Quantum Key Distribution: The Application of Quantum Mechanical Principles to Cryptographical Systems

Alex Koen
English 12 TP
Handsworth Secondary School

May 28, 2019

Quantum Key Distribution: The Application of Quantum Mechanical Principles to Cryptographical Systems

Cryptography is omnipresent. Ever since the time of the Egyptians, societies and individuals have sought to protect their information by obscuring it behind a layer of code—altering it in such a way that only they, and those that they trust, can decipher it. Today, with the advent of modern computing technology, algorithms are readily available that can encrypt information so securely that the strongest supercomputers would require billions of years to decipher them. A new branch of computing—quantum computing, however, threatens to render obsolete nearly every known cryptosystem, and consequently cryptographers are researching new technologies to encrypt information in a way that is completely invulnerable. In the future, quantum mechanical principles will play a vital role in the development of cryptographical systems because of the insecurity of conventional systems against quantum computers, and because of the potential for quantum cryptosystems to be completely secure against any attack. The purpose of this paper is to examine the necessity and application of quantum cryptography, specifically quantum key distribution, in a manner that is clear and understandable by a formative audience.

Despite the fact that cryptographical security is a growing concern, provably unbreakable codes have existed for more than a century. During World War II, a cryptosystem known as the "one-time-pad" was used by German and Soviet forces for diplomatic communications (Hughes et al., 1995, p. 7). Such a system comprises of a secret key which is equal to the length of the message or data to be transmitted. This was proven in 1949 by Shannon to be truly random, as any potential eavesdropper would have an equal chance of decrypting any random sequence of characters with no way of knowing which one is correct, assuming that the one-time-pad is genuinely random and used only once (Hughes et al., 1995, p. 6). Below, Hughes et al. (1995) explains the methodology behind the one-time-pad cipher using the fictional characters 'Alice' and 'Bob':

> In this system, if Alice has a plaintext message, P, composed of a character sequence $\{p_1, \ldots, p_n\}$ (the ps will be bits, digits or letters) she uses her key, $K = \{K_1, \ldots, k_n\}$

> to produce the cryptogram $C = \{c_1, \ldots, c_n\}$, where
>
> $$c_i = p_i + k_i \ (mod\ N)$$
>
> using modular arithmetic in the base, N, of the message characters ($N = 2$ for bits, 10 for digits, and 26 for letters, which can be given a numerical value in the range 0 - 25 corresponding to their order in the alphabet).
>
> When Bob receives the cryptogram, C, he subtracts his key from it, again using modular arithmetic, to recover the plaintext, P (p. 6)

Although the resulting ciphertext is unbreakable, the flaw in this system lies in the key itself. Before a message can be sent, the secret key must be agreed upon by both parties, which entails the establishment of a secure channel between the two. This is not always possible. Either the key must be physically transported by a courier, or the key itself must be encrypted, which requires another key. Furthermore, if two different plaintexts are encrypted using the same secret key, any eavesdropper main gain more information about that key, assuming they know that is has been reused (Rosulek, 2019). According to Hughes et al. (1995), "demands placed on Soviet diplomatic communications at the start of WWII were so great that one-time-pads were reused, allowing cryptanalysts to unmask the Rosenberg spy ring and atom-spy Klaus Fuchs" (p. 8). Today, given the intrinsic challenges of physical key transportation, private key encryption has lost popularity compared to more practical public key cryptosystems.

In modern day cryptography, public, or *assymetic* encryption, is usually favoured over private, *symmetric*, one-time-pad keys despite its inherently inferior security. In asymmetric encryption, each entity has both a public key e and a private key d—typically large prime numbers that are easily to multiply but whose sum is nearly impossible to factor (Menezes, Van Oorschot, & Vanstone, 1996, p. 283). If anyone wishes to send an encrypted message to entity A, they must obtain a copy of As public key and encrypt it accordingly. A may then decrypt the ciphertext using his own private key d. Menezes et al. (1996) provide a helpful analogue as follows:

> Consider a metal box with the lid secured by a combination lock. The combination is known only to Bob. If the lock is left open and made publicly available then anyone can place a message inside and lock the lid. Only Bob can retrieve the message. Even the entity which placed the message into the box is unable to retrieve it. (p. 26)

Any public-key encryption algorithm depends on the existence of *trapdoor one-way functions*, in which knowledge of the public key e does not allow one to determine the respective entity's private key d (Menezes et al., 1996, p. 26). Asymmetric algorithms, which are more computationally intensive than their symmetric counterparts, are typically used to facilitate the transmission of a private key, which can then be used to establish a traditional private key channel of secure information (Menezes et al., 1996, p. 283). While these cryptosystems are vulnerable to a brute-force attack, in which an attacker tries every possible combination with the hope of guessing the correct one, they are secure in practice because such an attack is computationally infeasible with current hardware. According to John Nash, a mathematician who earned the Nobel Prize in 1994 for his work in game theory, "the most direct computation procedure would be for the enemy to try all $2^{\lambda/2}$ possible keys, one by one. Obviously this is easily made impractical for the enemy by simply choosing λ large enough" (Rosulek, 2019, p. 59). For example, a readily available 256-bit key ($2^{256/2}$) would take over a million times the age of the universe to crack using the fastest supercomputer readily available on the planet today. However, computing power is constantly increasing, and these incredibly secure cryptosystems may soon be solvable in a matter of days using the power of quantum computers.

