uses a hash-function to take a very large or infinite set of data and assigns it to a finite set. A simple example of this would be taking the integers and mapping it to the integers mod n. Most signature schemes have slow key generation and allow only a small number of signatures. Since XMSS is not susceptible to quantum algorithms and preserves its asymmetric properties, it does not face these issues and thus serves as an alternative to RSA [19].

ECC Methods and Improvements

ECC (Elliptic-curve Cryptography), first proposed in 1985 [16], is a cryptosystem that utilizes point addition on elliptic curves, generally over finite fields. The operation of point addition is passing a line through two points on an elliptic curve and the resulting third point created is reflected across the x-axis. When a point is added to itself, the tangent line to that point is used to find another point that intercepts the elliptic curve. The difficulty of this system comes from finding how many times it takes of adding a point to itself to get to another specific point [8].

Elliptic curve form: $Y^2 = X^3 + AX + B$ where $4A^3 + 27B^2 \neq 0$
Discrete logarithm problem: Give points P and Q find n such that $Q = nP$

This security can be compromised using Shor's algorithm, which can also be used to find n in the above equation. Estimates in the field of quantum computing find that it may be even easier to crack ECC than it is RSA, simple by finding n we solve the discrete logarithm problem. This means we would just need to find n^{-1} in our field. This would allow any eavesdropper to decrypt the message or key sent [20].

Published in 2011 [21], supersingular isogeny key exchange is a direct improvement to ECC that keeps in place many of the same systems already used. Given the elliptic curve form expressed above the j-invariant of an elliptic curve that is found via the Weierstrass equation is: [21]

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

If the j-invariant is the same for two different curves over the same closed field, then the two curves are isomorphic. This results in the supersingular isogeny Diffie-Hellman protocol using the isomorphisms of the supersingular elliptic curves and their isogenies for security. Isogenies are rational mappings between elliptic curves that is also a group homomorphism. The quantum resistant portion comes from the isomorphisms of two curves [21].

The Future of Quantum Computing

The future of quantum computing is constantly being developed. A timetable for when we will have viable quantum computers varies quite a bit between experts, some estimates are anywhere from 5 to 50 years [22] [23], and rely heavily on any noteworthy breakthroughs in the field. As of right now we don't have any quantum chips that work above 100 qubits. In order to perform any significant function in the field of cryptography, estimates put the necessary quantity of qubits in excess of 100 million [7] [22].

One major hindrance in the study of quantum computing is the fragility of qubits. Noise, temperature, electrical fluctuations, and vibrations affect the state of qubits and how they operate. These disturbances can lead to loss of data contained within the qubit. Since much of the work in the field relies on working with qubits at fractions of a degree above absolute zero, it is important to consider the environment the qubits are in. The key to getting the qubits to work effectively is to create an environment void of undesired observance and physical disturbances. Currently, research is being made in order to eliminate these irregularities and create more efficient and effective quantum chips [23].

As of 2018, some of the more successful breakthroughs include Google's creation of a 72-bit quantum chip which is the largest of its kind so far. MIT has reported a triple-photon light. Intel is working on silicon-based processors for qubits [24]. IBM's quantum computer (see Figure 5) is currently available for use on the cloud. While these breakthroughs don't appear significant for quantum computing, there is a massive push by countries and companies to expand the boundaries of what is possible. This is a major focus for many in the tech industry because once major breakthroughs are made, then our current cyber-security infrastructure will be at risk.

Figure 5: IBM Quantum Computer

References

[1] *Visualizing 2-Qubit Entanglement*
http://algassert.com/post/1716

[2] *Quantum Theory*
https://whatis.techtarget.com/definition/quantum-theory

[3] *Quantum Error Correction*
https://en.wikipedia.org/wiki/quantum-error-correction

[4] *Richard Feynman Talks*
https://en.wikiquote.org/wiki/Talk:Richard$_F eynman$

[5] *Superposition Double-Slit Paradox*
https://phys.org/news/2014-10-superposition-revisited-resolution-double-slit-paradox.html

[6] *Alice and Bob Lab Example*
https://ieeexplore.ieee.org

[7] *Complexity of Classical vs Shor's Algorithm*
https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/110-Shor%27s_algorithm.html

[8] Jeffrey Hoffstein, Jill Pipher, J.H. Silverman *An Introduction to Mathematical Cryptography* 2008: Springer-Verlag New York

[9] *How secure is today's encryption against quantum computers?*
`https://betanews.com/2017/10/13/current-encryption-vs-quantum-computers/`

[10] *Advanced Encryption Standard*
`https://en.wikipedia.org/wiki/Advanced`$_E ncryption_S tandard$

[11] *Grover's Algorithm*
`https://en.wikipedia.org/wiki/Grover%27s_algorithm`

[12] *Hash-based cryptography*
`https://en.wikipedia.org/wiki/Hash-based`$_c ryptography$

[13] *Quantum Computing Lecture*
`https://people.eecs.berkeley.edu/ luca/quantum/lecture02.pdf`

[14] *Advanced Encryption Standard*
https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[15] *Kerberos (protocol)*
https://en.wikipedia.org/wiki/Kerberos_(protocol)

[16] *Overview of History of Elliptic Curves and its use in cryptography*
https://www.ijser.org/researchpaper/Overview-of-History-of-Elliptic-Curves-and-its-use-in-cryptography.pdf

[17] *The 256-bit AES Resists Quantum Attacks*
https://www.researchgate.net/publication/316284124_The_AES-256_Cryptosystem_Resists_Quantum_Attacks

[18] *RSA (cryptosystem)*
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[19] *XMSS: Extended Hash-Based Signatures*
https://tools.ietf.org/id/draft-irtf-cfrg-xmss-hash-based-signatures-10.html

[20] *Elliptic Curve Cryptography: ECDH and ECDSA*
http://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/

[21] *Supersingular isogeny key exchange*
https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange

[22] *Quantum Computing: How Close Are We?*
https://www.osa-opn.org/home/articles/volume_27/october_2016/features/quantum_computing_how_close_are_we/

[23] *How Close Are WeâReallyâto Building a Quantum Computer?*
https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/

[24] *Timeline of quantum computing*
https://en.wikipedia.org/wiki/Timeline$_of_quantum_computing$

List of Figures

1 Alice and Bob Example [6] 1
2 Alice and Bob Example [6] 2
3 Complexity Comparisons [7] 3
4 AES Schematic [14] 4
5 IBM Quantum Computer 7