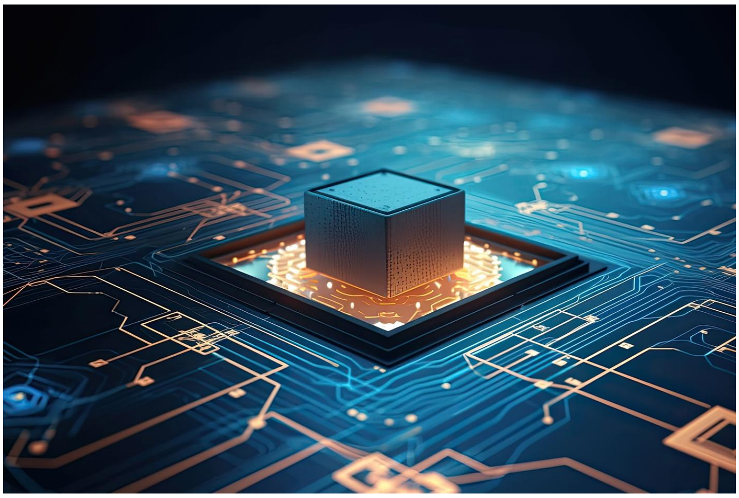
Quantum Key Exchange

Léo Gabaix - Francesco Mosanghini



1. Introduction

1.1 What is quantum cryptography?

Quantum cryptography was proposed first by Stephen Wiesner, then at Columbia University in New York, who, in the early 1970s, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78–88, 1983). In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes.

A decade later, building upon this work, Charles H. Bennett, of the IBM Thomas J. Watson Research Center, and Gilles Brassard, of the University of Montreal, proposed a method for secure communication based on Wiesner's "conjugate observables". In 1990, Artur Ekert, then a PhD student at Wolfson College, University of Oxford, developed a different approach to quantum key distribution based on quantum entanglement.

1.2 What is a Qubit?

Before beginning to talk about quantum key distribution and exchange, it's essential to define the qubit and its role inside quantum computing.

A qubit is like a more advanced version of a regular computer bit. Normally, bits in computers are either a 0 or a 1. But a qubit, which is used in quantum computing, can be both 0 and 1 at the same time thanks to quantum physics. This allows quantum computers to process complex calculations much faster than traditional computers. Additionally, qubits can be entangled, meaning the state of one qubit can depend on the state of another, no matter the distance between them, leading to highly efficient information processing and communication capabilities.

NB. a qubit can exist in typical states $|0\rangle$,$|1\rangle$ or in any linear combination of these two states, such that $a|0\rangle+b|1\rangle$, where $a,b \in C$ and $a^2 + b^2 = 1$

1.3 What is Quantum Key Distribution?

Quantum key distribution (QKD) is a secure communication method that leverages components of quantum mechanics to enable two parties to generate a shared random secret key exclusively known to them. This key, produced solely for encryption and decryption purposes, is often associated with the one-time pad algorithm, offering provable security when paired with a secret random key. QKD, more akin to a communication architecture than a cryptographic protocol, implements a quantum-cryptographic protocol to facilitate the creation and exchange of this shared secret key between the parties involved.

An important and unique property of quantum key distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e., the eavesdropper has no information about it). Otherwise no secure key is possible, and communication is aborted.

1.4 What is Quantum Key Exchange?

Quantum Key Exchange (QKE) is a cryptographic concept originally explored by Donald Beaver. QKE is a revolutionary field at the intersection of quantum physics and cryptography, it offers a cutting-edge solution to the ever-increasing threat posed by quantum computers to classical encryption methods. It leverages the intriguing properties of quantum mechanics, such as superposition and the no-cloning theorem, to enable two parties to generate a shared encryption key that remains secure even in the presence of a powerful eavesdropper. This technology holds the potential to redefine the landscape of secure communication in a future where quantum computers could break classical encryption, providing a robust foundation for post-quantum cryptography.

