# The QKD (Quantum Key Distribution) Application in Cyber Security

**Sorin SOVIANY, Cristina – Gabriela GHEORGHE**
National Institute for Research and Development in Informatics - ICI Bucharest
sorin.soviany@ici.ro, cristina.gheorghe@ici.ro

**Abstract:** This paper makes a review of Quantum Key Distribution (QKD) protocols and focuses on their application in Cyber Security. The research work presents the results of some QKD simulations for both categories of protocols: single-photon protocols (based on Heisenberg's uncertainty principle and the polarization state for a single photon) and entanglement-based protocols (based on entangled photon pairs). The simulations depict the secret key generation process. The reliability of the overall process strongly depends on the number of measurements. The QKD protocols represent a reliable approach to complete the conventional Cyber Security systems with use-cases requiring the reliable detection of the passive attacks.
**Keywords:** Quantum Key Distribution, entanglement, passive attacks, Cyber Security.

## INTRODUCTION

The QKD (Quantum Key Distribution) protocols were designed based on quantum mechanics principles as a reliable way to secure the secret key exchange in cryptographic systems. The initial QKD design goal was focused on point-to-point cases, but later the scientific and practical interest extended to multi-point design cases leading to quantum networks with multi-hop paths between the transmitter and the receiver.

The QKD protocols allow to properly address the main limitations of the conventional security mechanisms. These limitations have a major impact on the data confidentiality protection cryptographic function and its performance vs. complexity optimal trade-off, as following:

- the high dependency between the security degree and the power of the conventional cryptographic mechanisms (computational-conditioned cryptography);
- a reduced efficiency concerning the application-level performance, Quality of Services (QoS), overhead and timing;
- the vulnerability of the conventional systems and their communications support to passive attacks (eavesdropping). The passive attacks cannot be efficiently detected using conventional security systems like cryptographic mechanisms, intrusion detection systems (IDS), firewalls or Virtual Private Networks (VPN). The passive attacks usually do not change the message or stream

https://doi.org/10.54851/v5i2y202309

integrity and/or sequencing and there are no signs or patterns to be recognized by the conventional security systems, in order to prevent or to block the malicious actions. However, the passive attacks can be very dangerous because a cryptanalyst could extract useful information for the intended purposes even from the best cryptograms. The extracted information could be correlated with other contextual data allowing to get the original message contain.

The security of the conventional cryptographic systems is constrained by the computational complexity of the underlying cryptographic mechanisms with respect to the available resources of the attacker (time, processing and storage). The attacker can assume a certain difficulty in his efforts to break a conventional cryptosystem. The increased complexity of the security function based on computational cryptography rises additional issues concerning the overhead and execution time. These issues have a negative impact on the application performances as expected by design.

These issues justify the increasing interest for cryptographic mechanism based on quantum principles and especially for QKD protocols. QKD is a reliable solution addressing the problem of securing the secret cryptographic keys exchanges for symmetric cryptosystems. QKD application can properly handle the cases of passive attacks detection, especially if using entanglement-based protocols.

The remainder of the paper is structured as following. Section II makes a brief overview of the actual QKD protocols development and presents the categories of QKD protocols with corresponding examples and their simulation, showing the secret key generation process using QKD protocols belonging to both categories: single-photon and quantum entanglement-based protocols, respectively. Section III concludes this research work and proposes some further research directions in this field, both theoretical and applicative ones.

## OVERVIEW OF QKD PROTOCOLS

### Short history of the QKD protocols

Table 1 contains a list of the most important QKD protocols in their chronological development and introduction. The authors and a short description are provided. The basic protocols are BB84 and E91. The other protocols are derived from the basic ones.

