Quantum Key Distribution as a Next-Generation Cryptographic Protocol

Andrew Campbell

Abstract

Promising advances in the field of quantum computing indicate a growing threat to cryptographic protocols based on integer factorization. To counter this threat, researchers have already designed and tested alternative protocols that do not rely on factorization. Quantum key distribution, a cryptographic mechanism that relies on the inherent randomness of quantum mechanics, serves not only as an option to replace techniques made vulnerable by quantum computing, but also as a more secure protocol that works fundamentally differently from previous cryptographic techniques. However, it is still subject to clever forms of eavesdropping and poses a significant challenge to implementation.

1. Motivation

Secure communication and authentication in the modern ages stems mostly from the idea of public-key cryptography proposed by Diffie and Hellman(1976). This technique and its successors provide security by allowing two parties to establish secure communications solely through the exchange of publicly available keys, without revealing the privately held keys needed to decrypt the messages. It is mathematically possible to calculate the private key by using the publicly available information, thus breaking the security of the technique, but this proves to be intractable given the power of modern computers. For a sufficiently long key, solving the factorization problem to crack the private key would take longer than the age of the universe. Because of this assurance, public-key cryptography forms the backbone of a variety of authentication protocols such as SSL. Even applications that rely on more powerful symmetric key encryption rely on public-key cryptography to perform the series of 'handshakes' needed to securely pass the secret key used in the encryption process. As a result, the Diffie-Hellman technique is present in almost all modern cryptographic exchanges.

However, the intractability that has made public-key cryptography so useful does not apply to the steadily growing field of quantum computing. Quantum computers use the energy states of atoms rather than electric switches to represent information. In a traditional computer, a single bit can be set to either 0 or 1 through the application or removal of current. Thus a computer consisting of n bits may store any one of 2^n values. Due to quantum uncertainty, though, a quantum bit (qubit) may exist in a *coherent superposition* of the states 0 and 1, meaning it holds both values at the same time. A quantum computer containing n qubits can store all 2^n possible values at the same time, and on any given computational cycle can perform an operation on all numbers simultaneously.

As a result, quantum computers may be programmed in a manner fundamentally different from classic computers. There exist quantum algorithms that have no known analogues on current computers. One such algorithm, developed by Shor in 1994, is a polynomial time solution to the integer factorization problem (Shor, 1995). The algorithm takes advantage of the simultaneity of quantum states to rapidly solve a periodic function that is the most time-consuming step in more traditional factorization algorithms. Like most quantum algorithms, Shor's method contains an element of randomness and does not guarantee a correct answer on any given iteration. However, even traditional computers can quickly check whether or not a proposed factor of an integer is correct, so Shor's algorithm may be rapidly run as many times as needed to produce the correct answer.

The quantum factorization algorithm has already been tested on a rudimentary quantum computer and found to be correct. While the sample problem used, factoring the number 15, was trivial, the proof of concept demonstrates that public-key cryptography faces a looming danger from quantum computing. As more advanced quantum computers are developed, it will become trivial to crack the current key sizes used in RSA. Because Shor's algorithm is polynomial, increasing the key size will not prove to be an effective deterrent to cracking attempts. In order to protect information in the quantum computing age, entirely new cryptographic techniques will be required.

2. Quantum Key Distribution

An encryption method with the potential of not only circumventing the shortcomings of public-key cryptography but also of revolutionizing the way secure messages are exchanged has been under development for the last 20 years. This technique is known as quantum key distribution(QKD), and relies on the laws of quantum mechanics to provide a new method of exchanging a secret encryption key. Under traditional cryptography, there is no way for two individuals to securely share a secret key over an unprotected channel because of the possibility of an eavesdropper. This is why public-key cryptography is often used to authenticate a communication channel before a secret key is exchanged. In contrast, QKD provides a mechanism by which two parties may create a secret key in

the presence of an eavesdropper without having their security compromised.

