International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

Quantum computing

Shital, Tanaya, Bhumika, Rani

Date of Submission: 11-03-2024 Date of Acceptance: 21-03-2024

ABSTRACT
Quantum Computing is a technology, which promises to overcome the drawbacks of conventional CMOS technology for high density and high performance applications. Its potential to revolutionize today's computing world is attracting more and more researchers towards this field. However, due to the involvement of quantum properties, many beginners find it difficult to follow the field. Therefore, in this research note an effort has been made to introduce the various aspects of quantum computing to researchers, quantum engineers and scientists. The historical background and basic concepts necessary to understand quantum computation and information processing have been introduced in a lucid manner. Various physical implementations and potential application areas of quantum computation have also been discussed in this paper. Recent developments in each realization, in the context of the DiVincenzo criteria, including ion traps based quantum computing, superconducting quantum computing, nuclear magnetic resonance (NMR) quantum computing, spintronics and semiconductor based quantum computing have been discussed.

INTRODUCTION

I. Today's computational processors decode information into binary bits 0's and 1's and logic gates based on switching transistors are used to process them. These computers work on sequential principles where processes are carried out in a sequential manner until results are arrived. Currently, computing is governed by the rules of classical physics till the size of semiconductor transistors approaches the dimensions of atom. In 1975 Gordon Moore predicted that transistors in integrated circuits will double after every eighteen month [1]. It is believed within the next 10 years, the clock frequency of current computer processor systems may reach about 40 GHz. It is expected that by 2024, it would be hard for the Moore's law to endure further as size of conventional classical bits approaches dimension of atom [2]. Under such conditions

II. material particles are no longer described by classical physics, and a new model of the computer may be necessary by that time. Subsequently, it is important to accomplish the computing at atomic size that follows non-traditional physics called quantum mechanics. In dealing with the problems presented, the quantum computer is one proposal that may have merit. Quantum computing is attracting more and more interest of industrial sectors, not only broad-interest corporations like Microsoft or Google, but also companies more traditionally linked to the area of nanoelectronics and nanotechnology (e.g., IBM and Intel). The arena of quantum computing was accepted in 1980s. In 1999, first quantum computer was developed out of superconductors by D-Wave Systems a Canadian organization. In 2007, 28-qubit quantum computer was illustrated, trailed by 128 qubits in 2010, 512 qubits in 2013and 2000 qubits in 2018. As far as quantum computing research and implementation is concerned, at present we have just a couple of quantum computer gadgets in a lab domain. The requirement for quantum computers to recreate quantum physics effectively, was first predicted by Richard Feynman [3]. A quantum computer does the calculations dependent on the quantum mechanics.

III. Quantum computers aren't constrained to two states; they encode data as quantum bits, or qubits, where bits can be 0 or 1 or both 0 and 1 at the same time in what is called superposition. Moving down to the atomic level quantum computers can be physically realized by atoms, photons, ions or electrons and their corresponding control devices that are working collectively to act as computer processor and memory. At the degree of fundamental research exploration facilities numerous other physical realizations of qubits have been proposed and examined. Recently, solid-state implementations have won overwhelming interest owing to their capacity for scaling to large numbers of qubits. Josephson junctions in superconductors and spin qubits in silicon fall into the course of solid-state qubits. The similarity of silicon qubits with CMOS foundries is an

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

extraordinary resource. Quantum computers utilizing the property of superposition can process and store multiple states simultaneously, thus ensuring it's potential to be millions of times extra dominant than today's most brand influential supercomputers. Moreover, quantum computers guarantee secure transmission, ultrahigh speed and ability to store large amount of information than its classical counterparts

QUANTUM COMPUTING SYSTEMS

Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems. The study of quantum computing is a subfield of quantum information science. Fundamentally computing systems rely on the ability to store and manipulate information. Bits are manipulated individually by current computers. Quantum computers make use of a quantum-mechanical phenomenon (e.g., superposition and entanglement) that allows data to be represented as quantum bits (qubits) - these are not constrained to conventional 0 or 1 binary values, but instead can be a superposition of zero and one simultaneously. Hence, a set of qubits can represent exponentially more values than their classical-bit counterparts. This makes quantum computing a promising platform which could potentially solve computational problems unmanageable for even the most advanced conventional supercomputer. In this section, the discussions will be presented about the fundamentals of quantum computing, various qubit representations, and quantum properties leveraged by qubits and how they are used to compute.

