University of Ottawa

MODERN CRYPTOGRAPHY IN A QUANTUM WORLD

A Glimpse into what the future holds for Cryptography

Matthew Langlois
7731813
PHY1300
Winter 2018
March 29

Contents

List of Figures

List of Tables

Abstract

As we shift into a quantum world our cryptographic algorithms will need to be updated to reflect the shift. Modern day cryptographic algorithms will become child's play to the computers the future may bring. It is important to ensure that the methods used for encryption are updated to reflect these changes.

This report analyzes how standard cryptographic algorithms offer security in modern computing. It will determine how modern cryptography stands up in a quantum era. Furthermore it will offer some insight into the future of cryptographic algorithms which will continue to work in a quantum world.

1 Introduction

Everyday millions of people around the world rely on computers to provide secure communication over the internet. Often times we take it for granted that the underlying cryptography algorithms just work - keeping our personal information secure in transit. Every time a website is visited with a green lock we trust, without hesitation, that our information will be secure from end to end.

As we slowly shift to a quantum world this may no longer be the case. Today's strong cryptographic algorithms will become weak to tomorrow's computers. Quantum will render extremely difficult tasks much easier to compute.

2 Modern Cryptography

The goal of cryptography is to offer fast computations one way while making the reverse extremely complex. In modern cryptography there are two types of systems which are able to do this: asymmetric and symmetric encryption systems. Asymmetric cryptography allows for the secure communication between multiple parties, commonly known as public key cryptography. Symmetric encryption enables the encryption of data through a secret key. Both of these type of encryptions have become standards with the National Institute of Standards and Technology, proving how resilient they are against today's computers.

2.1 Asymmetric ciphers

Public key cryptography systems, such as RSA, rely on the fact that factoring two extremely large prime numbers is very slow on current computers while multiplying the two numbers is simple and quick to compute. In fact attacking RSA is so slow that DigiCert claims cracking a 2048-bit key will take a modern computer over 6.4 quadrillion years to break [4]. However this will not always be the case, especially as we enter a quantum world.

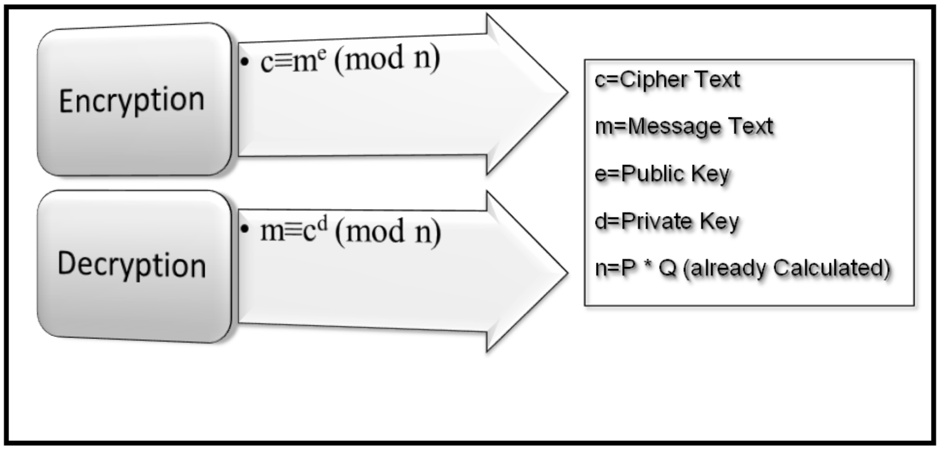


Figure 1: RSA Encryption/Decryption Algorithm [12]

Figure 1 demonstrates that when generating the modulus n for RSA two extremely large prime numbers known as P and Q are generated. In order to break RSA an attacker would need to determine the the prime factors which were used to generate n. The current standard is to use 2048-bits with RSA which is known to be secure since up to this point the highest number which has been factored was 768 bits long, which was achieve in 2009. RSA-1024 offers 1000 times more security that 768 bits and even RSA-1024 is considered obsolete at this point.