In the near future, quantum computers may be able to solve these asymmetric cryptographic algorithms exponentially faster than what is possible with conventional computers. A quantum computer with around 2,300 logical qubits would likely be able to solve any of the above ciphers in less than a day using Shor's algorithm, a known method of integer factorization which runs in exponential time rather than sub-exponential time (National Academies of Sciences, Engineering, and Medicine, 2019, p. 97). According to the National Academies of Sciences, Engineering, and Medicine (2019), such a system "could break all key exchange methods currently used in practice.

Specifically, key exchange protocols based on variants of the Diffie-Hellman and the RSA protcols would be insecure" (p. 97). It is evident that measures must be taken to counteract this global security threat, as even though advances in computing technology are necessary for scientific progress, secure encryption is vital to many aspects of modern society, from text messaging to international banking. As such, the National Institute of Technology (NIST) has recently begun the process of replacing standard asymmetric cryptosystems with those that are quantum secure (National Academies of Sciences, Engineering, and Medicine, 2019, p. 97), and quantum mechanics itself may play a vital role in shaping the ciphers of the future.

In the future, quantum computers will be used to send encoded messages that are resistant against attacks from any computer—resistant because of the fundamental laws of quantum physics, specifically Heisenberg's Uncertainty Principle and the quantum no-cloning theorem. According to Tan (2013, pp. 118–119), Heisenberg's Uncertainty principle states that "attempting to measure an elementary particle's position to the highest degree of accuracy, for example, leads to an increasing uncertainty in being able to measure the particle's momentum to an equally high degree of accuracy" (p. 118). This means that a particle has neither a position nor a velocity until it is measured, and that any attempt to measure either of its properties will cause a detectable disturbance to the particles themselves. A helpful analogy can be drawn as follows: consider a lake on a windy day. The frequency of the waves on its surface can be determined easily. If three waves pass by in one second, then their frequency is 3 Hz. However, one cannot determine the position of the wave—it covers the entire lake. In contrast, if a rock is thrown into the same lake, its position can be determined easily but its frequency cannot. Since all elementary particles behave like waves, both the position and velocity of a particle cannot be determined to an arbitrary precision (Griffiths, 2005). This is given by the formula

$$\sigma x \sigma p \geq \frac{\hbar}{2}$$

where σx is the standard deviation of the particle's position, σp is the standard deviation of the particle's momentum, and $\hbar$ is the reduced Plank's constant (Griffiths, 2005). Similarly, the quantum no-cloning principle states that an arbitrary quantum state cannot be duplicated perfectly

(Tan, 2013, p. 117). This means that it is impossible for an attacker to make an unlimited amount of copies of the quantum key and test each dynamical variable to an arbitrary precision.

Quantum cryptography makes use of these principles to protect the transmission of a series of quantum bits. A classical bit—like one would find in modern computer hardware—stores a binary value, either a 1 or a 0 (Mjolsnes, Hjelme, Lydersen, & Makarov, 2011, p. 76). A quantum bit, however, can represent a 1 or a 0, or it can represent a combination of the two in a state know as superposition (National Academies of Sciences, Engineering, and Medicine, 2019, p. 2). According to Mjolsnes et al. (2011, pp. 76–77), the classical bit can be thought of as a box in which either a red or a blue ball can be placed. When the box is opened again, the ball will always be the same colour as when it was placed in the box. On the other hand, the box in which the figurative quantum bit is placed has two doors. To read the quantum bit information accurately, the correct door must be opened. If the other door is opened, the information stored in the qubit will change to a random bit value. This is illustrated by the following diagram:

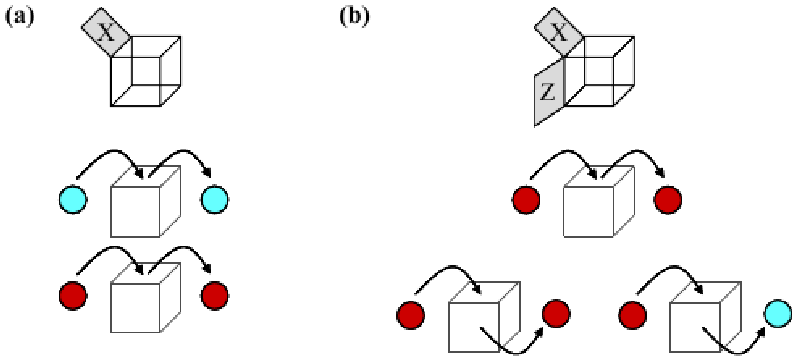

Figure 1. Classical versus quantum bit. (a) Classical bit: the colour of the ball is always the same as when it is put in. (b) Quantum bit: The ball is the same colour as it was when it is put in only when the correct door is used. If the incorrect door is used, the colour is random. Reprinted from *A mutlidisciplinary introduction to information security* (p.73), by Mjolsnes, S.F., Hjelme, D. R., Lydersen, L. & Makarov, V., 2011, New York, NY: Chapman and Hall/CRC. Copyright 2011 by the Norwegian University of Science and Technology.

Scientifically, the superposition of a qubit is represented as the probability of the specific qubit resolving to either a 1 or a 0, with the sum of both probabilities adding to one hundred percent (National Academies of Sciences, Engineering, and Medicine, 2019, p. 35). Furthermore, the information about the qubit's superposition is destroyed upon measurement, during which the wave-function collapses into a single state (National Academies of Sciences, Engineering, and Medicine, 2019, p. 35). The most popular form of quantum cryptography, quantum key distribution, applies this principle to a manifestation of the quantum bit, the polarized photon, to make the secure transmission of a "one-time-pad" symmetrical key possible without risk of interception (Mjolsnes et al., 2011, pp. 3, 5).

Named after the year in which it was first proposed, the BB84 protocol is the most popular form of quantum key distribution and the one that holds the most promise for the future (Mjolsnes et al., 2011, p. 4). In the book *A Multidisciplinary Introduction to Information Security*, Mjolsnes et al. (2011, pp. 5–6) explains the protocol in detail, which uses a stream of polarized single photons to transmit a secure key. In this protocol, the sender, entity A, polarizes the photons randomly using either horizontal (bit value 0) and vertical (bit value 1) polarization, or −45° (bit value 0) and 45° (bit value 1) polarization. These two options are synonymous with the two doors of the figurative quantum box described above. To receive the qubits, entity B uses two polarizing beamsplitters at random, one to distinguish between the horizontal and vertical polarizations, and one to distinguish between the −45° and 45° polarizations. If entity B chooses the beamsplitter that is compatible with entity A's polarization choice, then entity B will read the value correctly. However, if entity B chooses the beamsplitter that is incompatible with entity A's polarization choice, then it will read a random value. After enough photons are transmitted, entity B will announce which beamsplitters it used for each photon—while keeping the results of it's measurements a secret—and entity A will have it discard each measurement where it used the wrong beamsplitter. Since entity B will, on average, only use the correct beamsplitter half the time, they will be left with a key roughly half the length of the number of photons that were transmitted. This allows both entities to agree on a specific one-time-pad key, but more importantly, it is resistant to eavesdropping. If a third entity C intercepts the transmission, it's random choice of beamsplitters will be different than that of entity *B* and so it has no way of confirming whether or not it's measured values are accurate. Furthermore, if entity *C* tries to read part of the transmission, it will invariably modify the polarizations of half of the photons. When entities *A* and *B* then compare a random subset of their key over a public channel, they will notice a discrepancy and repeat the process until their keys match. If the random subset of their key does match, however, then they know that it has not been intercepted and they can begin to encrypt information using it. While there are many more variables to account for in practice, this is the basis behind modern quantum cryptography, and the technology is on the verge of becoming a commercially viable option for secure communication.

Although this technology is still under development, progress is being made towards the use of quantum cryptography as a readily-available alternative to current cryptosystems. A recent analysis by researchers at the Naval Surface Warfare Center's Dahlgren Division shows the public-facing research output of several of the countries most heavily invested in the technology, shown in Figure 2 below. In 2018, the European Commission announced plans for a €1 billion, 10-year research project on quantum technology centering around four major areas: quantum communication, computation, simulation, and sensing and metrology (National Academies of Sciences, Engineering, and Medicine, 2019, p. 158). While Europe is pursuing this technology, it is the United States and China, however, who are doing the most research. Recently, Chinese researchers established the first intercity quantum key distribution channel between Beijing and Shanghai (National Academies of Sciences, Engineering, and Medicine, 2019, p. 229), and QKD was recently deployed internationally with the first ever quantum-encrypted video teleconference using satellites and ground connections across a distance of 7600 km (Liao et al., 2018, "Abstract," para. 1). It is evident that many of the world's nations are concerned by the possible repercussions of quantum computing, and are putting resources towards the development of these quantum cryptographical technologies to protect themselves and their information.