1.1 BIT VS QUBIT

In this section we are introducing the properties of qubits, comparing and contrasting their properties to those of classical bits [4]. The fundamental concept of classical computation and classical information is a bit. A bit is either in state 0 or in state 1. Quantum computation is built upon an analogous concept, the quantum bit, or in short qubit. In the quantum regime we have systems in superposition of states. The difference between qubits and bits is that a qubit can be in a state other than 0 or 1, or we can say in a superposition of 0 and 1. Hence, a set of qubits can represent exponentially more values than their classical-bit counterparts. In other words a single qubit can be described by a linear combination of |0 and |1 given as = α |0 + β |1 (1) Where, α and β are probability amplitudes and can in general both be complex numbers with α2 + β2 = 1 (2) In two-dimensional complex vector space the state of the qubit can be generalized as a vector. The special states 0 and 1 are known as computational basis states, and form an orthonormal basis for this vector space, being |0 = (0, 1) and |1 = (1, 0) One picture useful in thinking about the evolution of the qubit state is the following geometric representation of the.

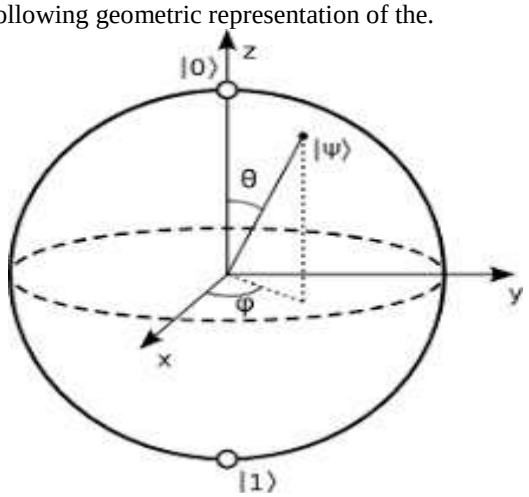


FIGURE 6. Bloch sphere representation of qubit.

pure state space of a two-level quantum mechanical system, named after the physicist Felix Bloch called Bloch sphere representation as shown in Fig. 6.

B. REPRESENTATION OF QUBITS

In quantum mechanics states are often represented in Dirac notation [5], and by extension in quantum computing as well. Dirac notation is used due to the fact that it is miles more compact than the equivalent matrix representation. Vectors are communicated via "kets" in dirac representation, hence the given vector "a" might be stated as |a and "bras" are used to express dual vectors, so the dual vector "b" could be stated as |b. Alternatively, matrix representation as expressed in (3) denotes the probability of the qubit to be in some particular state. Within the matrix, the topmost entry symbolizes the probability of collapsing to state 0, and the lower access within the matrix represents the possibility of collapsing to state 1. 0 = 1 0 ; 1 = 0 1 (3) Matrices representing bits 0 and 1 Eq. (4) depicts the overall state of a single qubit in matrix form and Dirac notation. | = α0 |0 + α1 |1 = α0 α1 |α0| 2 + |α1| 2 = 1 (4) Where α0 and α1 are complex numbers and represent the probability amplitudes of state vectors that must add up to 1. This overall structure can be stretched to n qubits too, and every prospect will lead to a complex entry, with the limit that all squared absolute values sum up to one. It is essential to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

bring up that these inseparable complex numbers turns to one among the two potential levels dependent totally of their chances to happen. It is important to point out here that the probability amplitudes of every single imaginable state are interconnected and while a qubit state is determined it will "collapse" to one of the potential states. In order to obtain more insight clarification of qubits with regards to processing the pursuer is alluded to [6]. As the number of qubits in a quantum system increases the matrix representation becomes cumbersome, for n number of qubits, there may be n2 records within the matrix. As matrix 64 VOLUM.
Quantum Cryptography

