Quantum Security in Cryptography

Harpreet Kaur Wadhwa
Assistant Professor, Department of Applied Sciences (Mathematics)
GGN Khalsa College, Civil lines Ludhiana, Punjab (India)

Abstract- Cryptography is literally the art of "secret writing". It is used to secure communication by protecting the confidentiality and integrity of messages and sensitive data. Without it, anyone could read a message or forge a private conversation. Messages are made secret by transforming them from "plaintext" into "ciphertext" using a cipher and performing the process of encryption. Decryption turns scrambled and unreadable ciphertext back into plaintext. When cryptographers talk about a "key", they are referring to a shared secret that controls the ability to hide and un-hide information.

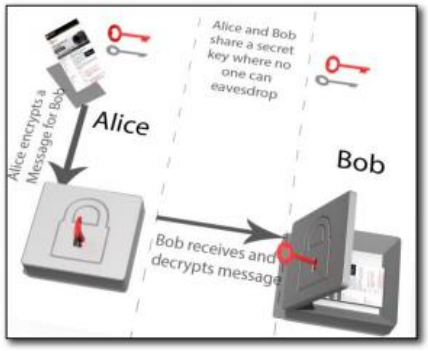
I. INTRODUCTION

There are two types of cryptography that are often referred to as "symmetric key" and "public key" cryptography:

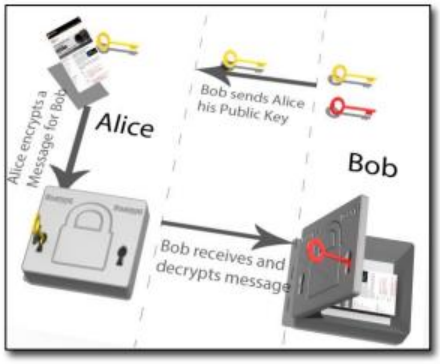
1. In symmetric key cryptography, the same key is used for both encryption and decryption, and that key needs to be kept a secret by everyone who is sending and receiving private messages. The major difficulty of symmetric key cryptography is to provide the secret keys to legitimate parties without divulging the keys to eavesdroppers.
2. Public key cryptography1 is more involved and complex. There are two keys, one for encrypting and another key for decrypting. The two keys are mathematically related, and only one key is intended to be kept a secret. Public key cryptography allows anyone to send an encrypted message, but only one person, with the private key, can decrypt the message. Public key cryptography can also be used for digital signatures where someone with a private key can sign a message that anyone can verify with the public key.

Cryptography is necessary but not sufficient for secure transmission of information. In practice, information is secured using cryptography within the context of security protocols which handle message formatting, key management and a plethora of other considerations that are used to broaden the primitive concept of secret message passing to the more practical art of modern secure communications.

While cryptography is not the entirety of security, it is an essential part. If the cryptography fails, all of the secret messages that are sent over public channels become readable to anyone who can passively observe. Cryptography is important because without it, everyone could read anything they intercept, regardless of whether it was intended for them. Cryptography keeps sensitive data a secret (confidentiality), it is used to protect against changes to data over an unreliable public channel (data integrity), and it can ensure that communicating parties are indeed who they claim to be (authentication).



A - Symmetric Key Cryptography



B - Public Key Cryptography

Fig.1: Cryptography Basics - Encryption and Decryption

II. QUANTUM COMPUTING

Today's computers are governed by the laws of classical physics and Moore's law2 which states that, historically speaking, computers double their speed and capacity every 18 months because chip makers are able to squeeze twice as many transistors onto a computer chip. In order for these computing improvements to continue, placing more transistors on a computer chip means that transistors need to get smaller. But physics presents a natural barrier in that once technology has shrunk a transistor to the size of a single atom there are no more improvements to be made to transistor size. But what if the transistor could be replaced with a better technology, a

technology that allows for a new paradigm of computing? The laws of physics that can be seen, observed, and understood through experiences in everyday life are referred to as classical physics, and these laws govern the workings and computational capabilities of computers as they are known today.

However, everything that is described by classical physics at a macroscopic level can be described by quantum physics at a nanoscopic level, and these different physical laws are known as quantum mechanics. In the past few decades, researchers have realized that the ways in which the laws of physics allow different things to happen to very small objects can be harnessed to make computers out of novel materials, with hardware that looks and behaves very differently from the typical classical computers that people use in their homes and offices today. Quantum computers, obeying the laws of quantum mechanics, can calculate things in ways that are unimaginable from the perspective of people's regular day-to-day experiences.