QKD can be implemented in a variety of manners depending on the medium of transmission and the error-correcting schemes in place, so it may be more illustrative to first discuss the differences between QKD and current cryptographic techniques. At the heart of QKD is the encoding of the information to be transferred as a quantum state, whether that be a polarized photon or a pair of particles experiencing quantum entanglement. Throughout the history of cryptography, all ciphers have had one thing in common: the set of symbols used to represent information carried the same meaning to an eavesdropper as it did to the intended recipient. Whether the message being transmitted consisted of letters, pictures, or differences in electric potential indicating binary digits, an eavesdropper had the ability to copy the information before allowing it to reach the true recipient. This 'man in the middle' attack has been an ever-present threat that cryptologists have had to take into account when designing protocols.

Quantum particles, however, operate in fundamentally different manner than traditional means of conveying information. Namely, due to quantum uncertainty it is literally impossible to recreate an arbitrary quantum state. This means that when a bit of information is encoded as a particle and sent down a quantum communication line, and eavesdropper who intercepts the particle is no longer guaranteed the ability to copy it and send it on to the intended recipient. Thus, quantum encoding offers the ability to design protocols that talk over the head of a man in the middle for the first time in history. It must be emphasized that this means that not only does QKD offer immunity to the integer factorization attacks that threaten modern cryptography, when properly implemented it offers a fundamentally more secure means of communication. As long as the laws of quantum physics are found to be valid, QKD offers a guarantee against complete eavesdropping that is not found in any other means of information transmission.

This is not to say that quantum communication is a magic bullet that solves the problem of secure communication. In order for a protocol to allow two individuals to communicate effectively via a quantum channel, some restrictions must be placed on the allowed states of the particle being used to transmit the message. If this were not the case, the same inscrutability that denies eavesdroppers the opportunity to attack would prevent the intended recipient from extracting any information from the message. By restricting the states, however, it becomes possible for a lucky attacker to gain some information by applying knowledge of the allowed states to the tapped communication line. Thus, a complete QKD protocol consists of several components: a scheme for encoding binary data in quantum states, a mechanism that uses these quantum states to allow two users to agree on a shared random key, error-correction processes to reduce the effects of noise in the communication line, and a privacy-enhancing process to reduce the information acquired by a clever eavesdropper to an unusable level. Once these steps are complete the users should have available a shared, randomly-generated, secret key of which an intruder knows nothing or close to nothing. This key can then be used in a symmetric key cryptographic algorithm or as a one-time pad to allow the two users to communicate securely over traditional channel. Quantum key distribution is thus a mechanism for delivering via quantum channels a cryptographic key for use in existing communication systems.

3. The BB84 Protocol

The discussion to this point has been kept vague due to the great variety available when designing a QKD system. Many papers have been published since the invention of QKD on the different schemes available for encoding numbers as quantum states, which in turn affects the mechanism for generating a random key. However, a concrete example would help illustrate more clearly the concepts that have so far been discussed only abstractly.

The first QKD protocol ever designed was presented by Bennet and Brassard in 1984. Their system, known as the BB84 protocol, used polarized photons as the means for transmitting information (Bennet & Brassard, 1985). When a photon is polarized, it oscillates along a single axis as it propagates through space. An immediate application of this idea is to agree upon an orientation to represent the number one, and transmit photons corresponding to the number one polarized so that they oscillate in that orientation. A detector can be configured to verify whether or not the incoming photon is in that orientation. If it is, the receiver knows that a 1 has been transmitted, and if not then a 0. It is important to note that the detector can only register whether or not the photon was in a given orientation. The act of observing it destroys the orientation, so if the photon was not oscillating along the axis agreed upon to represent 1, it is impossible to determine which axis it was in fact oscillating along.

If the system relied only upon this single axis representing 1 the protocol would still be vulnerable to an eavesdropper who knew what this orientation was and tapped into the communication line with a receiver of their own. Therefore the BB84 protocol calls for four states, two representing 1, and two representing 0. These four states provide two bases for transmitting the information. This means that for a receiver to properly decode the qubit it must not only have access to the photon but also know which basis was being used to transmit it. With this modification an eavesdropper in the middle is faced with a conundrum. In order to properly intercept messages they must choose one of the two bases with which to interpret incoming photons. Without any outside knowledge they will have to guess, meaning they will on average choose the

incorrect basis for half the photons. These photons will provide no usable information, and thus the attacker is limited to accessing at most half the material being transmitted.