ABSTRACT
Modern cryptography algorithms are based over the fundamental process of factoring large integers into their primes, which is said to be "INTRACTABLE". But modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one-way functions such as that of factoring large integers. So the solution is to introduce quantum physics into cryptography, which lead to evaluation of quantum cryptography. Quantum cryptography is one of the emerging topics in the field of computer industry. This paper focus on quantum cryptography and how this technology contributes value to a defense-in-depth strategy pertaining to completely secure key distribution. The scope of this paper covers the weaknesses of modern digital cryptosystems, the fundamental concepts of quantum cryptography, the real-world implementation of this technology along with its limitations, and finally the future direction in which the quantum cryptography is headed towards. We describe results from an apparatus and protocol that is designed to implement the quantum key distribution by which two users who share no secret information (without having any private or public keys known before hand) initially exchange a random quantum transmission consisting of very faint flashes of polarized light
Keywords
Quantum Cryptography systems, Large Scale distributed computational systems, Cryptosystems, Quantum physics.

1. INTRODUCTION

Quantum cryptography recently made headlines when European Union members announced their intention to invest $13 million in the research and development of a secure communications system based on this technology. The system, known as SECOQC (Secure Communication based on Quantum Cryptography), will serve as a strategic defense against the Echelon intelligence gathering system used by the United States, Australia, Britain, Canada and New Zealand. In addition, a handful of quantum information processing companies, including MagiQ Technologies and ID Quantique, are implementing quantum cryptography solutions to meet the needs of businesses, governments, and other institutions where preventing the unauthorized disclosure of information has become a critical success factor in maintaining a competitive advantage over adversaries. While the modern cryptosystems are said to be very effective in other words they are said to be "INTRACTABLE" then why a lot of money is been spent to develop a new cryptosystem – quantum cryptography ?

2. Limitations

of Modern Cryptosystems Since public key cryptography involves complex calculations that are relatively slow, they are employed to exchange keys rather than for the encryption of voluminous amounts of data. For example, widely deployed solutions, such as the RSA and the Diffie-Hellman key negotiation schemes, are typically used to distribute symmetric keys among remote parties. However,because asymmetric encryption is significantly slower than symmetric encryption, a hybrid approach is preferred by many institutions to take advantage of the speed of a shared key system and the security of a public key system for the initial exchange of the symmetric key. Thus, this approach exploits the speed and performance of a symmetric key system while leveraging the scalability of a public key infrastructure. However, public key cryptosystems such as RSA and Diffie-Hellman are not based on concrete mathematical proofs. Rather, these algorithms are considered to be reasonably secure based on years of public scrutiny over the fundamental process of factoring large integers into their primes, which is said to be "intractable". In other words, by the time the encryption algorithm could be defeated, the information being protected would have already lost all of its value. Thus, the power of these algorithms is based on the fact that there is no known mathematical operation for quickly factoring very large numbers given today's computer processing power. While current public key cryptosystems may be "good enough" to provide a reasonably strong level of confidentially today, there is exposure to a handful of risks. For

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

instance, advancements in computer processing, such as quantum computing, may be able to defeat systems such as RSA in a timely fashion and therefore make public key cryptosystems obsolescent instantly. As another example, while the DES algorithm, which has a 56 bit key, was once considered to be secure, it is no longer thought of as such since advancements in technology have made it trivial to defeat. The fact that powerful computers may crack DES in a few hours served as a catalyst for the development of the replacement Advanced Encryption Standard. Hence, one area of risk is that public key cryptography may be vulnerable to the future technology developments in computer processing. Secondly, there is uncertainty whether a theorem may be developed in the future or perhaps already available that can factor large numbers into their primes in a timely manner. At present, there is no existing proof stating that it is impossible to develop such a factoring theorem. As a result, public key systems are thus vulnerable to the uncertainty regarding the future creation of such a theorem, which would have a significant affect on the algorithm being mathematical intractable. This uncertainty provides potential risk to areas of national security and intellectual property which require perfect security. In sum, modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one way functions such as that of factoring large integers. If a factoring theorem were publicized or computing became powerful enough to defeat public cryptography, then business, governments, militaries and other affected institutions would have to spend significant resources to research the risk of damage and potentially deploy a new and costly cryptography system quickly

