How long can Public key encryption stay secure? Introducing the implications of the Riemann Hypothesis and Quantum Computing

Mo Adda, Mo.Adda@port.ac.uk
Abby McKeever amckeever@gmail.com
Amanda Peart Amanda.Peart@port.ac.uk
University Of Portsmouth, Portsmouth, UK

Abstract

As the power of computing increases, public key cryptography adapts by increasing the size of the prime numbers used by the underlying cryptographic algorithms. Public-key algorithms have been in use since the 1970s, but how long can these algorithms remain secure? In light of the emergence of quantum computing together with the prospect that the Riemann Hypothesis has been proved, this paper will investigate the possible impact on the security of current encryption algorithms.

If these theoretical technological advancements become reality, what will be necessary to maintain the security of the global system? It is imperative that the security of communication is not compromised. Therefore to overcome the problem of the exponential increase in computational power of quantum computing is to use it to bolster the potential insecurities of current algorithms by developing a cryptographic system based on quantum mechanics.

The Quantum Key Exchange approach demonstrates the strength of such a system. It is believed from our current understanding of quantum physics that this method is very secure and that an eavesdropper cannot intercept the key without both sender and receiver having knowledge that the key had been compromised, as the polarization will have been altered. The limitation with this system is if the intruder has connected to the channel before the communication has begun, neither sender nor receiver will be aware of the interception.

Current encryption algorithms will not remain secure permanently; therefore it is essential that to maintain a secure system that cryptology constantly evolve. There are many technologies that could be used in cryptology but either of the advancements above could destroy the safeguards of current methods.

1. Introduction

As the power of computing increases, public key cryptography adapts by increasing the size of the prime numbers used by the underlying cryptographic algorithms. But how secure are prime numbers? The problem is finding a way of encrypting information that will be secure in the future as well as today.

Public-key algorithms have been in use since the 1970s, and primes have been applied to the area of cryptology for even longer, so just how long will they remain secure? With the emergence of ideas such as quantum computing and the possibility that someone may have proved the Riemann Hypothesis, the current methods of encryption may soon be dated. Even if the current methods of encryption become obsolete, why should anyone be concerned? Unfortunately, the problem is now one

greater than just academic interest. With the rise of the Internet, over the last 20 years, these encryption technologies have been incorporated into the whole infrastructure of the global economy.

From individual purchases in an online store, to global inter-bank transactions, our society and all the information underpinning it, is now stored in a digital format interconnected by what has been dubbed the Digital Nervous System. With this digital evolution, any compromise of the current security mechanisms could cause catastrophe on a global scale.

The intention of this paper is to investigate the encryption algorithms in current use, and to explore the mathematical theories underpinning them. From this investigation we should be able to analyse how secure these algorithms are, and how vulnerable these current technologies would become if future developments materialise.

2. Security Algorithms

There are two common categories of encryption algorithms symmetric and asymmetric. However, symmetric algorithms are outside the scope of this paper, therefore the focus is on asymmetric public-key technologies.

2.1 Public Key Cryptography

The basic idea of public key algorithms is that both the sender (normally referred to as Alice) and the receiver (Bob) create a public key (Ka +, Kb +), which is made publicly available, and private keys (Ka -, Kb -), which are kept secret. To make these keys secure, they contain 30 or more digits. Alice encrypts the message with Bob's public key. The only way to decrypt, and therefore read the message, is to use Bob's private key; this is denoted by [23]:

Encryption	$K_b^+(M)$
Decryption	$K_b^-(K_b^+(M)) = M$

2.2 RSA

One of the most common public key algorithms is called the RSA (Rivest, Shamir, Adleman) algorithm, which uses prime factorisation in a trapdoor one-way function [25]. To assess how secure this and other similar algorithms are, we first need to briefly cover the mathematical theories they are based on.

Primes are used to created keys by the following computation [3]:

Find 2 large (>30 digits long) primes, called *p* and *q*

n = pq and
$\phi(\mathbb{Z}) = (p-1).(q-1)$

Define a private key ***d*** and a public key ***e***, such that:

$d * e = 1 \bmod (\mathbb{Z})$

Prime number based public key encryption, such as RSA, is based on the assumption that it is relatively simple to find 2 large prime numbers, but it is very difficult to factor a large composite into its prime factorisation form [3]. Based on this assumption, public key algorithms appear very secure. Moreover, if an intruder (Trudy) cannot acquire the private key, it would take a long time (somewhere around the age of the universe) and a significant amount of computational power to undertake a brute force decryption [21].

This method of using prime numbers for factorisation has never been proved, but it has been accepted as secure due to a negative proof, i.e. in most mathematicians' professional opinions, that is, because there is no known proven method to factoring prime numbers, the resulting keys are for all practical purposes unbreakable. The big problem with a negative proof, is just because we are currently unable to break the prime number based public key encryption, we can't assume that it cannot be done; therefore a negative proof, albeit statistically favourable, is not a proof. Concerns have arisen following two recent developments that could make PKI algorithms vulnerable; the possible proof of the Riemann Hypothesis, together with the evolution of quantum computing.

3. Riemann Hypothesis

This mathematical hypothesis was conjectured by Riemann in 1859, and states that all the nontrivial (complex) zeros ρ of $\zeta(s)$ lying in the critical strip $0 < \mathrm{Re}(s) < 1$ must lie on the critical line $\mathrm{Re}(s)=½$, that is, $\rho=½+it$, where ρ denotes a nontrivial zero of $\zeta(s)$. [24]. Basically, the proposed formula calculates the number of primes less than a given number. Until this theory it was suggested primes were just scattered with no apparent pattern among the whole numbers. If Riemann's conjecture is correct it could have great implications for the way we encrypt information, as the mathematics surrounding the solution could reveal quicker ways to factorise the numbers. If correct, the hypothesis can be diagrammatically shown as in figure 1. The position of the complex zeros can be seen slightly more easily by plotting the contours of zero real (red) and imaginary (blue) parts. The zeros (indicated as black dots) occur where the curves intersect [24].

As this hypothesis has not been proved or disproved (at least not publicly) although, a Purdue University mathematician, Louis De Branges, claims to have proven the Riemann hypothesis [8]. This is likely to take several years to confirm as the mathematical community has to analyse the proof and accept it as correct, but it is quite likely that the cryptology experts will, in the not too distant future, need to find a new way of encrypting data. There is the possibility that this hypothesis is never proven, or that even if is correct, it does not follow that computers will be able to factorise numbers faster. This is not to say that our current method of security is timeless. Another technology on the horizon is that of 'Quantum Computing', which could yield the power to crack a public key cryptographic system in a relatively short time using a brute force attack (based on current claims of the power available).

To assess the impact that quantum computers could have, we need to review the basic ideas behind them. A quantum computer works by manipulating atoms (or light) instead of silicone. The data is represented either by two different polarisations of light, or two different electronic states of an atom. Quantum mechanics is the area of physics seeking to understand events occurring at the atomic level. Quantum mechanics dictates that as well as the two distinct electronic states that an atom can have, the atom can also be under the effect of 'superposition', which basically means that the atom can be in two electronic states at the same time. In the area of computing, this equates to each quantum bit, called a qubit, being able to be both a 1 **and** a 0 [1].

This idea of superposition comes from experiments that look at the behaviour of light, where a photon can take 2 paths at once [4]. Superposition was also the basis for one of history's most intriguing, puzzles –Schrödinger's Cat. This involved the idea of putting a (hypothetical) cat in a box, and if the test atom decayed, the box would be filled with a lethal gas and the cat would die, and if the atom did not decay the gas would not be released and therefore the cat would live. However, according to superposition this atom could be in both a state of decay **AND** a state of non-decay, therefore the cat would be in a state of alive and dead at the same time.

As this does not happen (cats being both dead and alive in the same moment) some physicists, including Einstein, proposed that there were some 'hidden variables', but John Bell later ruled out most of these in 1964. The only 'hidden variables' that were not ruled out were non-local variables, which meant they could act instantaneously across a distance.

This interaction between particles is known as quantum entanglement with changes of state in one particle resulting in complimentary and instantaneous changes in the other particle [12]. Entanglement has lead to 2 further theories; quantum information theory, which implies that information, can travel at speeds faster than the speed of light, and quantum teleportation. From quantum teleportation, Bennett et al [5] showed the following:

> *If both Alice and Bob had one of 2 particles that are entangled together a quantum state can be transmitted from A to B.* [5].

If this were proven to be true, and manageable, this could revolutionise the way communication is carried out! This is outside the scope of this paper, however, the idea of superposition can be continued further. A standard computer with a set of data, say a byte in size, 8 bits, can represent **one** of a maximum of 256 possible numbers; with a quantum computer, 8 qubits can represent **all** the 256 possible numbers at once! With this exponential increase in computational power, it is not hard to see that a time consuming task, such as factorisation, could be completed in a reasonable time with a quantum computer.

4. The way forward

One way that could provide a means of encryption that is secure against both the potentially flawed mathematics postulated by the Riemann hypothesis, and the extreme computational power of Quantum Computing, would be to use a cryptographic system based on quantum mechanics. There are already some basic options available in the field of Quantum Cryptography, predominantly around the area of Quantum

Key Exchange (for example products made by Magiq); this approach offers a very secure communication channel, however, this is currently very expensive due to each key channel requiring a dedicated optical fibre, and has a low data rate for technical reasons. However, due to our current understanding of the laws of Quantum Physics, this is very secure as there is apparently no way an eavesdropper, even with unlimited computing power, could intercept the key without both sender and receiver knowing that the key was compromised. To understand why this is so secure, we first have to look at how this method works. A quantum system consists of a transmitter, a receiver, and a quantum channel through which the polarised photons can be sent. [6]. These polarised photons can have 4 different polarisations:

0°, 45°, 90°, 135° which are defined as → , ↗ ,↑, ↖ respectively

The receiver can either distinguish between the rectilinear polarisations (→,↑) or between the diagonal polarisations (↗,↖) at one time. A good example of how this could be used to send a key, is by using a quantum version of the Diffie-Hellman key exchange/distribution system (proposed by Bennett and Brassard in 1984) as shown below:

1. Alice uses the transmitter to send a series of random photons with different polarisations to Bob, for example:

↖ → ← ↖ ↑ ↗ → ← ↑

2. Bob then uses the receiver to measure the polarisations, recording the results (keeping them secret):

↖ ↖ ↗ ↖ ↑ ↗ → → ↑

3. Bob (publicly) tells Alice the type of measurements he made, and Alice confirms which of the measurements were correct:

√ - - √ √ - √ - √

4. Alice and Bob translate all cases where Bob observed the correct polarisation type, into bits – these bits then form the key:

↖ ↖ ↑ → ↑
1 1 1 0 1

Where ↖ and ↑ = 1, ↗ and → – 0

5. Using this key, Alice can now encrypt the message for Bob using a classic public key algorithm (this would involve a larger number of photons to be able to create a secure enough key) [3].

This is secure from eavesdroppers, as even if they could measure the photons, they could not do this without altering the polarisation, therefore alerting Alice and Bob that the channel has been compromised.

5. Conclusion

The main problem with the above proposed quantum cryptography based solution is that if a man-in-the-middle attacker, Mallory, managed to connect to the quantum channel before Alice and Bob began communication, he could impersonate Alice and Bob, i.e. tell Alice he is Bob, and tell Bob he is Alice, and therefore would not have the problem of intercepting the photons and changing the polarity. Mallory could then in theory establish a quantum key exchange with both Alice and Bob, allowing Mallory to read a message from Alice, and then encrypt this message using the key agreed with Bob. Using this technique it is entirely possible that neither Alice nor Bob will ever know there was is a problem. This situation, although unlikely, is possible and should be investigated; however, one possible solution may be procedural rather than trying to solve it by modifying the algorithm. A much more significant point to be made about a quantum computing solution is that quantum computing is still only theoretical, in that a quantum computer is only experimental. Although it is only a matter of time as the physics behind it have been proven (to a point) and it is now just an engineering problem to be overcome (managing individual photons, and creating entangled atoms that are stable enough to be useful). However, it will still be some years before this would be widely available to the public. In the meantime, the Riemann Hypothesis could be proved, so realistically we need a more achievable method of encryption using existing technologies. One possible solution would be to

utilise biometric data, such as a retinal scan into the key, but this solution is out of the scope of this report.

We cannot be sure what will occur in the future the Riemann Hypothesis maybe be disproved and that quantum computing could be unachievable, which would result in prime numbers remaining secure. Even if these two particular issues do not destroy current encryption methods, primes are going to be made insecure at some point, therefore cryptology needs to keep evolving by investigating new areas.

In conclusion, the area of encryption and security has been dependant upon the security of primes, and in order not to have a single point of weakness security needs some revolutionary ‘out-of-the-box’ ideas giving viable alternatives to the current methodologies and logic.

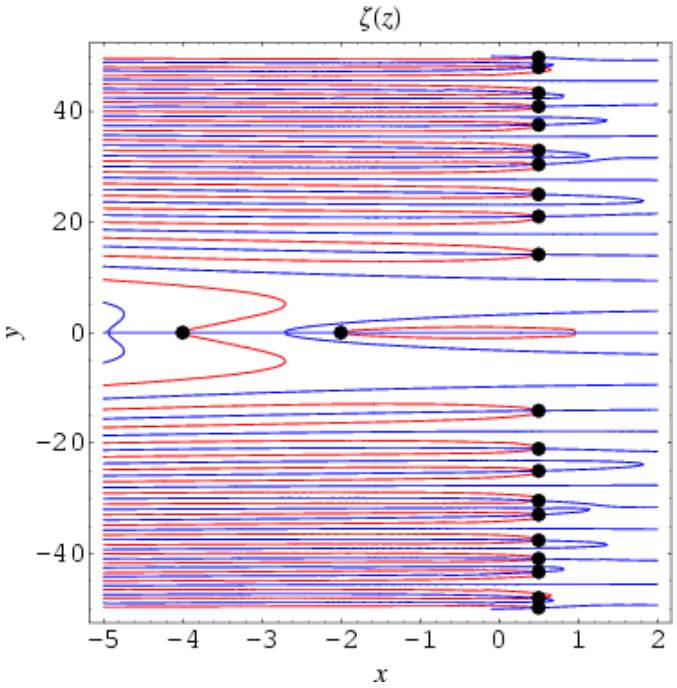

Figure 1. Riemann Hypothesis [24]