2. Quantum Key Exchange

Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security. There are several different approaches to quantum key distribution, but they can be divided into two main categories depending on which property they exploit:

- **Prepare and measure protocols**

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. In general, measuring an unknown quantum state changes that state in some way. This is a consequence of quantum indeterminacy and can be exploited in order to detect any eavesdropping on communication (which necessarily involves measurement) and, more importantly, to calculate the amount of information that has been intercepted.

- **Entanglement based protocols**

The quantum states of two (or more) separate objects can become linked together in such a way that they must be described by a combined quantum state, not as individual objects. This is known as entanglement and means that, for example, performing a measurement on one object affects the other. If an entangled pair of objects is shared between two parties, anyone intercepting either object alters the overall system, revealing the presence of the third party (and the amount of information they have gained).

These two approaches can each be further divided into three families of protocols: discrete variable, continuous variable and distributed phase reference coding. Discrete variable protocols were the first to be invented, and they remain the most widely implemented. The other two families are mainly concerned with overcoming practical limitations of experiments. The two protocols described below both use discrete variable coding.

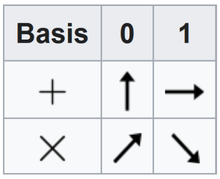
2.1 Protocols

2.1.1 BB84: Charles H. Bennett and Gilles Brassard (1984)

2.1.1.1 Introduction

This protocol, known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information. However, any two pairs of conjugate states can be used for the protocol, and many optical-fiber-based implementations described as BB84 use phase encoded states. The sender (Alice) and the receiver (Bob) are connected by a quantum communication channel which allows quantum states to be transmitted. In the case of photons this channel is generally either an optical fiber or simply free space. In addition they communicate via a public classical channel, for example using broadcast radio or the internet. The protocol is designed with the assumption that an eavesdropper (Eve) can interfere in any way with the quantum channel, while the classical channel needs to be authenticated.

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot in general be measured without disturbing the original state. BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left-and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used.



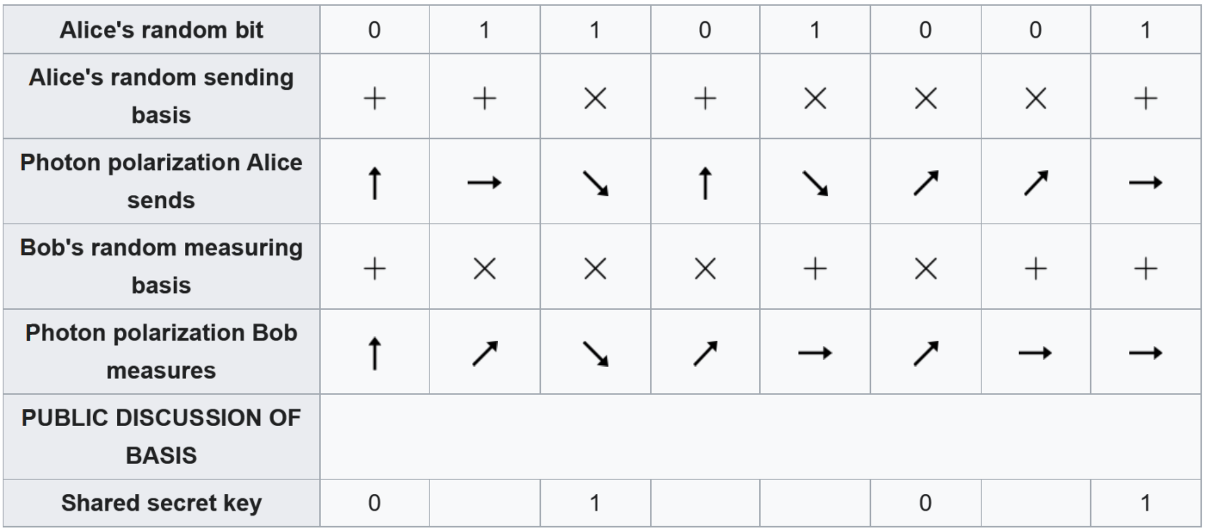
Basis	0	1
+	↑	→
×	↗	↘

2.1.1.2 Quantum Transmission

Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the adjacent table. So for example a 0 is encoded in the rectilinear basis (+) as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 135° state. Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent.