3. Quantum Cryptography

In Theory Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact, quantum cryptography rests on two pillars of 20th century quantum mechanics –the Heisenberg Uncertainty principle and the.

principle of photon polarization. According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a photon filter with the correct polarization can only detect a polarized photon or else the photon will be destroyed. It is this "one-way-ness" of photons along with the Heisenberg Uncertainty principle that make quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. Bennet and Brassad stated that an encryption key could be created depending on the amount of photons reaching a recipient and how they were received. Their belief corresponds to the fact that light can behave with the characteristics of particles in addition to light waves. These photons can be polarized at various orientations, and these orientations can be used to represent bits encompassing ones and zeros. These bits can be used as a reliable method of forming onetime pads and support systems like PKI by delivering keys in a secure fashion. The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing systems. Since the principle of physics will always hold true, quantum cryptography provides an answer to the uncertainty problem that current cryptography suffers from; it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer Factorization problem.

4. A Quantum Key Distribution

Example The following is an example of how quantum cryptography can be used to securely distribute keys. This example includes a sender, "Alice", a receiver, "Bob", and a malicious eavesdropper, "Eve" Alice begins by sending a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0,45,90 or 135 degrees). For each individual photon, Bob will randomly choose a filter and use a photon receiver to count and measure the polarization which is either rectilinear (0 or 90 degrees) or diagonal (45

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

or 135 degrees), and keep a log of the results based on which measurements were correct vis-à-vis the polarizations that Alice selected. While a portion of the stream of photons will disintegrate over the distance of the link, only a predetermined portion is required to build a key sequence for a onetime pad. Next, using an out- of-band communication system, Bob will inform Alice to the type of measurement made and which measurements were of the correct type without mentioning the actual results. The photons that were incorrectly measured will be discarded, while the correctly measured photons are translated into bits based on their.polarization. These photons are used to form the basis of a onetime pad for sending encrypted information. It is important to point out that neither Alice nor Bob are able to determine what the key will be in advance because the key is the product of both their random choices. Thus, quantum cryptography enables the distribution of a one-time key exchanged securely.

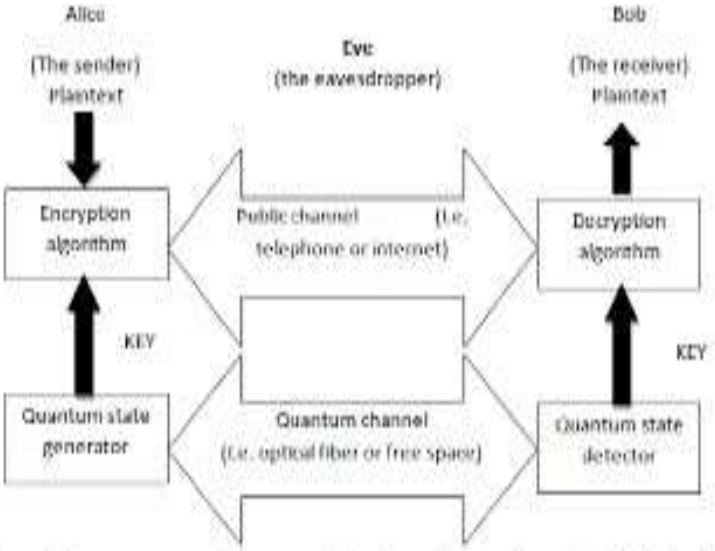
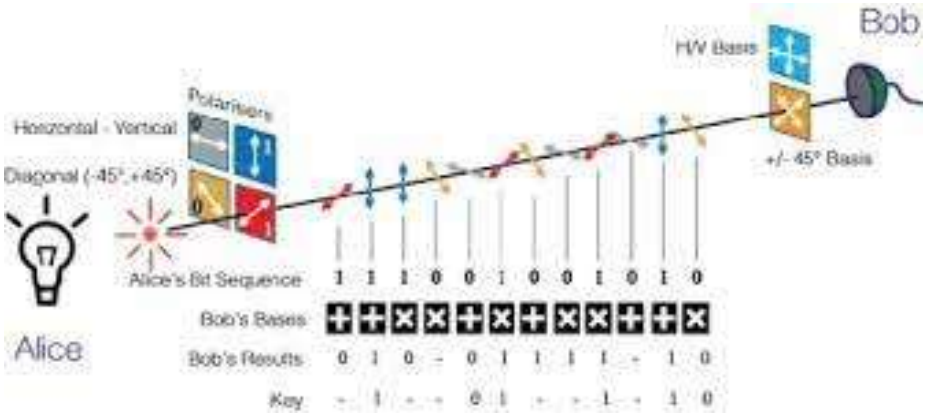