The position of the complex zeros can be seen slightly more easily by plotting the contours of zero real (red) and imaginary (blue) parts. The zeros (indicated as black dots) occur where the curves intersect. [24].

Bibliography

Printed Resources

1. Chuang, I. L., Nielsen, M. A. (2000). *Quantum Computation and Quantum Information.* Great Britain: Cambridge University Press.
2. Giblin, P. (1993). *Primes and Programming – An Introduction to Number Theory with Computing.* Great Britain: Cambridge University Press.
3. Yan, S. Y. (2000). *Number Theory for Computing.* Germany: Springer-Verlag.

Electronic Resources

4. Barenco, A., Ekert, A., Machiavello, C., Sanpera, A. (1996). *A Short introduction to Quantum Computing*. From www.qubit.org/library/intros/comp/comp.html
5. Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wootters, W. (1995). *Quantum Teleportation.* From www.research.ibm.com/quantuminfo/teleportation/
6. Bennett, C. H., Brassard, G., Ekert, A. K. (1992). *Quantum Cryptology.* From Scientific American, 26-33.
7. Bloor, R. (2004). *What is the Riemann Hypothesis and Why Should I Care?* From http://it-director.com/article.php?articleid=12296
8. Boutin, C. (2004). *Purdue Mathematician Claims Proof for Riemann Hypothesis.* From http://news.uns.purdue.edu/UNS/html4ever/2004/040608.DeBranges.Riemann.html
9. Caldwell, C. K. (n.d.). *Riemann Hypothesis At The Prime pages*. From www.utm.edu/research/primes/notes/rh.html
10. Castro, M. (n.d.). *Do I Invest in Quantum Communications Links for My Company?* From www.doc.ic.ac.uk/~nd/surprise_97/journal/vol1/mjc5/
11. Centre for Quantum Computation. From www.qubit.org/
12. Henderson, L., Vedral, V. (n.d.). *CQC Introductions: Quantum Entanglement.* From www.qubit.org/library/intros/entang/index.html
13. Hoffman, J. (2004). *Prime Time.* From www.bostonreview.net/BR29.2/hoffman.html
14. IBM Zurich Research Lab. (n.d.) *Information Security and Cryptography.* From www.zurich.ibm.com/csc/infosec/
15. IBM Zurich Research Lab. (1998). *Researchers Close Security Gap in the Internet.* From www.zurich.ibm.com/news/98/n-19980824-01.html
16. LinuxSecurity.com Team. (2000). *Maths prize could revolutionise encryption*. From www.linuxsecurity.com/content/view/107695/65/
17. McKee, M. (2004). *New Scientist Special Report on Quantum World.* From www.newscientist.com/channel/space/quantum-world
18. Ost, L. (2004). *NIST System Sets Speed Record for Generation of Quantum Keys for 'Unbreakable' Encryption.* From www.nist.gov/public_affairs/releases/quantumkeys.htm
19. Reynolds, P. (2004) *Breaking Codes: An Impossible Task?* From http://news.bbc.co.uk/1/hi/technology/3804895.stm
20. Rincon, P. (2004). *Teleportation goes Long Distance.* From http://news.bbc.co.uk/1/hi/sci/tech/3576594.stm

21. Weisstein, E. W. (n.d.) *Prime Factorization.* From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PrimeFactorization.html
22. Weisstein, E. W. (n.d.) *Prime Number Theorem.* From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PrimeNumberTheorem.html
23. Weisstein, E. W. (n.d.) *Public-Key Cryptography.* From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/Public-KeyCryptography.html
24. Weisstein, E. W. (n.d.) *Riemann Hypothesis.* From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/RiemannHypothesis.html
25. Weisstein, E. W. (n.d.) *RSA Encryption.* From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/RSAEncryption.html
26. Whitehouse, D. (2004) *Largest Prime Number Discovered.* From http://news.bbc.co.uk/1/hi/sci/tech/3783149.stm
27. Whitehouse, D. (2000) *The Secret of Squares Revealed.* From http://news.bbc.co.uk/1/hi/sci/tech/665310.stm
28. Wikipedia. (2005). *Quantum Cryptography.* From http://en.wikipedia.org/wiki/Quantum_Cryptography