According to quantum mechanics (particularly quantum indeterminacy), no possible measurement distinguishes between the 4 different polarization states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states (an orthonormal basis). In fact, Photons can be polarized in different ways, such as horizontally, vertically, or at angles like 45° and 135°. When you measure a photon's polarization in the rectilinear basis (horizontal or vertical), if it was initially in one of these states, you get an accurate reading. But if it was in a diagonal state (45° or 135°), the measurement forces it into either horizontal or vertical randomly. This process also changes the photon's original state to the one it's measured in, erasing the previous polarization information.

As Bob does not know the basis the photons were encoded in, all he can do is to select a basis at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, measurement basis used and measurement result. After Bob has measured all the photons, he communicates with Alice over the public classical channel. Alice broadcasts the basis each photon was sent in, and Bob the basis each was measured in. They both discard photon measurements (bits) where Bob used a different basis, which is half on average, leaving half the bits as a shared key.



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Quantum transmission example

To check for the presence of an eavesdropper, Alice and Bob now compare a predetermined subset of their remaining bit strings. If Eve has gained any information about the photons' polarization, this introduces errors in Bob's measurements. Other environmental conditions can cause errors in a similar way. If more than p bits differ they abort the key and try again, possibly with a different quantum channel, as the security of the key cannot be guaranteed. p is chosen so that if the number of bits known to Eve is less than this, privacy amplification can be used to reduce Eve's knowledge of the key to an arbitrarily small amount at the cost of reducing the length of the key.

2.1.2 E91 protocol: Artur Ekert (1991)

Artur Ekert's method employs entangled pairs of photons, which can originate from Alice, Bob, or even an external source, including potential eavesdropper Eve. These photons are distributed in a manner that ensures both Alice and Bob possess one photon from each pair.

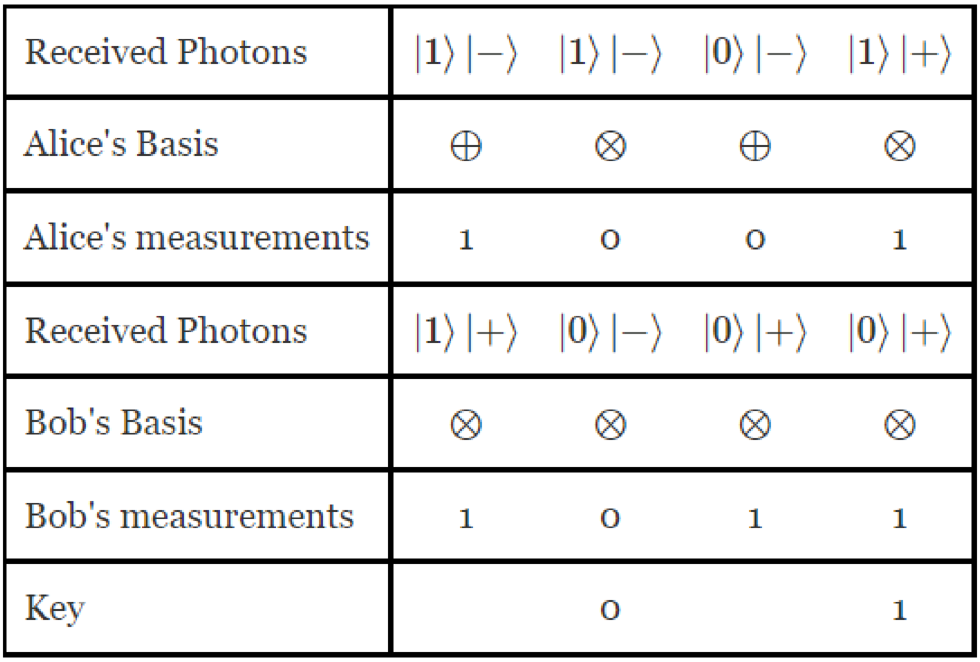
The protocol relies on the distinctive properties of entanglement. Firstly, the entangled states exhibit perfect correlation: when Alice and Bob independently measure their particles for vertical or horizontal polarizations, they unfailingly obtain identical outcomes with 100% certainty. This consistency necessitates precise synchronization between the two remote parties. Nonetheless, the specific results remain entirely random, rendering it impossible for Alice to foresee whether they will acquire vertical or horizontal polarization.