Figure 1: Quantum cryptographic communication System for securely transferring Random key

Now let us suppose that a malicious attacker attempts to infiltrate the cryptosystem and defeat the quantum key distribution mechanisms. If this malicious attacker, named Eave, tries to eavesdrop, she too must also randomly select either a rectilinear or diagonal filter to measure each of Alice's photons. Hence, Eve will have an equal chance of selecting the right and wrong filter, and will not be able to confirm with Alice the type of filter used. Even if Eve is able to successfully eavesdrop while Bob confirms with Alice the protons he received, this information will be of little use to Eve unless she knows the correct polarization of each particular photon. As a result, Eve will not correctly interpret the photons that form the final key, and she will not be able to render a meaningful key and thus be thwarted in her endeavors. In sum, there are three significant advantages of this system. First, the Heisenberg Uncertainty principle means that information regarding photons cannot be duplicated because photons will be destroyed once they are measured or tampered with. Since photons are indivisible, once it hits a detector, the photon no longer exists. Secondly, Alice and Bob must calculate beforehand the amount of photons needed to form the encryption key so that the length of the one-time pad will correspond to the length of the message. Since mathematically Bob should receive about 25 percent of transmitted photons, if there is a deviation for the predetermined fixed number, Bob can be certain that traffic is being sniffed or something is wrong in the system. This is the result of the fact that if Eve detects a photon, it will no longer exist to be detected by Bob due to Eve's inability to copy an unknown quantum state. If Eve attempts to create and pass on to Bob a photon, she will have to randomly choose its orientation, and on average be incorrect about 50 percent of the time –enough of an error rate to reveal her presence.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252



5. Desirable QKD Attributes

Broadly stated, QKD offers a technique for coming to agreement upon a shared random sequence of bits within two distinct devices, with a very low probability that other devices (eavesdroppers) will be able to make successful inferences as to those bits' values. In specific practice, such sequences are then used as secret keys for encoding and decoding messages between the two devices. Viewed in this light, QKD is quite clearly a key distribution technique, and one can rate QKD's strengths against a number of important goals for key distribution, as summarized in the following paragraphs.

5.1 Confidentiality of Keys

Confidentiality is the main reason for interest in QKD. Public key systems suffer from an ongoing uncertainty that decryption is mathematically intractable. Thus key agreement primitives widely used in today's Internet security architecture, e.g., DiffieHellman, may perhaps be broken at some point in the future. This would not only hinder future ability to communicate but could reveal past traffic. Classic secret key systems have suffered from different problems, namely, insider threats and the logistical burden of distributing keying material. Assuming that QKD techniques are properly embedded into an overall secure system, they can provide automatic distribution of keys that may offer security superior to that of its competitors.

