ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

# Effective Quantum Key Authentication in Optical Networks

[1]G. Venkateswarlu, [2]G. Murali
[1,2]Dept of CSE, JNTUACEP, Andhra Pradesh, India

**Abstract**

Secure distribution of the secret random bit sequences known as "key" material is an essential precursor to their use for the encryption and decryption of confidential communications. Quantum cryptography is a new technique for secure key distribution with single-photon transmissions: Heisenberg's uncertainty principle ensures that an adversary can neither successfully tap the key transmissions, nor avoid detection (Eavesdropping raises the key error rate above a threshold value). We have developed experimental quantum cryptography systems based on the transmission of non-orthogonal photon states to generate shared key material over multi-kilometer optical fiber paths and over line-of-sight links.

**Keywords**

Authentication, Classical Post Processing, Error Correction, Optical Networks, Privacy Amplification, Quantum Key, Shifting, Security Loop Holes in QKD

## I. Introduction

The main goals of cryptography are the encryption of messages to deliver them unintelligible to third parties and their authentication to certify that they have not been modified. These goals can be accomplished if the sender ("Alice") and recipient ("Bob") both possess a secret random bit sequence known as "key" material, which they use as a parameter in a cryptographic algorithm. It is essential that Alice and Bob acquire the key material with a high level eavesdropper of confidence that any third party ("Eavesdropper") does not have eavesdropper partial information about the random bit sequence. If Alice and Bob communicate solely through classical messages it is impossible for them to generate a certifiably secret key outstanding to the possibility of passive eavesdropping. How eavesdropper secure key distribution becomes possible if they use the single-photon communication technique of quantum cryptography, or more accurately quantum key distribution (QKD). The security of QKD is based on the inviolability of the laws of quantum mechanics and provably secure (information theoretic) data handling protocols. Eavesdropper can neither "tap" the key transmissions to the indivisibility of quantum nor copy them because of the quantum "no-cloning" theorem. QKD was potentially practical by constructing a working prototype system for the BB84 protocol, using polarized photons. In 1992 Bennett published a "minimal" QKD scheme ("B92") and proposed that it could be implemented using single-photon interference with photons propagating for long distances over optical fibers. QKD is also possible using line-of-sight transmissions in free space, we have developed a free-space QKD system for such applications and have achieved a transmission distance of one km at night and more recently, half km in daylight implementation of quantum cryptography in optical fibers and the performance of our system.

## II. Related Work

To understand QKD we must first move away from the conventional key distribution metaphor of Alice sending particular key data to Bob. Instead, we should have in mind a more symmetrical starting point in which Alice and Bob initially generate their own secret independent random binary number sequences containing more bits than they need for the key material that they will ultimately share. They will perform a bit-wise comparison of these sequences of numbers to identify a shared random subset, which will become the key material, using quantum transmissions over a quantum channel and a discussion of the results over a conventional public channel. It is important to appreciate that Alice and Bob do not need to identify all of their shared numbers or even particular ones because the only requirements on the key material are that the numbers should be secret and random. For simplicity we will first describe the minimal B92 QKD protocol in terms of the preparation and measurement of single-photon polarization states. Alice and Bob first agree through public discussion on how to implement the B92 protocol, For example they can agree that Alice will transmit photons to Bob with either of two non-orthogonal polarizations: vertical polarization ("V") or +45° linear polarization, say. On the photons he receives, Bob can make either of two non orthogonal polarization measurements, each of which is orthogonal to one of Alice's: -45° linear polarization or horizontal polarization ("H"), in this case. The second step of the protocol is for Alice and Bob to generate independent secret sequences of random binary numbers. They proceed through their sequence bit-by-bit in synchronization with Alice preparing a polarized photon for each of her bits according to the rules sending it over the "quantum channel" to Bob (The quantum channel is a transmission medium that isolates the quantum state from interactions with the "environment.") Bob makes a polarization measurement on each photon he receives, according to the value of his bit as given by: records the result ("pass" = Y, "fail" = N). Note that Bob will never record a "pass" if his bit is different from Alice's, and that he records a "pass" on a random 50% portion of the bits that they have in common. Alice and Bob need a short, secret authentication key to start the QKD procedure, and can replenish this key with a small portion of the QKD material generated. For authentication based on random hashing they will need O (log2n) secret authentication bits for every n-bit public transmission. So from the foregoing, we see that a QKD procedure may be broken down into the following seven stages:

1. Alice and Bob acquire a secret authentication key;
2. [Alice and Bob generate independent secret sequences of random bits;
3. Alice and Bob use the quantum transmissions of a QKD protocol to compare their sequences and classical communications to identify a random sub-sequence of shared secret bits;
4. Alice and Bob perform an error correction procedure on the data;
5. Alice and Bob assess (from the error rate) how much knowledge eavesdropper may have acquired;
6. Alice and Bob perform an appropriate privacy amplification procedure over the public channel;
7. Part of the resulting key material is used to replenish the authentication bits required in step one. So that the system is ready for the next key generation session, the inventors of QKD proposed that the key bits should be used for the encryption of communications using the unbreakable "one-time pad" method. How eavesdropper, the key material could equally well be used

by Alice and Bob in any other symmetric key cryptosystem. For example, they could use a short string of their key bits (a few hundred bits) as an input "seed" to a cryptographically secure random number generator whose output would provide many secure bits for use in subsequent encryption. Typically, there would know more effective method for eavesdropper to attack this system than to exhaustively search all possible key strings, which would be computationally infeasible. Of the steps above, only one (step 3) involves the experimental physics issues that will be crucial to the practical feasibility of QKD. In our work we have therefore focused our efforts on this component of QKD. A fully functional key generation system would include careful implementation of the other steps, but these (with the exception of step 5) are better understood and may be readily incorporated once step three has been adequately demonstrated. Step five relates to the physics of eavesdropping and a full treatment of this topic is beyond the scope of this paper. We will therefore limit ourselves to a few additional remarks on this subject. In the simple form described above, the B92 protocol is vulnerable to eavesdropper measuring Alice's photons in Bob's basis and only sending on those photons she can identify. (This "Bob's basis" attack would allow Eavesdropper to "force" a key onto Bob because Bob only detects photons for which he and Alice have the same bit value.) This will cause a factor of four reduction bit rate unless eavesdropper sends out multiple photons instead of just one. In the original B92 paper Bennett proposed a solution to this problem using an interferometric scheme is very similar to the one we have implemented in our fiber experiments. Alice and Bob could also protect against this type of attack by Bob having multiple detectors to detect for multi-photon pulses, or they could use the BB84 protocol which does not have this potential vulnerability.

## III. Quantum Key Distribution

In the BB84 protocol Alice generates two random bits for each photon she sends to Bob. The first bit determines which of two conjugate bases she will use for the transmission, either (H, V) or (+45°, -45°), say. The second random bit determines whether she sends a "0" or a "1", with (0, 1) = (H, V) in the first basis, or (0, 1) = (+45°, -45°) in the other basis. For each incoming photon Bob generates one random bit, which determines his measurement basis: either (H, V) or (+45°, -45°). He records whether or not a photon arrived and its polarization: H or V, or +45° or -45° depending on his basis choice. Bob then communicates to Alice over the public channel the locations in the photon transmission sequence where he detected photons (but not the polarization he found) and his choice of basis in each case notice that in BB84 in contrast to B92 Bob may incorrectly identify the bit value of a detected photon because he and Alice were using different bases. The protocol is completed with Alice informing Bob over the public channel to retain only those detected bits for which they used the same basis, the sub-sequence of bits for which Bob detected a photon and they used the same basis are perfectly correlated. Alice and Bob use this sub-sequence as their key because Alice and Bob only select the "correct basis" bits after Bob has detected Alice's photons, Eve has no possibility of performing a "Bob's basis" attack. The BB84 protocol is twice as efficient as B92 per transmitted photon. From the perspective of the physics involved B92 and BB84 are so similar that demonstration of one protocol indicates that the other will also be possible under the same physical conditions. For QKD, Alice and Bob share two communication channels: a quantum channel that is used to transmit qubits (Quantum bits) and a classical (standard) channel to send classical messages. The quantum channel is generally an optical fiber or a free-space link connecting Alice and Bob, while the classical channel may be the Internet.

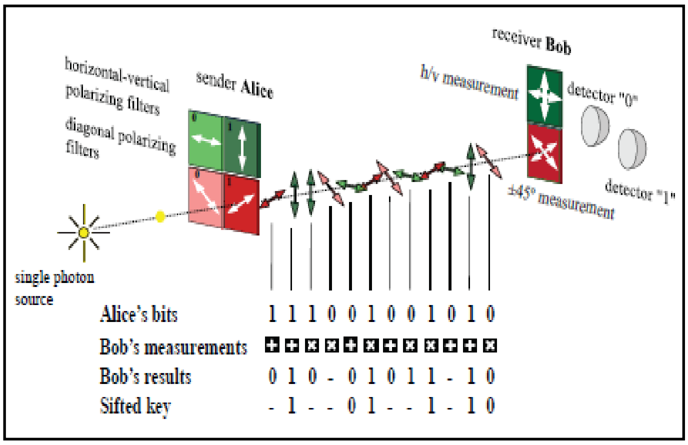
horizontal-vertical polarizing filters
diagonal polarizing filters
sender Alice
0
1
0
1
single photon source
receiver Bob
h/v measurement
detector "0"
±45° measurement
detector "1"
Alice's bits 1 1 1 0 0 1 0 0 1 0 1 0
Bob's measurements + + × × + × + × × + + ×
Bob's results 0 1 0 - 0 1 0 1 1 - 1 0
Sifted key - 1 - - 0 1 - - 1 - 1 0

Fig. 1: Illustration of the BB84 Protocol

Quantum key distribution was proposed in 1984 by Charles Bennett and Gilles Brassard the first QKD protocol, generally referred to as the BB84 or four-state protocol, uses four different quantum states that form two pairs, chosen such that, This property is sometimes also referred to as unconditional security, a technical term that refers to the fact that the security is not based on mathematical assumptions. This meaning must not be confused with secure without any conditions. The difference (overlap) between any two states, one from each pair, is the same. A specific bit value is assigned to each state.

## IV. Classical Post-Processing

Classical post-processing in QKD consists of four operations, as shown in fig. 2.

### A. Sifting

Alice and Bob start by performing key sifting: Bob communicates which photons he detected, and which measurements he performed in these cases. However, he does not specify the results he obtained. Alice and Bob only keep those bits from their raw keys where Bob detected a photon, and that resulted from correct measurements (as defined above). All other bits are discarded. The result of this step is called the sifted key. Ideally, the sifted key would be error 4 we use the usual ket-notation to denote quantum states. e.g. |ψ> denotes the quantum state ψ5 Note that other, more sophisticated eavesdropping strategies exist. However, regardless of the strategy, an eavesdropper gaining information about the photon states inevitably introduces errors at Bob's. See, but in practice, no communication system is perfect and thus a small error rate, generally referred to as the quantum bit error rate (QBER), always remains. In addition, errors introduced by eavesdropping may also be present in the sifted key.

### B. Error-Correction

The next step is to perform error correction: Alice sends Bob additional information that allows him to generate an error-corrected key that is identical to Alice's. Furthermore, this procedure yields the QBER. Error correction in QKD is similar to error correction in classical communications, with the sifted key in QKD being analogous to the transmitted message. However, there is one important difference: rather than combining information that allows correcting errors directly into the message to be transmitted, this information is sent after key sifting is complete as it is only at this point that the message to be corrected is known. Furthermore, we need not worry about protecting the information for error correction against transmission errors as we can use existing protocols that provide error-free communication. With this in mind, the Cascade error correction protocol was originally designed for QKD. It requires many rounds of back-and-forth communication between Alice and Bob, which limits the maximum key rates that can be handled, due to communication delays. More recently, Low-Density Parity-Check codes have been adapted from classical communication protocols – they are capable of handling larger key rate.

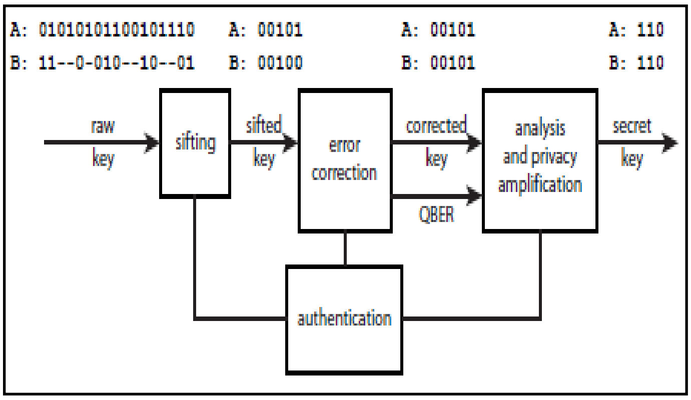

Fig. 2: Post-Processing in QKD. Example Keys for Alice (A) and Bob (B) are Shown

Only key bits resulting from correct measurements and photon detections are kept during sifting, yielding the sifted key. Remaining errors are corrected to form the error-corrected key. The eavesdropper's information about the error-corrected key is removed, yielding the secret key. Authentication is required for all steps.

### C. Privacy Amplification

The amount of information that an eavesdropper may have obtained is estimated. The analysis considers several factors:

1. First, the maximum amount of information Eve may have gained from measuring photons in transit. It is evaluated from the error rate introduced into the sifted key. Generally, all errors are attributed to eavesdropping as this is the worst-case scenario. If QKD is implemented using extremely faint laser pulses (containing on average less than one photon) instead of single photons, this procedure has to take into account the possibility of a so-called photon number splitting (PNS) attack. This attack exploits the fact that faint laser pulses sometimes contain more than one photon. It is generally thwarted by adding decoy states qubits encoded into faint pulses with 340 Femtosecond-Scale Optics Quantum Key Distribution different mean photon number to the signals used to establish the sifted key. This allows determining the information gained by the eavesdropper from PNS attacks, and makes implementations using faint laser pulses comparable to those using (much more difficult to generate) single photons.
2. Second, the eavesdropper gains additional information by monitoring the error-correction procedure. The amount, Iec, is directly given by the number of bits exchanged.
3. Third, as we will discuss in more detail later, an implementation of QKD using imperfect devices can impact the security of the protocol. Sometimes, it is possible to quantify the information leakage Ileak Using these three contributions, the length of the secret key to be distilled from the corrected key is computed. Assuming for simplicity that Alice has used true single photons6, the secret key per error-corrected bit amounts to privacy amplification, implemented by both Alice and Bob, then maps the error-corrected keys onto shorter secret keys in a way that knowledge of many bits in the corrected key is required to calculate any bit of the secret key.

$$Isecret = 1 - It - Iec - Ileak \qquad (1)$$

This step is typically performed by multiplication of the corrected key (expressed as a bit vector) with a suitably chosen binary Toeplitz matrix. This removes the eavesdropper's information about the key.

### D. Authentication

An important consideration in all post-processing steps is to ensure that Alice and Bob are in fact going through this process with each other. Otherwise, an eavesdropper could simply block all quantum and classical communication between Alice and Bob and perform QKD with Alice while taking on Bob's role and vice versa. This is known as a man-in-the-middle attack, and would allow Eve to establish different secret keys with both Alice and Bob. She could then intercept a secret message, for example, being sent from Alice to Bob, decrypt it using the key she shares with Alice, read it, and then encrypt it again using the key she shares with Bob before forwarding it to him. She could thus read the entire message. To avoid man-in-the middle attacks, the classical channel has to be authenticated. In other words, Alice and Bob have to identify each message they send as originating from themselves. This can be achieved using a protocol known as Wegman-Carter authentication. Hence, while the eavesdropper can listen to the conversation during post-processing, she cannot modify or replace it. Authentication requires a short initial key, which is consumed during the first round of QKD.

## V. Security Loopholes in QKD

As introduced above, eavesdropping qubits encoded into individual photons during transmission is revealed through the observed error rate, regardless of the strategy. However, loopholes in the actual implementation of QKD may exist and can be exploited for attacks that are not reflected in the QBER. This was already noted in the very first implementation of QKD, where Charles Bennett realized that the noise emitted by the QKD system rendered the key only secure against an eavesdropper who happened to be deaf.