***Table 1.*** *QKD Protocols (Wikipedia, n.d.)*

| Name | Year of appearance | Short description |
|---|---|---|
| BB84 | 1984 | Quantum Key Distribution scheme created by Charles Bennett and Gilles Brassard. First quantum cryptography protocol |
| E91 | 1991 | Quantum cryptography method known as Arthur Eckert scheme |
| BBM92 | 1992 | Quantum Key Distribution Method developed by Charles Bennett, Gilles Brassard and N. David Mermin |
| B92 | 1992 | Quantum Key Distribution method invented by Charles Bennett |
| MSZ96 | 1996 | Quantum Key Distribution protocol |
| SSP | 1998 | Quantum Key Distribution method version of BB84 that uses six-state polarization scheme created by Pasquinucci and Gisin |

| | | |
|---|---|---|
| DPS | 2002 | Quantum Key Distribution method proposed by Kyo Inoue |
| Decoy state | 2003 | Quantum Key Distribution method created by Hwang and Co. |
| SARG04 | 2004 | Quantum Key Distribution protocol (more robust than BB84) developed by Scarani, Acin, Ribordy and Gisin |
| COW | 2005 | Quantum Key Distribution protocol, named Coherent One – Way Protocol |
| Three-Stage Quantum Cryptography | 2006 | Quantum cryptography protocol known as Kak's three stage protocol |
| KMB09 | 2009 | Quantum Key Distribution protocol named after Muhammad Mubashir Khan, Michael Murphy and Almut Beige |
| HDQKD | Developed in the 2020s | Technology for secure communication between two entities, named High-Dimensional Quantum Key Distribution |
| T12 | | Quantum Key Distribution protocol proposed by Lucamarini |
| S09 | | Created by Eduin Esteban Hernandez Serna. It uses private and public key encryption |

## Evolution of the QKD protocols

The first quantum cryptography protocol, called BB84, was created in 1984 by Charles Bennet and Gilles Brassard. The cryptography scheme is based on the polarization state of a single particle. A user sends series of photons characterized by random polarizations and thus suggests a key (Dhanaraj, 2022). In 1991, Eckert proposed the E91 protocol based on the polarized state of entangled photons. Then, in 1992, an improvement of this scheme was proposed by introducing the BBM92 protocol. The new scheme was introduced by Charles Bennett, Gilles Brassard and N. David Mermin. The B92 protocol was invented by Charles Bennett in 1992. This protocol uses only two states of the photon (one in H polarization and one in +45º polarization), unlike BB84 protocol with four states. In 1996, the MSZ96 protocol was introduced, which works on the basis of four non-orthogonal quantum states. In this protocol, photon polarization as in BB84 and entangled photons as in E91 are not required. The SSP (Six-State Protocol), created by Pasquinucci and Gisin, in 1998, is based on a six-state polarization scheme. In 2002, Kyo Inoue proposed the DPS (Differential Phase Shift) protocol which was then tested on two non-orthogonal states. Then, in 2003, Hwang and Co. introduced the Decoy State Protocol. In this scheme, the "decoy" pulses are added to photon pulses. Scarani, Acin, Ribordy and Gisin developed, in 2004, a new protocol which was called SARG04. In this protocol, the four states of polarization, used in BB84, were encrypted with unique data. In 2005, in the frame of COW (Coherent One-Way) protocol an interferometer is built on the additional observing line, which is used for detection of an attack from a secret agent. The Three-Stage Quantum Cryptography Protocol was originally proposed in 2006 and then it was realized in 2012. This protocol is based on asymmetric cryptography. Several photons are used for an improved data transfer between the sender and the receiver. In 2009, Muhammad Mubashir Khan, Michael Murphy and Almut Beige named their protocol QKD KMB09. This protocol has a high bit error rate, around 50%. The HDQKD (High-Dimensional Quantum Key Distribution) protocol uses the high-dimensional QKD algorithms. Thus, it increases the resilience of communications to noises and a higher secret key rate is achieved. The QKD protocol named T12 was proposed by Lucamarini. This protocol is secure and efficient in the situations of finite size. The S09 protocol obtained by Eduin Esteban

Hernandez Serna performs private and public key encryption. With S09, information is sent securely in an open network. The transfer of qubits can be done under any condition.