5.2 Authentication

QKD does not in itself provide authentication. Current strategies for authentication in QKD systems include prepositioning of secret keys at pairs of devices, to be used in hash-based authentication schemes, or hybrid QKD-public key techniques. Neither approach is entirely appealing. Prepositioned secret keys require some means of distributing these keys before QKD itself begins, e.g., by human courier, which may be costly and logistically challenging. Furthermore, this approach appears open to denial of service attacks in which an adversary forces a QKD system to exhaust its stockpile of key material, at which point itcan no longer perform authentication. On the other hand, hybrid QKD-public key schemes inherit the possible vulnerabilities of public key systems to cracking via quantum computers or unexpected advances in mathematics.

5.3 Sufficiently Rapid Key Delivery

Key distribution systems must deliver keys fast enough so that encryption devices do not exhaust their supply of key bits. This is a race between the rate at which keying material is put into place and the rate at which it is consumed for encryption or decryption activities. Today's QKD systems achieve on the order of 1,000 bits/second throughput for keying material, in realistic settings, and often run at much lower rates. This is unacceptably low if one uses these keys in certain ways, e.g., as one-time pads for high speed traffic flows. However it may well be acceptable if the keying material is used as input for less secure (but often secure enough) algorithms such as the Advanced Encryption Standard. Nonetheless, it is both desirable and possible to greatly improve upon the rates provided by today's QKD technology.

5.4 Robustness

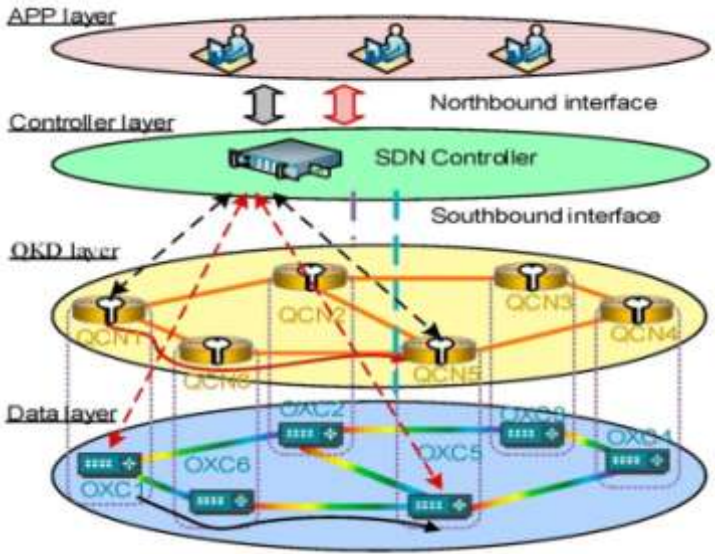
The QKD community has not traditionally taken this into account. However, since keying material is essential for secure communications, it is extremely important that the flow of keying material not be disrupted, whether by accident or by the deliberate acts of an adversary (i.e. by denial of service). Here QKD has provided a highly fragile service to date since QKD techniques have implicitly been employed along a single point-to-point link. If that link were disrupted, whether by active eavesdropping or indeed by fiber cut, all

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

flow of keying material would cease. In our view a meshed QKD network is inherently far more robust than any single point-to-point link since it offers multiple paths for key distribution.

5.5 Distances and Location Independence

In the ideal world, any entity can agree upon keying material with any other (authorized) entity in the world. Rather remarkably



Computer on the Internet can form a security association with any other, agreeing upon keys through the Internet IPsec protocols. This feature is notably lacking in QKD, which requires the two entities to have a direct and unencumbered path for photons between them, and which can only operate for a few tens of kilometers through fiber

5.6 Resistance to Traffic Analysis

Adversaries may be able to perform useful traffic analysis on a key distribution system, e.g., a heavy flow of keying material between two points might reveal that a large volume of confidential information flows, or will flow, between them. It may thus be desirable to impede such analysis. Here QKD in general has had a rather weak approach since most setups have assumed dedicated, point-topoint QKD links between communicating entities, which thus clearly lays out the underlying key distribution relationships.