2.2 Symmetric ciphers

The second set of cryptographic algorithms used in modern cryptography are known as symmetric ciphers. Symmetric ciphers take an input and a secret key to produce an encrypted output. Unlike public key cryptography the key size required is much smaller to produce the same amount of security. In today's standards AES-128 is the recommended level of encryption to use for storage of documents securely, and would take approximately one billion billion years for a modern computer to crack [1]. In AES when a brute force attacked is performed, in the worst case scenario 2^{128} keys would need to be checked, something which is not possible in a reasonable amount of time with modern technology.

2.3 Security comparison

As you may have seen, asymmetric ciphers require many more bits to provide the same amount of security. This is due to the nature of generating a modulus. Unfortunately the more bits required the longer encryption takes, thus defeating the purpose of fast one way computations.

Table 1: Asymmetric vs Symmetric Key Comparison [13, p. 306]

Symmetric Key Size	**RSA Modulus**
80	1024
112	2048
128	3072
192	7680
256	15360

Table 1 demonstrates how rapidly the RSA modulus grows in comparison to a symmetric key size. In the modern era of computers this doesn't matter much since even with the smaller amount of bits we're still offered billions of years of security for both of these keys to be cracked. However these key sizes will come into play when analyzing them in a post quantum world.

3 Modern Cryptography in a Quantum World

Once again it is important to analyze how both symmetric and asymmetric ciphers will hold up in a quantum world. However before we can analyze the security of these two ciphers one must understand the basics of the theory behind a quantum computer.

3.1 What is "Quantum"?

The basis of quantum computing revolves around the ability to analyze data in multiple states rather than just an individual 1 or 0 as seen in modern computers. Quantum states are represented through quantum bits which are more commonly referred to as qubits. Qubits have the ability to store much more information at once while requiring much less energy to manipulate [2]. Essentially the information which can be stored in one qubit is much more than that of a bit in a classical computer.

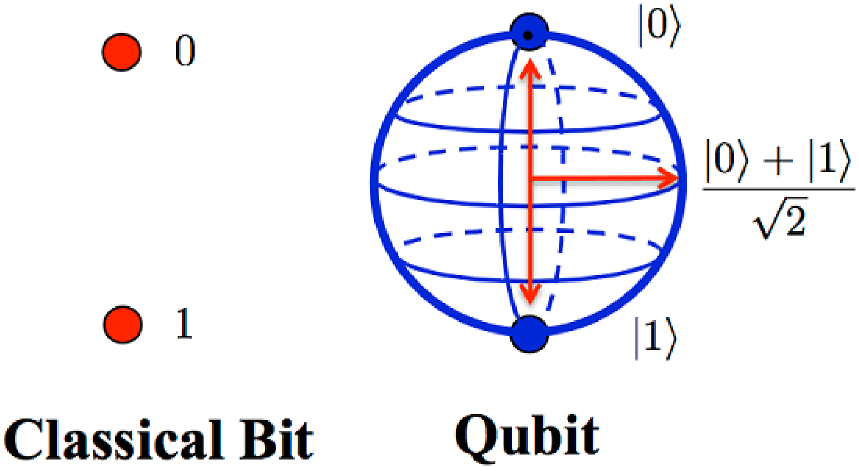


Figure 2: Classical Bit vs. Qubit [6]

Figure 2 demonstrates how a qubit is able to store much more information than a single bit in a classical computer. Ultimately a qubit can simultaneously represent a zero and a one which greatly improves the time for complex calculations. This ability to analyze multiple states is what will ultimately break modern cryptography. Now that there is a basic understanding of how a quantum computer stores information it is possible to determine how modern algorithms hold up in a quantum world.

See appendix A.1 for an example of a quantum computer being used for Artificial Intelligence research at Google.