Of course, the true recipient of the message faces the same problem. The BB84 protocol thus specifies a mechanism for the two users to extract meaningful information despite this handicap. The session begins when the users(known as Alice and Bob, of course) generate some random numbers. Alice needs two numbers, one to encode as photons and transmit to Bob, and another to determine which basis to use for each qubit she sends. It is important that the bases be selected randomly so that Eve, the malicious attacker, cannot gain more than 50% of the message. Bob's random number, on the other hand, is used to decide which basis he will use when receiving Alice's qubits.

Alice begins transmitting her random number to Bob one qubit at a time using a randomly selected basis each time. Bob meanwhile receives each qubit according to his randomly selected basis. Because half of Alice's qubits, on average, were encoded using a different basis, Bob has had to guess on what value half of them held. Since he will be right about half the time when guessing, he now has a copy of the random number Alice sent him in which about 25% of the bits are incorrect. However, Alice and Bob can now announce on a public channel which bases they used for each qubit and throw away each qubit they differed on. Ignoring for the moment errors introduced by the photon transmission process, Alice and Bob now possess a shared number derived from the random numbers each of them originally generated.

This whole scenario took place without the interference of Eve, however. Imagine now that Eve had gained access to the quantum channel and had been making her own guesses as to the basis being used by Alice. At the end of the transmission when Bob and Alice announce which bases they were using, Eve now knows which of her qubits are useless and can discard them too. However, because she used a different set of bases than the ones randomly selected by Bob her set of mismatched bases is completely different from his. As a result, when she throws away the qubits Alice and Bob are discarding, she is still missing about half the qubits that were transferred, meaning she cannot gain access to the secret key.

It could be rightfully declared that having an eavesdropper possess even half the key is an undesirable scenario. Fortunately, the scenario described above in which Eve plays along with Alice and Bob as they go through the key creation process is impossible. This is because, as observed earlier, quantum information is irrevocably altered upon viewing. In order to eavesdrop without being detected, Eve must send each piece of information she intercepts off to Bob in order to conceal her interference. However, because her bases differ from Alice's Eve has lost about half the information she intercepted. This means she can only guess at what the qubits contained when she sends her false copies on to Bob. When Alice and Bob compare results after creating their key, they will find that there is still a 25% error rate in the data because of the corruption caused by Eve's interference. This error rate is easily detectable, and will reveal to Alice and Bob that there is an intruder in their communication line.

This summary of the BB84 protocol highlights the differences between QKD techniques and traditional quantum computing practices. However, it also made several idealizations along the way. For one, error due to degradation of the quantum signal was discounted, which is a quite unrealistic assumption to make given the complexity of current quantum transmission devices. Secondly, the intruder detection based on error rate only holds true if the eavesdropper attempts to intercept every photon. A clever intruder who is aware of this limitation might try to intercept only a fraction of the incoming qubits, thus driving the error rate down to a level that may be attributed to signal degradation rather than malicious intrusion. In order to complete this, or any other QKD protocol, measures must be taken to correct for these possibilities.

Fortunately the tasks of removing the flaws introduced by signal error and reducing the information held by an intruder are challenges faced by conventional cryptographic algorithms, and thus techniques currently exist for fighting both problems. The methods available for error correction are varied, and the particular one used does not matter as long as it minimizes the private information shared by Alice and Bob during the correction process. It is important to ensure that Eve does not gain access to any additional material beyond that acquired during her initial snooping.

Once the errors have been removed and Alice and Bob share a secret key, they can begin using techniques to minimize the information held by Eve. In general, these methods rely on recombining the bits of the secret key in some fashion such that Eve, who is missing many of the bits, will find impossible to follow. One simple example mentioned by Gisin et al. in their discussion on the subject is the technique of randomly selecting segments of the key, xoring them, and replacing the segments with the result (Gisin et al., 2002). Eve may know which segments are being selected if Alice and Bob agree on them over a public channel, but because she lacks all the bits she will lose information each time an xor is carried out on incomplete segments of her key.

4. Obstacles and Vulnerabilities

As revolutionary and intriguing as QKD is, it is far from a perfect solution to the problem of secure communications. There are several obstacles to the creation of a system capable of running QKD protocols, and while quantum mechanics offers security unavailable to

other cryptographic methods there are still vulnerabilities that must be guard against.