## Main categories of QKD protocols

Quantum cryptography includes the quantum-based algorithms or protocols designed and applied to secure the secret key exchange or distribution. The overall process is named Quantum Key Distribution and it addresses the main problem of the conventional cryptosystems with secret keys (symmetric cryptography): how to securely distribute a secret cryptographic key between the transmitter and receiver under the vulnerabilities of the communications channels. Quantum cryptography with QKD is based on the information encoding in individual quantum systems (like single photons or entangled pairs of photons, depending on the QKD protocol type). The security degree is provided by the quantum physics principles. Particularly the security functionality exploits by design the main properties of the involved quantum systems, as support for the information transmission process:

- Heisenberg's uncertainty principle with the polarization state of photons (support for the 1st category of *QKD protocols with single-photon schemes*);
- Entangled photons properties (support for the 2nd category of *QKD protocols* that basically exploit *the quantum entanglement property*).

In this way, the security should not depend on the computational complexity of the attacker's actions. However, the practical implementation of QKD protocols requires additional and dedicated devices that may have their own potential weakness. The QKD protocols design and implementation for real application use-cases should not depend on a certain device. On the other hand, it seems that an increased security can be achieved with the cost of a lower key generation rate. This requires and justifies the actual efforts towards a proper trade-off, allowing to provide a given trust level for certain devices and ensuring an optimal key generation rate with respect to the end-user's expectations.

The QKD protocols can be classified according to several criteria. Firstly, depending on the type of the involved variables, one can distinguish between two categories of QKD protocols (Quantum Computing, 2022), (Babeș-Bolyai University, 2022):

- *QKD protocols with discrete variables (DV-QKD)*, in which the quantum information is encoded using a photons detector to properly measure the quantum states. The measurement outputs come from a finite set and the protocol works with a finite dimensional Hilbert space (like a qubit). In DV-QKD, single photons are sent through the channel and this process is conducted one at a time. The encoded quantum state is the polarization state of the photon;
- *QKD protocols with continuous variables (CV-QKD)*, in which the protocol makes use of an infinite dimensional system and, therefore, there is a continuum of measurement outcomes. In this case, a continuous beam of light is sent, as in the optical communication systems. The information encoding can be performed by modulating the amplitude and phase of the electromagnetic wave.

The 1st QKD protocols belong to the DV-QKD category, like BB84. These protocols were defined and introduced in the 1980s and 1990s, while CV-QKD protocols were specified later, in the 2000s (Quantum Computing, 2022). From the design and operation principles, the QKD protocols belong to the following main categories (Haitjema, 2007):

- *QKD protocols based on Heisenberg's uncertainty principle;*
- *QKD protocols based on Quantum Entanglement.*

## Heisenberg principle-based QKD protocols

### *a) BB84 Protocol*

The 1st QKD protocol was proposed and developed by Charles Bennet and Gilles Brassard in 1984 (BB84). This protocol is based

on the Heisenberg's uncertainty principle and the individual photons polarization state. This protocol still has a sufficient degree of robustness and reliability, allowing to be applied and integrated in many security systems and requiring to securely exchange the secret cryptographic keys. The actual implementations of the BB84 protocol follow the original version or some enhanced versions that were developed later (Anghel, 2012). This protocol enables the two communicating entities needed for secured data communications to establish a secret shared key using polarized photons. The QKD implementation with BB84 protocol makes use of the photon's polarization state with linear and diagonal bases. A basis contains a pair of orthogonal states. Table 2 presents the convention for association between the classic information bits and the quantum information (qubits, defined using the photon's polarization state).

***Table 2.*** *Photons polarization state and information encoding in BB84 protocol (Anghel, 2012)*

| Basis | Linear L | | Diagonal D | |
|---|---|---|---|---|
| Polarization | 0° | 90° | 45° | 135° |
| Qubit | → | ↑ | ↗ | ↖ |
| Bit | 0 | 1 | 0 | 1 |

The BB84 protocol-based quantum key distribution process is performed within the following steps:

1. The transmitter entity (named Alice) generates a random sequence of bits s;
2. The transmitter Alice randomly selects a polarization basis for each of the photons belonging to the generated sequence, resulting in a sequence of the photons polarization states *b*. The polarization basis contains a pair of orthogonal states in which each state represents a certain polarization of the photon;
3. The transmitter generates a sequence of polarized photons (qubits) *p*. The encoding of the bits belonging to the sequence s is based on the polarization of the photons belonging to the sequence *p*;
4. The qubits belonging to the sequence p are sent through the quantum channel (optical fibre) from the transmitter Alice to the receiver Bob;
5. The receiver Bob randomly selects a polarization basis for each of the qubits belonging to the received sequence $p`$. The selected polarization basis sequence is $b`$;
6. The receiver Bob measures each qubit (polarized photon) belonging to the received sequence, using the randomly selected polarization basis (step 5). Following this measurement and also using the encoding mapping among qubits, polarization state and corresponding information bits, the process generates a bit's sequence $s`$;
7. The communication process accomplished on the public channel between the transmitter Alice and the receiver Bob involves: the polarization basis chosen by the transmitter for each bit (information sent from the transmitter Alice to the receiver Bob); the elements belonging to the received qubits sequence for which the receiver selected the same polarization basis (information sent from the receiver Bob to the transmitter Alice); the removal of the bits corresponding to the photons having different polarization states, in the sequences s and $s`$;
8. The bits sequences owned by the transmitter Alice and receiver Bob are compared after their encoding and decoding, respectively. This step leads to a unique and secured shared key. Then, this generated secret key can be applied to secure the data transmission process in an unsafe channel. This is done during the following sub-steps (Anghel, 2012):
   - Secret Key (Information) Reconciliation (SKR, IR), a procedure for the errors correction within the raw key that allows to remove the errors with different sources such as: choosing different polarization basis by transmitter and receiver, respectively; noises; attackers

actions (eavesdropping). This is a binary searching process for the errors in which:
  - the generated bits sequence (raw key) is divided into separate blocks of bits;
  - the parity of each block of bit is compared;
  - if there are any parity differences at a block-level, the corresponding block is further divided into smaller sub-blocks and the parity checking is applied again.
- Privacy Amplification (PA), a security procedure allowing to reduce the amount of information an attacker is able to get about the secret key that should be shared between transmitter and receiver. The following operations are performed, in order to establish a fully secured key:
  - a permutation of the bits in the secret key;
  - removal of a bit's subset by the transmitter Alice and receiver Bob, based on some common criteria.

The security of the BB84 QKD protocol is provided by the information encoding into non-orthogonal states. According to the quantum uncertainty principle, these states cannot be measured without perturbing the original states. This protocol uses two pairs of the photon polarization states. Each state pair is conjugated to the other. Also, the states within a pair are orthogonal to each other. A polarization basis contains just the paired orthogonal states. The polarization states that are used for this protocol, according to Table 2, are: linear basis L, with vertical ($0^0$) and horizontal ($90^0$) directions, and diagonal basis D ($45^0$ and $135^0$). The simulation of BB84 protocol is performed using the simulation environment developed within the QuVis project (*Quantum Mechanics Visualisation*) conducted by St. Andrews University (n.d.). Two major simulation cases are presented, as following (see Figures 1-16, based on the St. Andrews University's simulation environment).

The 1st case is depicted for the BB84 protocol application with polarized photons – particles having spin 1 (bosons). Linear and diagonal bases (pairs of orthogonal states) are used to describe the polarization state of photons. The association (coding) convention between classical information bits (the message to be sent) and quantum information qubits (the polarization state of the photon) is given in Table 2. In the quantum approach, changing the polarization state of the photon as a result of a measurement on the transmission channel allows to detect any interception (eavesdropping attempt) of the messages, which is not possible in classical cryptographic systems. The testing/evaluation process looks to the final goal of the QKD protocol, namely, the sharing by the two legitimate entities (Alice and Bob) of a secret perfectly random binary sequence representing a secure key. In a classical system, the secure sharing of a secret cryptographic key is not feasible with maximum security, as the impossibility of intercepting the secret key during transmission cannot be guaranteed. The principles of quantum mechanics enable secure key distribution. The overall process of the secure secret key generation is based on polarized photons. The polarization state of the single photons is assumed to be the quantum state of the qubits (the quantum information elements).