Secondly, any interception attempt by Eve disrupts these correlations in a manner that Alice and Bob can readily detect. Comparable to the BB84 protocol, this scheme involves a private measurement procedure, which precedes the identification of Eve's potential presence.

In the Ekert's protocol the source, in which Alice and Bob have access to, distributes entangled pair of qubits among them, states of the form:

$$|\Psi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The scheme uses two different basis $\oplus=\{|0\rangle,|1\rangle\}\oplus=\{|0\rangle,|1\rangle\}$ and $\otimes=\{|+\rangle,|-\rangle\}$



Received Photons	$\|1\rangle\,\|-\rangle$	$\|1\rangle\,\|-\rangle$	$\|0\rangle\,\|-\rangle$	$\|1\rangle\,\|+\rangle$
Alice's Basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$
Alice's measurements	1	0	0	1
Received Photons	$\|1\rangle\,\|+\rangle$	$\|0\rangle\,\|-\rangle$	$\|0\rangle\,\|+\rangle$	$\|0\rangle\,\|+\rangle$
Bob's Basis	$\otimes$	$\otimes$	$\otimes$	$\otimes$
Bob's measurements	1	0	1	1
Key		0		1

Table 3. ***Implementation of E91 protocol***

Similarly to BB84, the protocol involves a private measurement protocol before detecting the presence of Eve.

2.1.3 SARG04 (2004)

SARG04 is developed by changing the information encoding at BB84, to become more robust against the photon-number-splitting (PNS) attacks. The first phase of the SARG04 protocol is exactly the same with BB84's first phase. The two protocols differ in the classical sifting procedure.

At the second phase, Alice does not announce the bases she uses to encode the bits. She chooses a pair of non-orthogonal states for every qubit she sends and she announces the two states, noticing which is the right one. Bob knows that the qubit he received was in one of the two states that Alice has announced. So, to learn the secret bit Bob must have enough to distinguish between the two states. Bob makes the measurement and if his measurement is in accordance with the announced states, announce that the bit is invalid.

This is because Bob cannot determine which of the two states is the correct one. If one of the states is inconsistent with his measurement, Bob announces the bit to be valid, as he can retrieve the secret key bit.

Considering that In the SARG04 protocol we have four sets:

$a_1 = (|0\rangle,|+\rangle)$, $a_2 = (|0\rangle,|-\rangle)$, $a_3 = (|1\rangle,|+\rangle)$ and $a_4 = (|1\rangle,|-\rangle)$.

Example

Let’s give an example:

Alice sends the state |0⟩|0⟩ with two photon pulses in the randomly selected set.

Alice reveals the set a_1 =(|0⟩,|+⟩) and notes 0 as the secret bit.

If Bob measures the state in the base ⊕={|0⟩,|1⟩}, the possible result is |0⟩, so this result is consistent with the state |0⟩. Due to the fact that this outcome is also possible if the transmitted state had been |1⟩, Bob announces the bit invalid.

If Bob measures the state in the ⊗={|+⟩,|−⟩}base then he obtains |1⟩ or |−⟩ with probability ⅕ . If his result is |1⟩ it is consistent with both states and if is |−⟩, Bob is certain that Alice's state is |0⟩since this result can never be obtained from the state |1⟩. Then, Bob knows that the secret bit is 0 and announces the bit is valid.

In this example, Eve gets |0⟩ using the ⊕={|0⟩,|1⟩} base and measures |+⟩ or |−⟩ with ½ probability. So, she cannot determine the state from her measurement's result in two-photon pulses. The advantage of the SARG04 protocol over the BB84 protocol is that the sender, Alice, never announces her encoding bases. So, the fraudulent user, Eve, has to store more photons to obtain reliable information about the secret bits, and this is more possible for her to be detected.

2.1.4 B92 Protocol

In 1992 Charles Bennett presented a new Quantum Key Distribution protocol, named by his surname and the year that was published. This protocol is essentially a variant of the BB84 protocol, with the main difference that the B92 uses two states of polarization, instead of four that are being used in the BB84 protocol. It is a two non-orthogonal quantum state protocol and with its architecture an eavesdropper can be detected.

B92 is a QKD scheme that uses polarized photons for the communication of two parties, Alice and Bob, through two channels. One classical public channel, where a fraudulent user can have access and one quantum channel. As BB84, B92 protocol has two phases, the quantum transmission that takes place into the quantum channel, and the second phase that takes place into the classical channel.

2.2 THREATS AND ATTACKS

Quantum Key Distribution is considered to be a procedure of generating and exchanging keys that is secure, as it is based on the laws of Quantum Physics. For the first QKD protocol, the BB84, proved to be secure by its creators against certain attacks and since then several proofs of security have been presented. The issue of Quantum Key Distribution security is of major importance and is an object of research. Although the protocols are designed to be unbreakable, from theory to practice there are some loopholes.

Due to imperfections in the creation of photons as well as in their measurement and generally imperfections in the quantum system hardware, there are many ways to perform attacks against QKD protocols. There are also some limitations in the single photon detectors or weak points in their optoelectronic interfaces. So, a fraudulent user exploits all these above and develops strategies to extract information in a communication channel.

2.2.1 Photon Number Split

Many times new protocols are proposed with the hope to be more secure and robust against certain attacks, as for example SARG04 was proposed as a stronger variation of BB84 against Photon Number Split (PNS) attacks. PNS attack exploits imperfections and weaknesses in the experimental implementation of Quantum Key Distribution protocols.

When Alice sends her photons to Bob with weak laser pulses, Eve splits off a signal photon and lets the remaining signal pass to Bob. Then, Eve waits for Alice to reveal the basis she used for each signal and therefore measures the photon she obtains and extracts information about the encoded bits and the secret key . Since the attack is performed without errors, Eve will not be detected, if we assume that the receiver, Bob, has no access to the statistics of photons he receives.

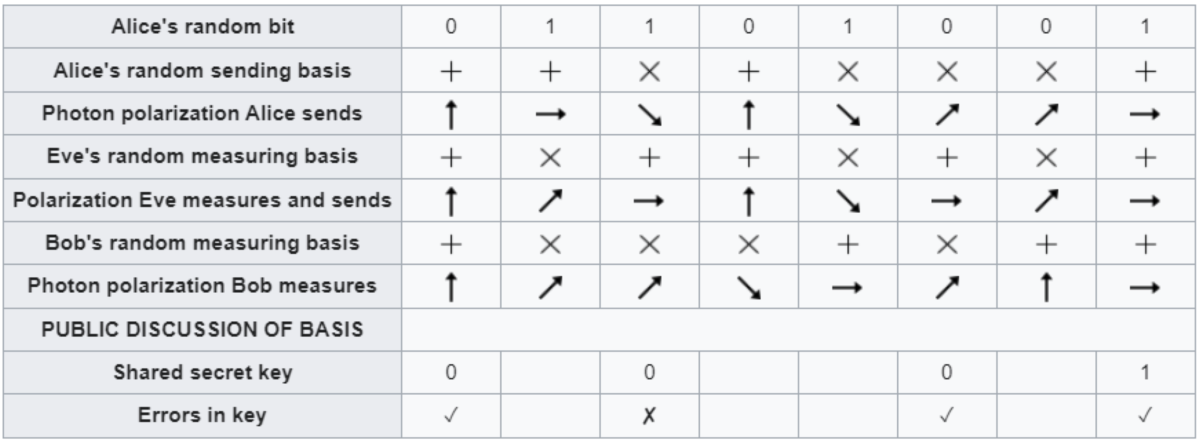
Two effective methods against the PNS attack is the SARG04 protocol and a strategy known as decoy states where the eavesdropper is detected as it uses a few different photon intensities.