6. Implementing Quantum Cryptography

Here we talk about different systems that have sucessfully implemented quantum Cryptography technology

6.1 The DARPA Quantum NetworkThe DARPA security model is the cryptographic Virtual Private Network (VPN). Conventional VPNs use both public-key and symmetric cryptography to achieve confidentiality and authentication/integrity. Public-key mechanisms support key exchange or agreement, and authenticate the endpoints. Symmetric mechanisms (e.g. 3DES, SHA1) provide traffic confidentiality and integrity. Thus VPN systems can provide confidentiality and authentication / integrity without trusting the public network interconnecting the VPN sites. In DARPA work, existing VPN key agreement primitives are augmented or completely replaced by keys provided by quantum cryptography.

The remainder of the VPN construct is left unchanged; see Fig. 2. Thus DARPA QKD-secured network is fully compatible with conventional Internet hosts, routers, firewalls, and so fort.

7. QKD Protocols Implementation Quantum cryptography involves a surprisingly elaborate suite of specialized protocols, which we term "QKD protocols." Many aspects of these protocols are unusual – both in motivation and in implementation – and may be of interest to specialists in communications protocols.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 03 Mar. 2024, pp: 200-208 www.ijaem.net ISSN: 2395-5252

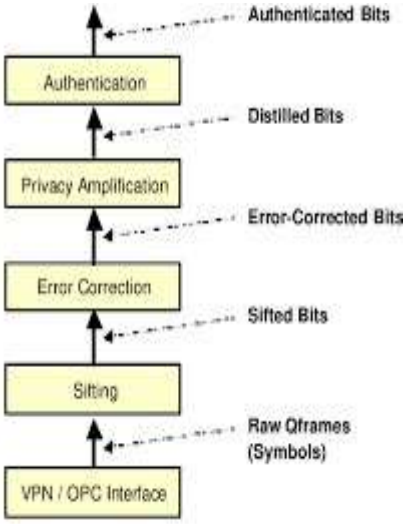


Fig. 9. The QKD protocol stack.

This section describes the protocols now running in our C language QKD protocol implementation. DARPA have designed this engine so it is easy to "plug in" new protocols, and expect to devote considerable time in coming years to inventing new QKD protocols and trying them in practice. As shown in Fig. 5, these protocols are best described as sub-layers within the QKD protocol suite. Note, however, that these layers do not correspond in any obvious way to the layers in a communications stack, e.g., the OSI layers. As will be seen, they are in fact closer to being pipeline stages.

7.1 Sifting

is the process whereby Alice and Bob window away all the obvious "failed q bits" from a series of pulses. As described in the introduction to this section, these failures include those qubits where Alice's laser never transmitted,

Bob's detectors didn't work, photons were lost in transmission, and so forth. They also include those symbols where Alice chose one basis for transmission but Bob chose the other for receiving. At the end of this round of protocol interaction – i.e. after a sift and sift response transaction – Alice and Bob discard all the useless symbols from their internal storage, leaving only those symbols that Bob received and for which Bob's basis matches Alice's.

7.2 Error Correction

Error correction allows Alice and Bob to determine all the "error bits" among their shared, sifted bits, and correct them so that Alice and Bob share the same sequence of error-corrected bits. Error bits are ones that Alice transmitted as a 0 but Bob received as a 1, or vice versa. These bit errors can be caused by noise or by eavesdropping. Error correction in quantum cryptography has a very unusual constraint, namely, evidence revealed in error detection and correction (e.g. parity bits) must be assumed to be known to Eve, and thus to reduce the hidden entropy available forkey material. As a result, there is very strong motivation to design error detection and correction codes that reveal as little as possible in their public control traffic between Alice and Bob.