*The process description*

In this process there are 2 legitimate entities: the transmitter (Alice) and the receiver (Bob). The sender (Alice) prepares each photon polarization state in one of the 2 bases: either linear (Horizontal H/Vertical V) or diagonal (+45/-45 degrees from the vertical direction). A polarizer with orientation along one of the 4 directions is used. The encoding convention is according to Table 2: the assigned binary value is 1 for the vertical orientation and -45 degree orientation and 0 for the horizontal orientation and 45 degree orientation, respectively. The quantum states for the corresponding qubits are as following (in Bra-ket Dirac notation):

|H>, |V> for the photon states with horizontal or vertical polarization, |+45> and |-45> for the photon states with +45 or -45 degree polarization, respectively. The transmitter sends a polarized photon to the receiver. The receiver has a polarization analyzer and a single photon detector. The receiver randomly selects one of the 2 bases and orients his analyzer along one of the directions in the selected basis. The transmitter informs the intended receiver about each photon transmission. The receiver registers or not the photon in his detector and determines the bit value. For example, if the analyzer belonging to the receiver is horizontally aligned, but the detector is not fired by a photon (there is no detection), then the returned bit value is 1 (vertical in the H/V basis). The transmitter and receiver record the selected measurement basis (H/V or +45/-45) and the corresponding bit value for each particle, independent of one another. Their bit values are perfectly correlated (the same values actually) only if the selected measurement bases are the same. The perfect correlation between the bit values means that, if the transmitter sends a bit of value 1, then the receiver should measure only the value 1. After finishing the measurements, the 2 entities (legitimate transmitter and receiver) make the public sharing of the used bases, but preserve the secrecy of the information, therefore the bit values still remain secret. Only the bits corresponding to the same selected measurement basis are preserved becoming part of the cryptographic key. The other bits (associated with the cases with different bases) are removed from the output. The error checking is done by the two by exchange a small number of their binary values; these values will then be removed from the final key material.

The overall process goal is to generate a secured cryptographic key. The issue is how to reliably detect an eavesdropping action. The evaluation of the BB884 protocol is done with several simulation sub-cases, defined according to the following criteria: *the randomness of the photon polarization state selection; the presence/absence of the attacker* (eavesdropping action), as depicted in Figures 1-5.

Figure 1 shows the transmission without interception, with the fixed selection of the bases (linear L, H/V) for both transmitter (Alice) and receiver (Bob). There are no errors because the sender and receiver use the same basis. The corresponding bits are part of the secret shared key. There is no eavesdropping on the communication path between the 2 entities (the absence of the attacker). The 2nd sub-case (Figure 2) is quite similar to the 1st one, except for the additional bit comparison operation (20 bits are compared). As in the previous sub-case, there are no errors in data transmission; any error should be detected by signalling the differences between the selected polarization bases of transmitter and receiver. The transmission process is unsecured because the bases are fixed for both transmitter and receiver. The fixed selection of the polarization bases (Figures 1–2) can be exploited by an attacker. The previous simulation sub-cases do not include an attacker's presence and, therefore, these are unsecured sub-cases without interception. In both cases, the theoretical number of key bits is the same with the total number of the generated bits.