Quantum hacking has become an important research field during the past five years, and various attacks have been proposed and experimentally studied. The most important one is briefly introduced below.

1. The already mentioned photon number splitting attack takes advantage of the fact that faint laser pulses sometimes contain more than one photon. This opens a security loophole when using the original BB84 protocol. Interestingly, this loophole can be closed by a small modification of the protocol, i.e. the addition of decoy states.
2. In the Trojan-horse attack, Eve exploits the fact that every optical element reflects some of the incident light. It is then possible to analyze the status of optical components such as phase (polarization) modulators by reflecting short pulses of light from them, yielding for instance information about the qubit state that is being generated. This technique is called reflectometry and is well known to optical engineers. Counter measures include active monitoring of light at the input of Alice and Bob, and, for Alice, an optical isolator.
3. QKD systems rely on single photon detectors. In the detector blinding attack, an eavesdropper exploits that these detectors can

be prevented from detecting photons, and then forced to announce detections at will using various mechanisms. In the time-shift attack the eavesdropper exploits a possible detection efficiency mismatch between two detectors in the time domain. In this case, controlling the arrival time of each photon at Bob's device allows the eavesdropper to modify the probabilities for certain detectors to detect a given photon, and thereby yields information about the key. Counter measures against attacks exploiting vulnerabilities of single photon detectors, often combining hardware and protocol modifications have already been proposed and investigated. It is of utmost importance to critically assess vulnerabilities of QKD systems and devise counter measures, either of theoretical or on the technological level, to remove the threat to security. Yet, even in the case of remaining potential loopholes, one should not underestimate that the security of QKD depends on the technological capabilities of the adversary at the time of the key exchange, in contrast to complexity-based cryptosystems that generate cipher texts that can be recorded and decoded later. This point is important for secrets that should remain secure over many years. QKD system it is important to distinguish between attacks that are possible with existing technology, which are limited to individual bit attacks, and potential future attacks that are limited only by the laws of physics. In particular, all current QKD experiments use approximate single-photon states that are obtained by attenuating the output of a pulsed laser so that he average photon number per pulse is less than one. Such pulses contain a poison distribution of photon numbers, and the low intensity is necessary to ensure that very few pulses are vulnerable to an eavesdropper using an optical beam splitter to "tap out" a photon from pulses containing more than one photon. In our experiment 28% of the detectable laser pulses leaving Alice's interferometer contain two or more photons because we operate at an average photon number per pulse of 0.63. This is a considerably higher fraction of multi-photon pulses than in our free-space QKD system where only 6% of the detectable pulses contain two or more photons (an average photon number per pulse of 0.1). Nevertheless, even with this large multi-photon pulse probability our optical fiber QKD system could be made secure against beam splitting and other single-bit attacks by appropriate use of privacy amplification.

## References

[1] Muralikrishna Gandluru,"Optical Networking and Dense Wavelength Division Multiplexing (DWDM)", [Online] Available: http://www.gandluru@cis.ohio-state.edu.

[2] Richard J. Hughes, George L. Morgan, C. Glen Peterson, "Practical Quantum key Distribution over a 48-km Optical Fiber Network", Physics Division Los Alamos National, Laboratory, Los Alamos, NM 87545.

[3] Philip Chan, Itze Lucio-Martínez, Xiaofan Mo, Wolfgang Tittel, "Quantum Key Distribution".

[4] Valerio Scarani, Antonio Ac´ıny Gregoire Ribordy, Nicolas Gisin, "Quantum cryptography protocols robust against photon number splitting attacks", Group of Applied Physics, University of Geneva 20, rue de l'Ecole-de-M´edecine, 1211 Gen`eve 4, Switzerland 2 Institut de Ci`encies Fot`oniques Jordi Girona 29, 08034 Barcelona, Spain

[5] Nur Atiqah Muhammad,"Implementation of BB84 Quantum Key Distribution Protocol's with Attacks", Department of Communication Technology and Network Faculty of Computer Science and Technology, UPM Selangor, Malaysia Zuriati Ahmad Zu karnain Department of Communication Technology and Network Faculty of Computer Science and Technology, UPM Selangor, Malaysia.

[6] Sheila Cobourne,"Quantum Key Distribution Protocols and Applications".