In classical computing, information is stored in fundamental units called bits, where a bit can hold a binary digit with the value of 0 or 1. In quantum computing, the fundamental unit can hold both a 0 and a 1 value at the same time; this is known as a superposition of two states. These quantum bits are known as qubits and measuring the state of a qubit causes it to select or "collapse into", being a 0 or a 1. Interestingly, if you prepare a string of qubits of the same length in the same way, the resulting bit string will not always be the same. This gives quantum computers an advantage over classical computers in that they can perform very rapid parallel computations.

III. QUANTUM COMPUTING IMPACT ON CRYPTOGRAPHY AND SECURITY

Cryptography plays a very important role in most secure electronic communication systems today because it ensures that only authentic parties can read each other's exchanged messages. Quantum computing threatens the basic goal of secure, authentic communication because in being able to do certain kinds of computations that conventional computers cannot, cryptographic keys can be broken quickly by a quantum computer and this allows an eavesdropper to listen into private communications and pretend to be someone whom they are not.

Quantum computers accomplish this by quickly reverse calculating or guessing secret cryptographic keys, a task that is considered very hard and improbable for a conventional computer. A quantum computer cannot break all types of cryptographic keys and some cryptographic algorithms in use today are also safe to use in a world of widespread quantum computing. The following sections will describe which types of cryptography are safe from quantum attacks and which ciphers, protocols and security systems are most vulnerable.

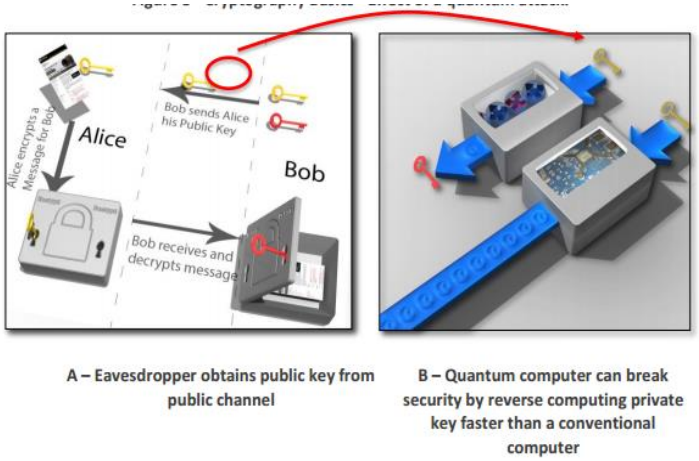


Fig.2 Cryptography Basics - Effect of a quantum attack.

IV. QUANTUM SAFETY AN IMPORTANT ISSUE

Information in many ways equates to geopolitical, social, and economic power. The economic, social, and political well-being of developed countries depends on integrity, confidentiality, and authenticity of sensitive data sent over networks. Corporations and governments have legal responsibilities to their investors, constituents, and customers to preserve the confidentiality of sensitive information. Whether this information consists of military communications, secret government documents, industrial trade secrets, or financial and medical records, interception of information allows adversaries to not only learn about the contents of these communications, but also to discover metadata in patterns within a network of communicators, to extract general patterns using machine learning, and even to insert false or misleading information or malware into a data stream. Previously, communications and transactions were considered secure when encrypted using an unbroken cryptosystem as part of an otherwise rigorous information security framework. Quantum computing challenges this assumption, because it offers a new and powerful set of tools under which many of these cryptosystems may collapse. Many ciphersuites have already been demonstrated to be insecure in the presence of a quantum computer, including some of our most pervasive cryptosystems such as RSA and Elliptic Curve Cryptography. Any data that has been encrypted using many cryptosystems whose security was based on the computational intractability of the so-called "hard problems" of discrete log and integer factorization is under threat of both eavesdropping and attack by future adversaries in possession of quantum computers. Without quantum-safe encryption, everything transmitted over an observable network is vulnerable to such an adversary. These issues do not only impact data that may be encrypted in this manner in the future, but apply to the information that is currently stored in this manner, or has been transmitted over an observable channel in the past. Choosing to ignore quantum-safe cryptography and security before quantum