The primary barrier to implementing QKD systems is the difficulty in creating and maintaining particles that exhibit desired quantum states without experiencing contamination from the environment. The polarized photons described in the BB84 protocol, for example, must be produced by a laser operating in a narrow range of frequencies. It is important that only one photon be dispatched at a time, and while there is no laser in existence that can guarantee that, minimizing the occurrence of double photons requires careful configuration. The receiving apparatus must also be carefully prepared, and false positives, signals received in the absence of a dispatched photon, are an unfortunate feature of non-idealized receivers.

The method of transporting the signal to the receiver poses another problem. While experiments in the laboratory have implemented QKD by launching photons through open space, this method is impractical over all but the shortest distances due to interference. Conventional fiber optic cables of the sort currently in use by telecommunications companies do not entirely solve the problem, however. The longer the length of cable, the greater the chance of the photon gradually shifting polarity as it travels down the length due to imperfections. While QKD has been run over fiber optic cables more than 20 kilometers long, it was observed that the error rate began increasing the longer the protocol was run as the cable slowly shifted out of alignment with the receiver.

These various challenges in design pose a significant obstacle to the general production and use of QKD systems. Because quantum encryption requires hardware not currently in use in most facilities and great expertise to tune the proper equipment once it is acquired, the technique is not currently useful outside the laboratories of the scientists who research it. Until more sophisticated and generally usable equipment is available, QKD is simply an impractical alternative for most users.

In addition to the physical challenges that impede the propagation of QKD systems, there are security considerations that need to be taken into account when considering a shift to quantum cryptography. A QKD protocol is only as strong as its weakest point. In the case of the BB84 protocol, Alice and Bob communicate a large amount of information to each other in the course of finalizing their key selection. While it is not important to the security of QKD that the channel they use for communication be private, it is critical that it be authenticated. If Eve has the ability to impersonate Bob or Alice, then she can simply share her information in place of the intended recipient and thus have her unknowing partner aid her in establishing the secure key. The most popular method of authenticating communication is public-key cryptography, which poses a chicken-or-the-egg dilemma to quantum cryptography as an heir to asymmetric key algorithms.

Assuming a secure method of authentication has been provided, however, there is still cause for caution when implementing a QKD system. A clever eavesdropper can calculate via probability and information theory the optimum strategy for intercepting qubits to maximize their information gain while minimizing their error rate. While it is still guaranteed that they can never acquire the whole key just by eavesdropping, the more key information obtained by the intruder the greater the chance of them cracking the resulting encryption. It is therefore still vital that users of the QKD protocol take steps to protect themselves from well-prepared intruders using optimized strategies.

Finally, a well equipped intruder can exploit the physical vulnerabilities of the system mentioned earlier to acquire more information than they could in the idealized model. For example, whenever a laser emitting photons as part of the BB84 protocol accidentally releases two photons simultaneously, an eavesdropper has the opportunity to capture and analyze one while allowing the other to reach its destination. Thus the intruder gains information without a corresponding increase in the error rate, decreasing the chance that they will be detected.

Because the field of quantum cryptography is still young, knowledge of potential attacks and their success rates is relatively undeveloped. As such, it is important that anyone implementing the QKD protocol not mistake the security offered by quantum mechanics as a guarantee of perfect security. As with any cryptographic protocol, good planning and cautious monitoring of a QKD implementation will go a long way towards protecting against attacks as they are developed.

5. Conclusion

Quantum key distribution offers greater potential for secure communications than any previous cryptographic protocol. The fact that is immune not just to the new types of attacks made possible to quantum computing, but is in fact unable to be totally compromised by any physical means makes it a very impressive application of quantum mechanics. However, due to the shortcomings of the technology currently available to implement quantum cryptography systems, it will be some time before the technique can be widely adopted.

As quantum computing develops towards the point at which modern day encryption techniques are called into question, the same technological advances that threaten secure communication should bring forth a new cryptography paradigm that will carry computers through the quantum age.

References

Bennett, C. H. & Brassard, G. (1985). Quantum public key distribution system. *IBM Tech. Discl. Bull*, 28, 3153–3163.

Gisin, N., et al. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74, 145-190.

Hughes, R., et al. (1995). Quantum cryptography. *Contemporary Physics*, 36, 149.

Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of Foundations of Computer Science ’94*.