3.2 Modern cryptography in a quantum world

Once again it is important to analyze both asymmetric and symmetric algorithms in a post quantum world. This will allow us to truly understand the impact quantum will have on modern day cryptography. Two key quantum algorithms will be analyzed to determine their impact on modern cryptography.

3.2.1 Asymmetric ciphers

Recalling how asymmetric ciphers work they rely on the principal that factoring is extremely difficult for modern computers to calculate, running in exponential time. Theoretically, in quantum computing factoring becomes much easier, so much so that it goes from exponential time to polynomial time. The algorithm which will break RSA in a true post-quantum world is known as Shor's algorithm [3].

Without going into too much detail, Peter Shor was able convert the problem of factoring a number into a quantum algorithm. Shor's algorithm works by converting factoring into a period problem, which can be done on a classical computer, and then finding the period using the existing quantum Fourier transform [3]. With Shor's algorithm RSA is rendered useless since the problem was taken from exponential time to polynomial time thus being solvable in a reasonable amount of real-time.

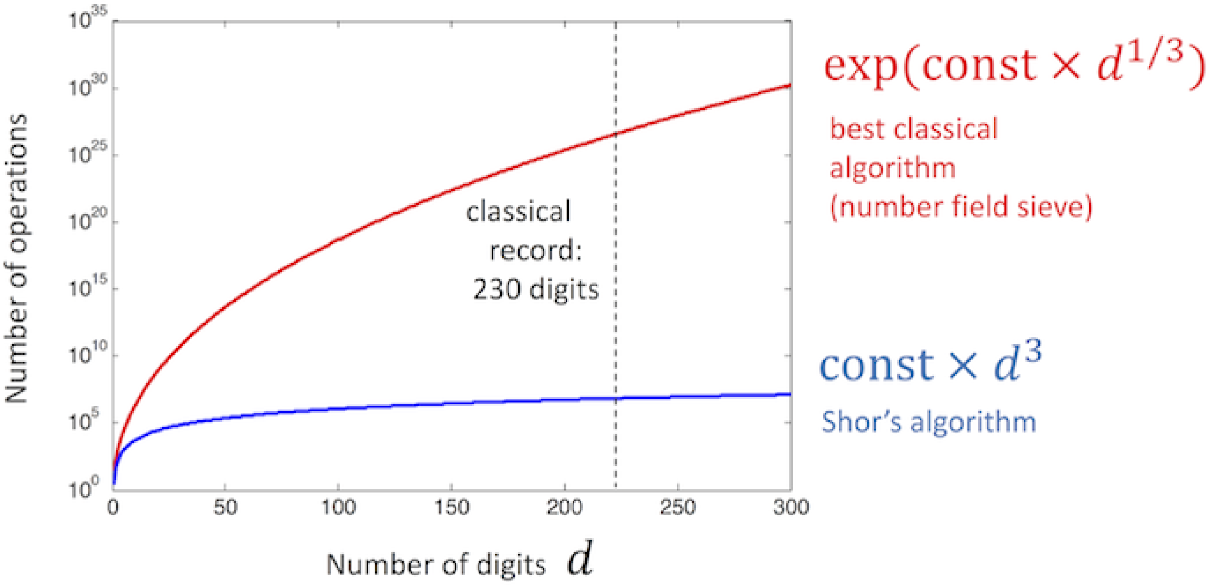


Figure 3: Shor's Algorithm vs Classical Algorithm [8]

Figure 3 demonstrates how Shor's algorithm is able to greatly increase the speed at which factoring is done. Thus with Shor's algorithm todays standard for asymmetric communications will become useless in a truly quantum world. Thankfully at this point the quantum machines are not stable enough, nor do they have enough qubits to properly implement Shor's algorithm.

3.2.2 Symmetric ciphers

In comparison to asymmetric ciphers, symmetric ciphers such as AES stand a much better chance in the quantum space. When stated earlier the worst case scenario in classical computing was that the entire key space of AES would require searching through a brute force attack. For example AES-128 would require 2^{128} operations to find the key.

In a quantum world Grover's algorithm can be applied to reduce that key space by a factor of 2. Thus AES-128 essentially become 2^{64} in the worst case, which is not considered secure by today's standards[9]. However this problem is easily solved by increasing the size of the key, for example using AES-256 now would be like using AES-128 in a quantum world. Recall that AES-128 takes billions of billions of years to crack thus symmetric ciphers are much more resilient to quantum attacks. NISTS's recommendation is to use larger keys on symmetric ciphers when moving to the quantum space [11].

4 Post-Quantum Cryptography Progress

As it stands right now quantum is such a new field that there is no single solution to cryptography in a post-quantum era. Currently the National Institute of Standards and Technology are exploring various algorithms to produce the first standard of post-quantum cryptographic algorithms.

Table 2: NIST Post-Quantum Standard Research Timeline [10]

Date	
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analyze Proposals
2 years later	Draft Standards

So, as seen in Table 2, there is no standard algorithm yet. In fact researchers are only just beginning to prepare for security in a post quantum world. There is still plenty of research which needs to be conducted before there is an algorithm which is deemed strong enough and has been thoroughly tested enough to be considered secure on a quantum computer.

There has been some research conducted into lattice based cryptography to replace modern public key cryptography. However these approaches to replacing modern cryptography are too new to fully determine if they would be able to stand up to a post-quantum world [5]. There is still plenty of research being conducted around lattice based cryptography.

5 Conclusion

Cryptography is essential to our daily lives and as computers evolve the algorithms to keep our data secure must also evolve. Unfortunately as it stands right now quantum computers will likely break modern cryptography. A new form of asymmetric ciphers must be developed to ensure a secure post-quantum era. Thankfully proper implementations quantum computing which may be capable of breaking modern cryptography are still a while away.

Currently NIST is researching standards to replace modern cryptography so once a quantum computing is around there will be algorithms which exist to keep communications and data secure. Furthermore not all algorithms will be broken, for example NIST recommends just increasing the key size for AES from 128 to 256. The proper steps are being taken to ensure when quantum computing is common the quantum cryptographic algorithms will also be common.

References

[1] Mohit Arora. *How secure is AES against brute force attacks?* URL: https://www.eetimes.com/document.asp?doc_id=1279619.

[2] Abigail Beall and Matt Reynolds. *What are quantum computers and how do they work? WIRED explains.* URL: http://www.wired.co.uk/article/quantum-computing-explained.

[3] Stephanie Blanda. *Shor's Algorithm – Breaking RSA Encryption.* URL: https://blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/.

[4] DigiCert. *The Math Behind Estimations to Break a 2048-bit Certificate.* URL: https://www.digicert.com/TimeTravel/math.htm.

[5] Jeong San Kim Dong Pyo Chi Jeong Woon Choi and Taewan Kim. *Lattice Based Cryptography for Beginners.* URL: https://eprint.iacr.org/2015/938.pdf.

[6] Eyeres. *Google Introduces OpenFermion, A Software To Ease Scientists In Using Quantum Computers.* URL: https://www.eyerys.com/articles/news/google-introduces-openfermion-software-ease-scientists-using-quantum-computers.

[7] Quentin Hardy. *Google Buys a Quantum Computer.* URL: https://bits.blogs.nytimes.com/2013/05/16/google-buys-a-quantum-computer/.

[8] IBM. *Shor's algorithm.* URL: https://www.qiskit.org/ibmqx-user-guides/full-user-guide/004-Quantum_Algorithms/110-Shor's_algorithm.html.

[9] Martin Roetteler Markus Grassl Brandon Langenberg and Rainer Steinwandt. *Applying Grover's algorithm to AES: quantum resource estimates.*

[10] NIST. *Post-Quantum Cryptography.* URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline.

[11] NIST. *Post-Quantum Cryptography: NIST's plan for the future*. URL: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/pqcrypto-2016-presentation.pdf.

