Post Quantum Cryptography

Tara O'Kelly, *(Hons) Software Development, GMIT*

***Abstract*—The security implications of quantum computers has seen to the investigation of quantum resistant cryptography. The integrity of many modular cryptographic systems, namely discrete logarithm and factoring based systems [1], are at risk. Examining the pre-quantum state of cryptography and the predicted affect of quantum on cryptography, we will discuss the need for post-quantum computing. Subsequently, we will delve into the viable solutions. Although there are quantum computers that exist today, all are far from capable of performing operations complex enough to break cyptographic algorithms widely used today. The attempts of post-quantum cryptography are in contention with the emerging technology, pursuing to implement a *feasible*, *flexible* and *computationally efficient* solution before a pertinent quantum computer can be built.**

I. Introduction

The exponential evolution and prosperity of technology has brought... RSA & ECC v popular. Warn about the following being a basic review to understand the relevant points.

A. Introduction to Cryptography

Cryptography is a method of protecting data from people who are not authorized to see it. Encryption, a significant mechanism in cryptography, is achieved by transforming the plaintext into ciphertext, with the intent of rendering it meaningless to those who do not have the classified resources. With these resources, the ciphertext is usually transformed it back to it's original state, a process called decryption.

Symmetric-key encryption utilizes the same key to both encrypt and decrypt, AES being the prevailing form. Symmetric encryption is more accomplished in achieving a faster outcome than that of asymmetric. Problematically, the sender and the receiver must hold the same key. How do they exchange keys digitally without another party eavesdropping? A typical solution would be to use asymmetric encryption to exchange symmetric keys.

Asymmetric-key encryption (a.k.a. public-key cryptography) practices an encryption technique with two differing, mathematically linked keys. The first key being a public key and the corresponding key being a private key. As implied in it's name, the public key is to be publicized. The private key is to be kept secret. The public key can be used to encrypt data, whereas the homologous private key can be used to decrypt the data. An ideal public-key cryptographic algorithm should serve as a trapdoor function. A trapdoor function is a function that is easy to perform one way, but has a secret that is required to perform the inverse calculation efficiently. The objective is to decrease the probability that the secret could be identified as much as possible.

So far, we have acknowledged AES, RSA and ECC; all can be adopted in pursual of a **confidential** message. Cryptography is also concerned with proving the **integrity**, **authenticity** and **non-repudiation** of a message e.g. MAC, Digital Signatures. Another method attempting the assurance of integrity could be by hash functions, e.g. SHA.

B. Rivest Shamir Adleman

Rivest Shamir Adleman (RSA) was first publicized in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman. The RSA algorithm is the most popular and perhaps the best understood public key cryptography system. RSA's security derives from the difficulty of factoring two large integers and the expeditious multiplication to get these large numbers; it is a befitting example of the "trapdoor" methodology.

Two prime numbers, p and q, are generated. The values p and q are multiplied together to get the maximum value, n. A number pub is selected to be the public key, such that pub is not a factor of $(p-1)$ and $(q-1)$. Then the private key $priv$ is generated, such that $(priv * pub) mod (p-1) * (q-1) = 1$. As long as you know the values p and q, you can compute a corresponding private key from this public key, explaining how factoring relates to breaking RSA. Factoring the maximum number into its component primes allows you to compute someone's private key from the public key and decrypt their private messages.

C. Elliptic Curve Cryptography

Although Elliptic Curve Cryptography (ECC) was originally proposed in 1985 by by Neal Koblitz and Victor S. Miller, it was not widely utilized until the 21st century. It is not as widely understood as RSA, with it's complexity to blame. ECC allows the use of smaller keys than RSA to get the same levels of security.

ECC is based on the algebraic structure of elliptic curves over finite fields [2]. ECC handles the following domain parameters: (p, a, b, G, n, h). To briefly explain the parameters, p is the field that the graph is defined over, the variables a and b are values that define the curve, G is known as the generator point (a.k.a. base point), n is the prime order of G and h is the cofactor of the curve.

The private key d is a randomly selected integer in the interval $[1, n-1]$. Subsequently, the public key $Q = dG$. The security of ECC is built upon the Elliptic Curve Discrete Logarithm Problem (ECDLP) [2]; ECDLP in ECC applies to the laborious task of locating the discrete logarithm of random elliptic curve element even with a known point. With the given the domain parameters and Q, ECDLP refers to the problem of determining d. In a real world standard application, it would be unfeasible to check all the possibilities of d.

D. Quantum Computing

blah blah blah

II. Security Implications of Quantum Computers

blah

Does not have to have a QC but could be relying on a service provided by another party that has a quantum computer.

A. Shor's Algorithm

blah

B. Grover's Algorithm

Grover's Algorithm was formulated by Lov Grover in 1996. Harmful affects by the algorithm in question can be seen in symmetric encryption and hash functions, including the ever popular AES and the SHA family. It important to note that Grover's algorithm only decreases the security of these cryptographic methods; it does not break them.

A classical computer can do a search with the speed of $O(N)$ assuming we do not know if the search parameter exists in an unordered domain. Grover's algorithm suggests that the same search can be implemented in $O(\sqrt{N})$ time using quantum queries. Grover's acceleration from $O(N)$ to $O(\sqrt{N})$ is not quite as calamitous as Shor's. However, indicates another significant quantum approach to cryptanalysis by exhaustively searching the key space of classical ciphers [3].

C. Social Concerns

Hackers.

Governments:

Citizen Privacy - use NSA's leakage of PRISM program as example. Refer to [1].

Increase Global Tensions by increasing a governments ability to spy on another.

III. Post-Quantum Cryptography

blah

A. Classical Solutions

blah

1) Ex 1:

2) Ex 2:

B. Quantum Solutions

blah

1) Ex 1:

2) Ex 2:

C. Integration and Standardization

blah

IV. Conclusion

According to Kudelski there is no need to worry about QC breaking current cryptographic systems for years to come; cryptographers have time to create an optimal solution [4]. However, one must also consider the time costs of integration and standardization. It could take companies years blah blah blah.

Appendix A
Proof of the First Zonklar Equation

Some text for the appendix. This is obvious.

Appendix B
Proof of the First Zonklar Equation

Some text for the appendix.

Acknowledgment

The authors would like to thank...

References

[1] A. Majot and R. Yampolskiy, "Global catastrophic risk and security implications of quantum computers." *Futures*, vol. 72, no. Confronting Future Catastrophic Threats To Humanity, pp. 17 – 26, 2015. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=edselp&AN=S001632871500 live

[2] D. Verma, R. Jain, and A. Shrivastava, "Performance analysis of cryptographic algorithms rsa and ecc in wireless sensor networks." *IUP Journal of Telecommunications*, vol. 7, no. 3, pp. 51 – 65, 2015. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=108921659&site=e live

[3] Q. Zhou, S. Lu, Z. Zhang, and J. Sun, "Quantum differential cryptanalysis." *Quantum Information Processing*, vol. 14, no. 6, pp. 2101 – 2109, 2015. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=102915247&site=e live

[4] J.-P. Aumasson, "Feature: The impact of quantum computing on cryptography." *Computer Fraud Security*, vol. 2017, pp. 8 – 11, 2017. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=edselp&AN=S136137231730 live