7.3 Privacy amplification Privacy

amplification is the process whereby Alice and Bob reduce Eve's knowledge of their shared bits to an acceptable level. This technique is also often called advantage distillation. The side that initiates privacy amplification chooses a linear hash function over the Galois Field GF[2n] where n is the number of bits as input, rounded up to a multiple of 32. He then transmits four things to the other end—the number of bits m of the shortened result, the (sparse) primitive polynomial of the Galois field, a multiplier (n bits long), and an m-bit polynomial to add (i.e. a bit string to exclusive-or) with the product. Each side then performs the corresponding hash and truncates the result to m bits to perform privacy amplification.

7.4 Authentication

allows Alice and Bob to guard against "man in the middle attacks," i.e., allows Alice to ensure that she is communicating with Bob (and not Eve) and vice versa. Authentication must be performed on an ongoing basis for all key management traffic, since Eve may insert herself into the conversation between Alice and Bob at any stage in their communication. The original BB84 paper [1] described the authentication problem and sketched a solution to it based on universal families of hash functions, introduced by Wegman and Carter [20]. This approach requires Alice and Bob to already share a small secret key, which is used to select a hash function from the family to generate an authentication hash of the public correspondence between them. By the nature of universal hashing, any party who didn't know the secret key would have an extremely low probability of being able to forge the correspondence, even an adversary with unlimited computational power. The drawback is that the secret key bits cannot be re-used even once on different data without compromising the security. Fortunately, a complete authenticated conversation can validate a large number of new,shared secret bits from QKD, and a small number of these may be used to replenish the pool.

There are many further details in a practical system which we will only mention in passing, including symmetrically authenticating both parties, limiting the opportunities for Eve to force exhaustion of the shared secret key bits, and adapting the system to network asynchrony and retransmissions. Another important point: it is insufficient to authenticate just the QKD protocols; we must also apply these techniques to authenticate the VPN data traffic.

DISCUSSION AND CONCLUSION

DARPA is now starting to build multiple QKD links woven into an overall QKD network that connects its QKD endpoints via a mesh of QKD relays or routers. When a given point-to-point QKD link within the relay mesh fails – e.g. fiber cut or too much eavesdropping or noise abandons that link abandoned and another used instead. This emerging DARPA Quantum Network can be engineered to be resilient even in the face of active eavesdropping or other denial-of-service attacks. Such a design may be termed a "key transport network." Looking to the later years of the DARPA Quantum Network, the principal weakness in untrusted QKD networks – limited geographic reach – may perhaps be countered by quantum repeaters. There is nogreat deal of active research aiming towards such repeaters, and if practical devices are ever achieved, they should slide neatly into the overall architecture of untrusted QKD networks to enable seamless QKD operations over much greater distances than currently feasible.

A proposed solution to the distance problem may be to "chain" quantum cryptography links with secure intermediary stations. Otherwise, an alternative solution is transmission through free space or low orbiting satellite. In this scenario, the satellite acts as the intermediary station, and there is less attenuation of photons in the atmosphere. Research into this area is still ongoing and work is underway in both the US and Europe to be able to send quantum keys up to satellites and then down to another destination securely.

While there have been substantial advancements in the field of quantum cryptography in the last decade, there are still challenges ahead before quantum cryptography can become a widely deployed key distribution system for governments, businesses, and individual citizens. Namely, these challenges include developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. However, the advances in computer processing power and the threat of obsolescence for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography. In fact, in is expected that nearly $50 million of both public and private funds will be invested in quantum cryptography technology over the next three years3. Quantum cryptography is still in its infancy and so far looks very promising. This technology has the potential to make a valuable contribution to e-commerce and business security, personal security, and security among government organizations. If quantum cryptography turns out to eventually meet even some of its expectations, it will have a profound and revolutionary affect on all of our lives.

REFERENCES

[1]. C. Bennett and G. Brassard, "Quantum Cryptography:Public Key Distribution and Coin Tossing," International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
[2]. A. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett. 67, 661 (5 August 1991).
[3]. Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use.Commun.ACM 38, 12 (entire issue).
[4]. Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002..
[5]. Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

About the authors: