Quantum Computing and its effects on Deciphering Public Key Encryptions

Jason Lin
Ethical Hacking and Systems Defense
University of Southern California
jasonjli@usc.edu

Abstract

Google's researchers has recently announced that the team was able to test the results of its quantum computing efforts and claimed their quantum annealing algorithm to run a hundred million times faster than a comparable classical algorithm. While it is the first time the search giant has attempted to prove its validity in the quantum realm, it is expected that in the foreseeable future quantum computing is going to become reality. We all know that quantum computing is good for solving optimization problems because of its nature of accepting a large variety of parameters. As most popular public-key algorithms today thrive on the fact that its nondeterministic polynomial complexity would take a classical computer unrealistic time to solve, the arrival of quantum computer would solve efficiently some of the problems that have challenged us for decades.

We investigate the fundamental principles of encryption and review in depth the three hard mathematical problems that reliable public-key encryptions today are based upon: the integer factorization problem, the discrete logarithm problem and the elliptic curve discrete logarithm problem. We then study the theoretical implementations of quantum computers and its advantages and disadvantages in real world applications of decryption. We also suggest alternatives to quantum computing and take a look at the prospect for the future of cryptography.

1. Introduction

Cryptography and encryption have been used for secure communication over thousands of years. The earliest signs of humans encrypting a message dates back to the Roman empire, when Julius Caesar shifted each character of his message by 3 positions down the alphabet in his private correspondence. As the demand for encryption grew from military civilian, the advent of computers have rendered classical substitution ciphers, an example of the earlier, obsolete and vulnerable. The tremendous need for information security (or otherwise known as infosec) arose by the Internet has resulted in the development of more complex encryption algorithm, as the value of digital information skyrockets and is now an integral part of our lives.

Modern day cryptography has evolved from rudimentary conversions to complex mathematical problems. Today there are three common types of cryptography in use: the symmetric key cryptography, public key cryptography and cryptographic hash functions. While symmetric key cryptography can be very secure and fast, a major disadvantage is that all parties involved have to obtain a copy of the same secret key used for both

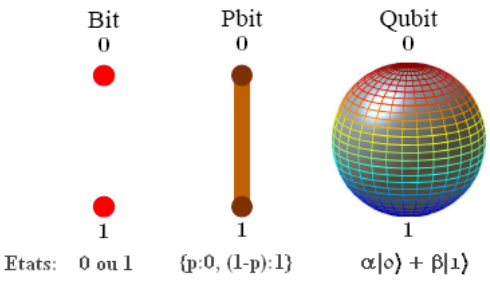
encryption and decryption. Hash functions, on the other hand, are irreversible and is mostly used for authentication purposes. Public key cryptography, the primary focus of this paper, is the "most significant new development in cryptography in the last 300-400 years" [1], and it involves a two-key system whereby "two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key". [1] The effectiveness of public key cryptography is made possible by so-called *one-way functions*, where outputs of such functions are easy but computing the inverse of such functions without knowing their original inputs is very difficult. Traditionally, it would take an unrealistic time for classical computers to compute answers to a public key algorithm, approaching billions of years of computation time.

With its theoretically unparalleled computational capability, quantum computers are said to be the end to most commercial available public key encryption algorithms in use today, including the RSA. The quantum-mechanics properties of qubits used in quantum computers allow it to run computations and simulations simultaneously, leveling its computational speed to be several orders of magnitude faster than traditional transistor processors [2]. While QC is at its early infancy, some scientists fear that a fully developed quantum computer system would bring chaos to the world order, specifically breaking every encryption system known in world's financial systems.

2. Quantum Computing

With statistical trends of Moore's law approaching its limits, scientists have been looking at venues to evolve traditional computers since the dawn of the century. Initially coined by Intel's co-founder Gordon Moore, Moore's law states that the overall processing power of computers will double every two years. However, the capabilities of traditional transistor based computers have seemed to hit a bottleneck, as price per transistor stopped falling and processing speeds are increasing at a slower rate. This phenomena prompted the research and development of a completely new form of computing that is based on the volatile properties of the atomic molecules surround us. Quantum computing studies theoretical computation systems which use quantum-mechanical phenomena (e.g., superposition, entanglement) to perform data operations. [3] Because of its tremendous speed in theory, quantum computing could be used to solve some of the unsolved optimization problems we have today (i.e. travelling salesman problem).

2.1 Qubits and Simultaneous Calculations

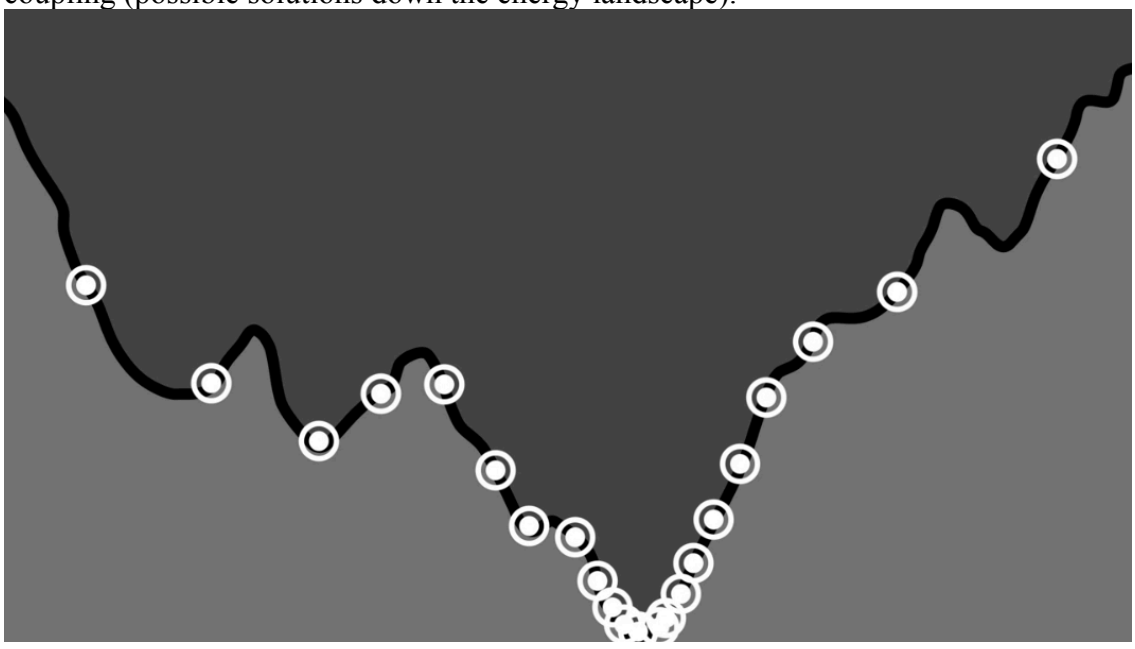


While the average computer's memory is made up of bits, a quantum computer's memory is made up of qubits. A regular computer saves information in binary form using zeroes and ones, which are called bits. These strings of numbers, which are comprised of 0s and 1s, create codes that instruct the computer on how

to proceed. However, a qubit in a quantum computer is a particle (e.g., atom, electron, photon) which is manipulated to store information, and in its normal state, it is in a superposition state of 0 and 1. It represent a two-state quantum-mechanical system, such as the polarization of a single photon, which can be vertical and horizontal polarization. The polarization and two-state property of qubits are achieved by magnetic fields that flow in the opposite direction. A quantum particle, say, a qubit, manipulated in its quantum properties like its spin or polarization can therefore have multiple properties. And because of the flexibility and variation of qubits, more information can be stored on a quantum computer. Most importantly, information can be processed at an exponentially faster rate. For example, a problem that would take a conventional computer several minutes to solve due it its complexity, could be solved in less than a second by a quantum computer. This is because today's conventional computers must go through each problem one step at a time, where a quantum computer has the ability to solve multiple problems instantaneously.

2.2 Quantum Annealing

Quantum Annealing is the way of using the intrinsic effects of quantum physics to solve optimization problems and probabilistic sampling. While optimization problems play a big role in artificial intelligence and machine learning, it is also crucial to optimizing our ever-evolving complex cryptographic algorithms and testing them with improving test cases so that they are up to date. From the physics perspective, quantum annealing is an adiabatic process of universal quantum computing where the goal is to find the minimum of an energy landscape while satisfying a preset list of biases and coupling (possible solutions down the energy landscape).

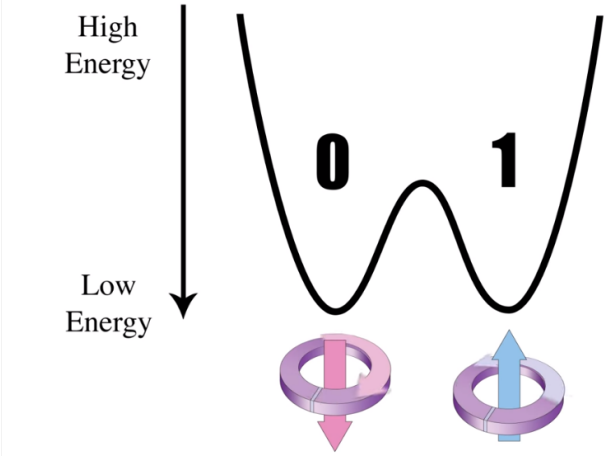


As we can see in the illustration above, there is a global minimum in the energy landscape, which could be controlled by the manipulation of magnetic field applied to the qubits, allowing for a phenomenon called quantum tunneling to take place. Quantum tunneling describes a probabilistic estimate of qubits penetrating through hills of the

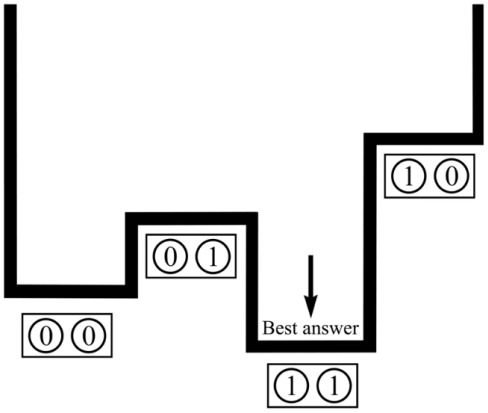
energy landscape through the form of a tunnel, racing up to millions time faster than classical computers in that respect.

2.2 Quantum Entanglement

We know already that a qubit is normally in a superposition of its two states, but how are we able to determine which state it is at a specific time, or even try to manipulate it? The answer is that when a magnetic field is applied to electrons or molecules, due to the difference in charges, the two quantum-mechanic states of a qubit distinguish themselves by their energy levels as illustrated below.



What gives quantum computing its exponential power is that the dominance of the two states in a single qubit could change and when coupled together with other qubits we can easily produce an exponential number of states from the combination. This phenomena is called quantum entanglement. For instance, when two objects are entangled they now have to be considered as a single object which has 4 states, each one corresponding to a different combination of the two qubits, each depending on the coupling applied to the pairs of qubits. Similarly, the number of possible states increases to 8 when we are dealing with three qubits, 16 with four, and so forth. With n qubits, we could theoretically reach 2^n expressions. Given $n = 300$, the number of calculations that could run simultaneously would be greater than the number of atoms in the universe.



However, scientists today are still struggling to maintain the behavior of a large number of coupled qubits because of how volatile atomic particles like electrons are to its surrounding energy and magnetic fields, aka. noise and other quantum decoherence. Another very peculiar aspect of quantum entanglement and what makes its particular useful in other domains is that while the states of a pair of entangled qubits are constantly fluctuating, when we examine the states of both at the same time, regardless of the distance between them, one would always turn out to positive and the other would be negative. A qubit could be on Earth and the other could be on the moon and the states could be still influencing each other because of the entanglement. The applications of such a substantial discovery have been used significantly in the field of quantum teleportation where Austrian Physicist was able to teleport atomic particles between two islands that are 144km apart.

3. Public-key Encryption

3.1 The Integer Factorization Problem

The unbalance in complexity between multiplication and factorization is the base problem of which many popular public key cryptosystems are built upon today [7]. A classical example of such a problem is the factorization of two primes from an integer. Given a sufficient large number (on the order of 40), retrieving it from the multiplication of its prime factors would take a minute while factorizing it into its two factors is simply computationally intractable. Further complications and variations have been added to include the product of partial primes and randomly generated factors (as improved from the original Diffie-Hellman implementation) so that with classical computers it can take over millions of years to crack. In the study of algorithms, such a problem is said to be both NP and co-NP, a.k.a. a Union between the two ($NP \cup coNP$):

- It is in NP, because a factor $p < k$ such that $p \mid n$ serves as a witness of a yes instance [8].
- It is in co-NP because a prime factorization of n with no factors $< k$ serves as a witness of a no instance. Prime factorizations are unique, and can be verified in polynomial time because testing for primality is in P [8].

3.2 RSA

RSA encryption, named for the surnames of the creators Ronald Rivest, Adi Shamir and Leonard Adleman, relies on the Integer Factorization Problem. The entire protocol is built from two large prime numbers. These prime numbers are manipulated to give a public key and private key. Once these keys are generated they can be used many times. Typically one keeps the private key and publishes the public key. Anyone can then encrypt a message using the public key and sent it to the creator of the keys. This person then uses the private key to decrypt the message. Only the one possessing the private key can decrypt the message. One of the special numbers generated and used in RSA encryption is the modulus, which is the product of the two large primes. In order to break

this system, one must compute the prime factorization of the modulus, which results in the two primes. The strength of RSA encryption depends on the difficultly to produce this prime factorization. Today, RSA Encryption is the most widely used asymmetric key encryption system used for electronic commerce protocols.

3.4 Shor's Algorithm

Peter Shor, mathematician at Massachusetts Institute of Technology, came up with a quantum algorithm that solves the integer factorization problem N on a quantum computer in polynomial time. Specifically, if there are n bits, the algorithm would be able to find its prime factors in $O(N^3)$ time. Using photonic qubits, multi-qubit entanglement was observed running Shor's algorithm and the factorization of 21 was achieved. [10]

4. Post Quantum Cryptography

To find the prime factors of a 2048 bit number it would take a classical computer millions of years, a quantum computer could do it in just minutes. [5] Scientists have
A hash-based public-key signature system (MD5, SHA256):
A multivariate-quadratic public-key signature system:

[9]

Cryptosystem	Broken by Quantum Algorithms?
RSA public key encryption	True
Diffie-Hellman key exchange	True
Elliptic curve cryptography	True
Bunchmann-Williams key-exchange	True
Algebraically Homomorphic	True
McEliece public key encryption	*False*
NTRU public key encryption	*False*
Lattice-based public key encryption	*False*

4.1 Implications to Information Security

Many elite government intelligence agencies have been trying to develop a quantum computer or pioneer the quantum cryptography field because, by harnessing the power of quantum computing, they could be invincible against many of the most secure cryptosystems used by foreign nations and military organizations. The prevalence of public key cryptography in use today means in a political stand point that nations who are able to crack the problem first would have an advantage over the world, just like the British in WWII, cracking of the German Enigma machine has led to an ultimate victory for the Allies. China emerges as one of the quantum powers as of late thanks to its dedicated efforts in quantum cryptography. What that means is data today should be encrypted taken into account of post quantum cryptography, rendering it futureproof. As increasing amounts of sensitive information is digitize and stored online, the old sayings prevails – the winner of cryptography is the winner of the war.

References

1. G. Kessler, **An Overview of Cryptography**, Gary Kessler Associates, 2015

2. L. Hardesty, **Scott Aaronson on Google's new quantum-computing paper**, Phys.org, 2015

3. Law Offices of S. Atrizadeh, "What is Quantum Computing?", Internet Lawyer Blog, 2015

4. N. McDonald, "Past, Present, and Future Methods of Cryptography and Data Encryption", *Department of Electrical and Computer Engineering, University of Utah*, 2015

5. Veritasium, **How To Make a Quantum Bit**, YouTube – Veritasium, 2013

6. D. Walliman, **How The Quantum Annealing Process Works**, YouTube – D-Wave Systems, 2015

7. P. Shor, **Quantum Algorithms**, *Lecture, MIT, NASA QFTC,* 2013

8. A. Roth, "Is integer factorization an NP-complete problem?", Theoretical Computer Science, 2010

9. D. Bernstein, **Post-Quantum Cryptography**, Springer, print. 2009

Appendix I – Effectiveness of Quantum Annealing vs. Classical Annealing Today