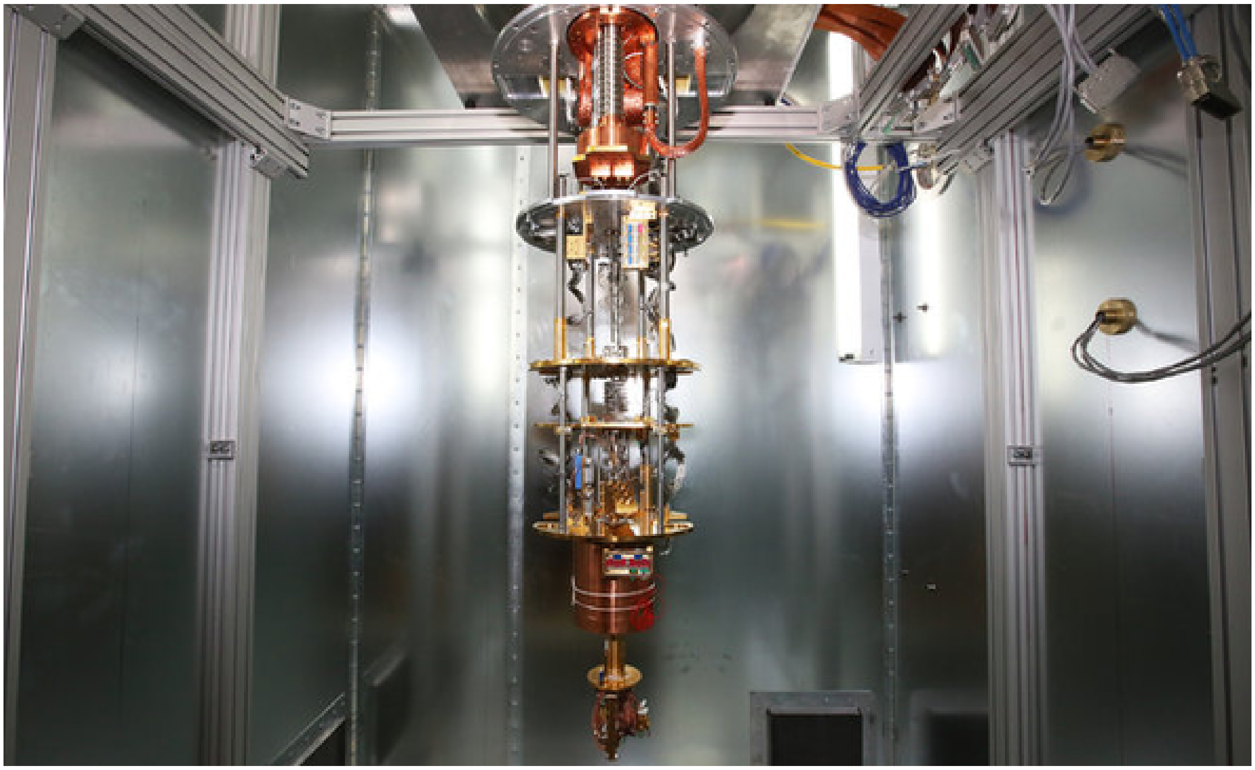
[12] Sourabh Somani. *RSA Algorithm with C#*. URL: https://www.c-sharpcorner.com/UploadFile/75a48f/rsa-algorithm-with-C-Sharp2/.

[13] William Stallings. *Cryptography and Network Security. Principals and Practices*. 6th ed. Pearson.

A Appendix

A.1 Google's Quantum Computer

It is cool to see the progress of quantum computers in today's age. Currently there is a race for quantum computing and while there isn't any perfect stable solution yet there has been quite a bit of progress. IBM offers 20 qubit cloud clusters for people to test their algorithms against while Google is working with NASA to perform AI research using their quantum computer.



Google's Quantum Computer being used for research in AI [7]