computers are able to perform these functions leaves almost all of present and future data vulnerable to adversarial attack. It is essential for industries with interest in keeping secret information safe from adversaries to be forward thinking in their approach to information security. This involves considering more than merely how soon a quantum computer may be built. It also means thinking about how long information needs to stay secure, and how long it will take to update the existing IT infrastructure to be quantum-safe. Specifically, it is necessary to consider: x: "how many years we need our encryption to be secure" y: "how many years it will take us to make our IT infrastructure quantum-safe" z: "how many years before a large-scale quantum computer will be built" If a large-scale quantum computer (z) is built before the infrastructure has been re-tooled to be quantum-safe and the required duration of information-security has passed (x+y), then the encrypted information will not be secure, leaving it vulnerable to adversarial attack. In real-world application, the value of x must be carefully considered, specifically: what are the practical consequences of a certain category of information becoming public knowledge after x number of years? For example, would it be a problem if your credit card numbers of today are made available to everyone in the world after x = 5 years? Probably not, because it is very likely that you would have a new credit card issued, having a new expiry date and security code.

On the other hand, if personal identity information is made public after x = 5 years, you may be exposed to identity theft and any resulting consequences. Indeed, one would also need to be cautious about defining the value of x in the case of certain other information categories such as top-secret military information, e.g. the orbits of secret military satellites, location of military bases and their resources and capabilities. Therefore, defining the value of x is a non-trivial matter, and requires a fair amount of thought, risk analysis and modelling.

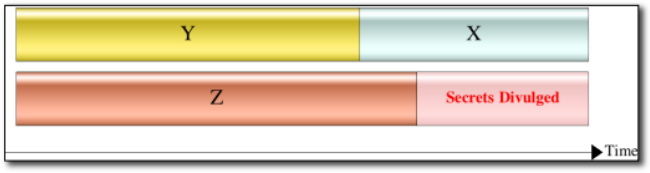


Fig.3 Lead time required for quantum safety

V.WORKING OFQUANTUM KEY DISTRIBUTION

Quantum key distribution is a process that uses an authenticated communication channel together with a quantum communication channel in order to establish a secret key. There are several different protocols for implementing quantum key distribution, all of which require both a quantum channel (to send quantum states of light), and an authenticated classical channel (for the sender, Alice, and the recipient, Bob, to compare certain measurements related to these quantum states and perform certain post-processing steps to distil a correct and secret key). The quantum channel uses optical fibres or free space/ satellite links to send photons (quantum states of light) between Alice and Bob, whereas the classical channel could be a simple (authenticated) telephone line that Alice and Bob use to talk to each other. Interestingly, both of these can be public. It is described that the quantum channel necessarily shows Alice and Bob when an eavesdropper has been listening in, and it is a fact of the QKD protocols that the classical channel could be broadcast publicly without compromising security. Quantum Key Distribution begins by Alice deciding to distribute some cryptographic key to Bob. Both Alice and Bob have the specialized optical equipment necessary for establishing the quantum channel, as well as access to a classical channel where they can communicate with one another. Alice uses a light source to send a stream of photons (quantum states) one-at-a-time. Each photon can be thought of as one bit of information. As each photon is sent, she randomly chooses to prepare it in one of two ‘’bases’’. Basis can be described as a perspective from which a photon is measured.

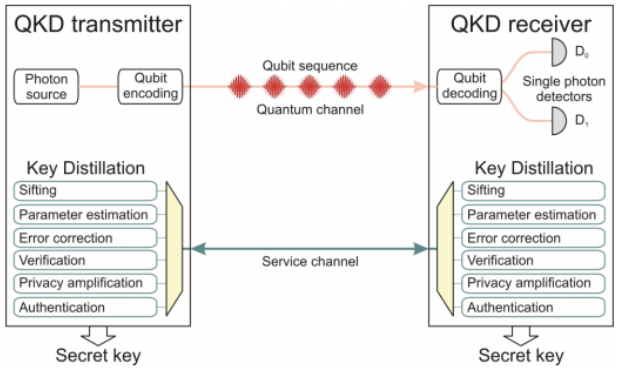


Fig.4 Illustration of a typical prepare-and-measurement QKD setup

As the recipient, Bob needs to record values for each photon he receives via the quantum channel. To do this, he must, like Alice, make a measurement of each one, and he therefore also chooses one of the two possible ‘’bases’’ and records which one he measured in. These choices are random and do not require any information about the bases that Alice chose when she was sending each bit. Afterward, Alice and Bob then communicate over the classical channel to compare which basis each bit was measured in at each end of the quantum channel. Sometimes Alice and Bob will randomly choose the same basis, and these are the bits for which they will get the same value for the photon (which is useful, so they will keep this bit as part of the key). When Alice and Bob measure the photon using different bases, they throw this bit away and do not use it in the final key. After each bit has been sent and received, Alice and Bob can speak publicly about which basis they used to measure each photon, and this can provide enough information for each of them to generate key from the received quantum states, but not enough information for an adversary to reconstruct the key. Thus, an