2.2.2 Intercept and resend

The simplest type of possible attack is the intercept-resend attack, where Eve measures the quantum states (photons) sent by Alice and then sends replacement states to Bob, prepared in the state she measures.

In the BB84 protocol, this produces errors in the key Alice and Bob share. As Eve has no knowledge of the basis a state sent by Alice is encoded in, she can only guess which basis to measure in, in the same way as Bob. If she chooses correctly, she measures the correct photon polarization state as sent by Alice, and resends the correct state to Bob.

However, if she chooses incorrectly, the state she measures is random, and the state sent to Bob cannot be the same as the state sent by Alice. If Bob then measures this state in the same basis Alice sent, he too gets a random result—as Eve has sent him a state in the opposite basis—with a 50% chance of an erroneous result (instead of the correct result he would get without the presence of Eve). The table below shows an example of this type of attack.



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

Table 4. ***Example of Intercept and resend attack***

The probability Eve chooses the incorrect basis is 50% (assuming Alice chooses randomly), and if Bob measures this intercepted photon in the basis Alice sent he gets a random result, i.e., an incorrect result with probability of 50%. The probability an intercepted photon generates an error in the key string is then 50% × 50% = 25%. If Alice and Bob publicly compare *n* of their key bits (thus discarding them as key bits, as they are no longer secret) the probability they find disagreement and identify the presence of Eve is:

$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

So to detect an eavesdropper with probability $P_d = 0.999999999$ Alice and Bob need to compare *n* = 72 key bits.

2.2.3 Man in the Middle

Quantum key distribution faces a comparable vulnerability to man-in-the-middle attacks as classical protocols when deployed without proper authentication. This is because quantum mechanics lacks any inherent capability to differentiate between trusted entities and potential adversaries. Just like in classical scenarios, establishing a secure connection between Alice and Bob necessitates a mechanism for confirming each other's identities, typically achieved through an initial shared secret.

In the presence of an initial shared secret, Alice and Bob can employ an authentication scheme with unconditional security, such as the Carter-Wegman method, in conjunction with quantum key distribution. This combined approach enables them to exponentially expand their shared key while utilizing a fraction of the newly generated key for mutual authentication in subsequent sessions.

Various techniques have been proposed to create this initial shared secret, including involving a third party or harnessing the unpredictability of chaos theory. However, it's crucial to note that only hash functions falling under the category of "almost strongly universal" are suitable for ensuring unconditional security in the authentication process.

Conclusion

In conclusion, this paper has explored Quantum Key Exchange (QKE), with a primary focus on the BB84 and E91 protocols, while also addressing potential vulnerabilities such as photon number split, man-in-the-middle, and intercept-and-resend attacks.

QKE presents an intriguing avenue for secure communication, leveraging the principles of quantum mechanics to generate encryption keys that are theoretically impervious to emerging computational threats, including quantum computers. However, it is essential to maintain a vigilant and balanced perspective.

While QKE offers a promising path forward in the pursuit of enhanced data security, it is not immune to challenges and potential attacks. Recognizing these vulnerabilities underscores the need for comprehensive authentication and verification measures in real-world implementations.

In a landscape where data security is paramount, Quantum Key Exchange remains a subject of ongoing research and development, offering a potential solution to the evolving demands of secure communication. Achieving this promise will require continued exploration, refinement, and thoughtful consideration of its practical applications and limitations.

Sources

Quantum Key Distribution: Basic Protocols and Threats

0.1 Ekert protocol for quantum key distribution

Quantum Key Distribution in the Classical Authenticated Key Exchange Framework | SpringerLink

Quantum cryptography based on Bell's theorem

The flowchart of BB84 Quantum Key Distribution Protocol steps. | Download Scientific Diagram

https://arxiv.org/pdf/2212.13089.pdf

Post-processing procedure for industrial quantum key distribution systems

Quantum Key Dance: How BB84 and E91 Keep Information Safe

Lecture 12: Quantum key distribution. Secret key. BB84, E91 and B92 protocols. Continuous-variable protocols. 1. Secret

Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications - PMC

Fundamentals of Quantum Key Distribution — BB84, B92 & E91 protocols