In conclusion, the need for quantum cryptography is illustrated both by the weakness of traditional cryptosystems against quantum attacks, and by the evidence that quantum ciphers are

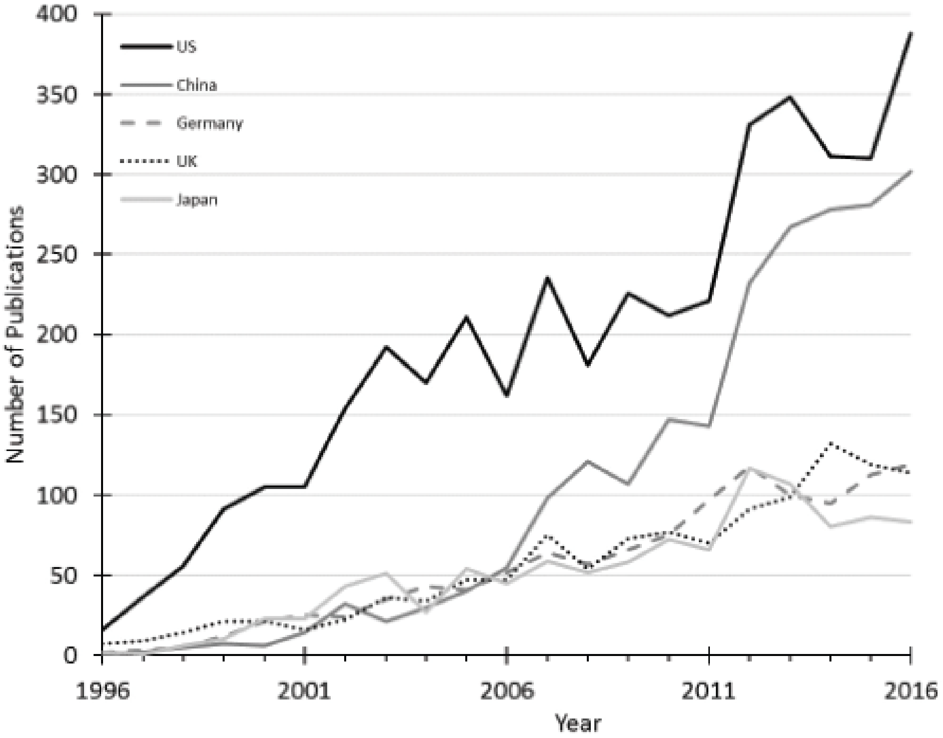

Figure 2. Number of papers published by nation of origin for top five global producers in quantum computing and algorithms. Includes only research pulications that are accessible to the public. Data are the result of a bibliometric analysis conducted by a team at the Naval Surface Warfare Center Dahlgren Devision. Reprinted from *Quantum computing: Progress and prospects* (p. 227), by the National Academies of Sciences, Engineering, and Medecine, 2019, Washington, DC: The National Academies Press. Copyright 2019 by the National Academy of Sciences.

physically impossible to decrypt. As quantum computing technology improves, ciphers such as the RSA and Diffie-Hellman algorithms which are virtually impossible to solve with conventional computers may soon be solvable by quantum computers and Shor's algorithm in less than a day. Faced with this challenge, countries around the world have seen the need to develop ciphers which are resistant against even these attacks, and currently, quantum key distribution has proven to be the most practical. Richard Feynman once famously stated that, "I think I can safely say that nobody understands quantum mechnics" (Feynman, 1964). The world of the very small may never be fully understandable by the human mind, but science has now reached the point where even the incomprehensible can be used to improve the safety and security of those who depend of the privacy of their information. The ambition of civilization will always be to uncover the mysteries of the universe, but some things are best left a secret.

References

Feynman, R. P. (1964). *Probability and Uncertainty: The Quantum-Mechanical View of Nature* [video file]. Retrieved from https://archive.org/details/probabilityanduncertaintythequantummechanicalviewofnature

Griffiths, D. J. (2005). *Introduction to quantum mechanics* (2nd ed.). Upper Saddle River, NJ: Pearson Education.

Hughes, R. J., Alde, D. M., Dyer, P., Luther, G. G., Morgan, G. L., & Schauer, M. (1995). Quantum cryptography. *Contemporary Physics*, *36*(3).

Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., . . . Liu, W.-Y., et al. (2018). Satellite-relayed intercontinental quantum network. *Physical review letters*, *120*(3).

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handsbook of applied cryptography*. Boca Raton, FL: CRC Press.

Mjolsnes, S. F., Hjelme, D. R., Lydersen, L., & Makarov, V. (2011). *A multidisciplinary introduction to information security*. New York, NY: Chapman and Hall/CRC.

National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum computing: Progress and prospects* (E. Grumbling & M. Horowitz, Eds.). Washington, DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

Rosulek, M. (2019). *The joy of cryptography*. Corvallis, OR: Oregon State University.

Tan, X. (2013). *Theory and practice of cryptography and network security protocols and technologies*. London, England: IntechOpen.