eavesdropper will not be able to discover the transmitted key for two important reasons. Firstly, the adversary cannot directly observe the photon without changing them, therefore being detected and having these bits discarded by Alice and Bob. Secondly, the adversary cannot indirectly observe the photon through observing the measurements of Alice and Bob, either, since Alice and Bob do not disclose the final measurement result for each quantum state. Rather, they only disclose which basis they used to measure it. By this time, it is too late for the adversary to measure the photon, because it has already been received by Bob, so knowing the basis that Alice used is not useful. It is wellestablished using information theoretic proofs that the measurement information is inadequate for an adversary to use to reconstruct the generated key.

VI. CHALLENGES FOR QUANTUM SAFE SECURITY

Many of the challenges for the adoption of quantum safe security are rooted in common best practices within the security industry. Very early in their careers security practitioners are taught to avoid new cryptographic algorithms that have not received years of public scrutiny, to not design their own security protocols, and rely only on well-established security standards. These security tenants are still sound and very relevant in a world with quantum computing but the industry needs to recognize the amount of lead-time required to make systemic changes to existing security products and infrastructure because of the pragmatic security mind-set. These best security practices that routinely block and protect against bad or questionable security schemes also slow the adoption of changes meant to protect against never-before-seen attacks. Some of the main barriers in security culture that need to be recognized and addressed before quantum safety will be widely adopted:

1. Confidence in Algorithms. There are many well-studied public key based cryptographic algorithmλ options that could be used as a substitute for RSA or ECC, however, many of these substitutes do not have the benefit of wide spread practical use.
2. Rigidity of Security Protocols. Quantum safe ciphers may not fit into an established protocolλ because of historical protocol design assumptions, key size choices and tolerance for message expansion. Earlier sections in this whitepaper give examples of common security protocols that demonstrate the varying degree to which quantum safe cryptography can be used effectively. Many protocols were not designed with cryptographic agility in mind, and may not easily accommodate a change of cipher.
3. Perception of non-urgency. An exact date for the arrival of general purpose quantum computingλ cannot be given, however, global interest is growing and steady progress is being made. As quantum computing matures, computer security weakens. Some businesses require their security to have medium longevity in the sense that confidential information that is worth protecting now, will also remain sensitive and should be kept private a year or two in the future. Other businesses require their security to have greater longevity, keeping information private for decades. Quantum safety is "not urgent" only for those with short term security needs but any business that requires its secrets to remain secret will need to consider their quantum safe transition strategy now. A quantum attack is just as effective at divulging all past communications, i.e. encrypted military information residing on physical storage medium

VII. REFERENCES

[1] L. M. Adleman and M.-D. A. Huang, Primality Testing and Abelian Varieties over Finite Fields, Lecture Notes in Mathematics, Volume 1512, Springer-Verlag, Berlin, 1992.
[2] O. L. Atkin and F. Morain, "Elliptic curves and primality proving", Math. Comp. 61, 29–68 (1993).
[3] E. Bach and J. Shallit, Algorithmic Number Theory, Volume I: Efficient Algorithms, MIT Press, Cambridge, MA, 1996.
[4] M. Blum and S. Goldwasser, "An efficient probabilistic public-key cryptosystem which hides all partial information", Advances in Cryptology — CRYPTO 84, Lecture Notes in Computer Science, Volume 196, Springer-Verlag, Berlin, 1985, 289–299.
[5] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin, 1993.
[6] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", Advances in Cryptology — CRYPTO 98, Lecture Notes in Computer Science, Volume 1462, Springer-Verlag, Berlin, 1998, 13–25.
[7] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. Info. Theory 22, 644–654 (1976).
[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. Info. Theory 31, 469– 472 (1985).

Harpreet Kaur Wadhwa did her B.Sc from Government college for Women, Ludhiana and M.Sc (Mathematics) from SCD Government college, Ludhiana and currently working as Assistant Professor in Applied Science Department in GGN Khalsa College, Civil lines Ludhiana