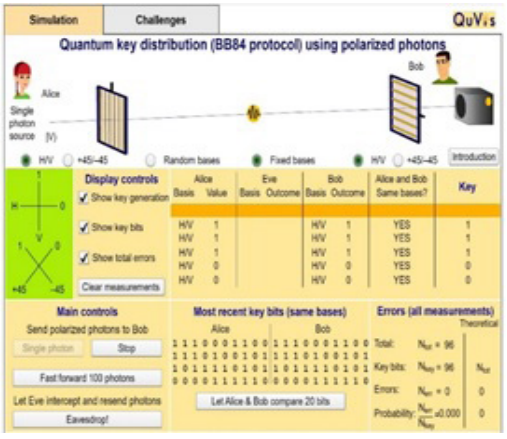


***Figure 1.*** *BB84 Simulation – no interception, fixed selection of the polarization bases – linear (H/V) basis*

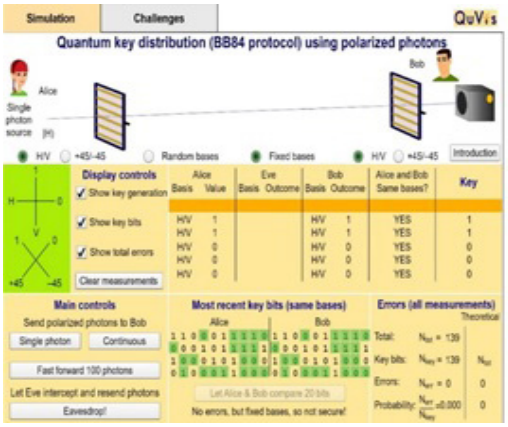


***Figure 2.*** *BB84 Simulation – no interception, fixed selection of the polarization bases – linear (H/V) basis, with bit comparison*

Figure 3 depicts the secured sub-case with the random selection of the polarization bases. The linear and diagonal bases are randomly selected. The random selection of the bases provides a higher security level. Although the theoretical number of key bits should be 1/2 of the total number of generated bits, in this simulation, the ratio of the number of key bits to the total number of generated bits slightly exceeds ½ up to the time of instantiation.

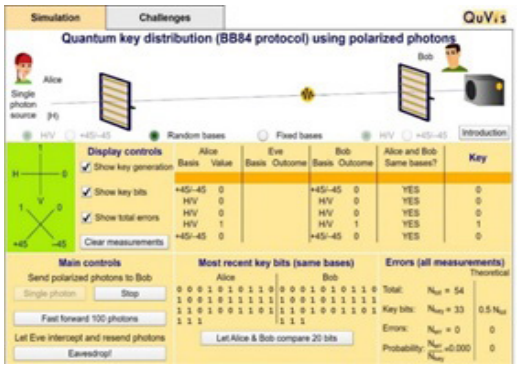


***Figure 3.*** *BB84 Simulation – no interception, random selection of the polarization bases*

The unsecured sub-case (fixed polarization bases) and with interception (the presence of the attacker) is depicted in Figure 4. One can see that, despite of the presence of the attacker, there is no error up to the instantiation time. This is due to the consistency between the selected polarization bases (as the transmitter, receiver and attacker used the same polarization base – the linear H/V one). Up to the current time in the experiment, the eavesdropper is not detected.

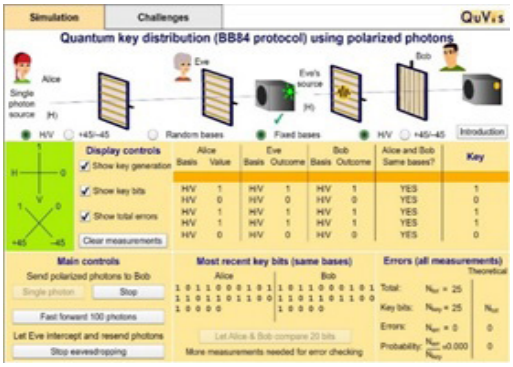


***Figure 4.*** *BB84 Simulation – interception, fixed selection of the polarization bases – linear (H/V) basis (L)*

Usually, more measurements are required for a reliable error checking, in order to ensure the statistical relevance of the information. In this sub-case the theoretical number of the key bits is the same with the total number of generated bits.

Figure 5 depicts the secured case (randomly selected polarization bases) and with interception (the presence of the attacker). The transmitter and receiver randomly select polarization bases – either linear (H/V) and diagonal D.

The attacker is present, but his polarization base is not right as it differs from the bases of the sender and receiver up to the current time (the emphasized row in the table showing the secret key generation process). Therefore, the generated bit may be included in the cryptographic key. Actually, the generated bits are included into the final key only if the condition regarding the consistency between the transmitter and receiver polarization bases is met (the same basis).

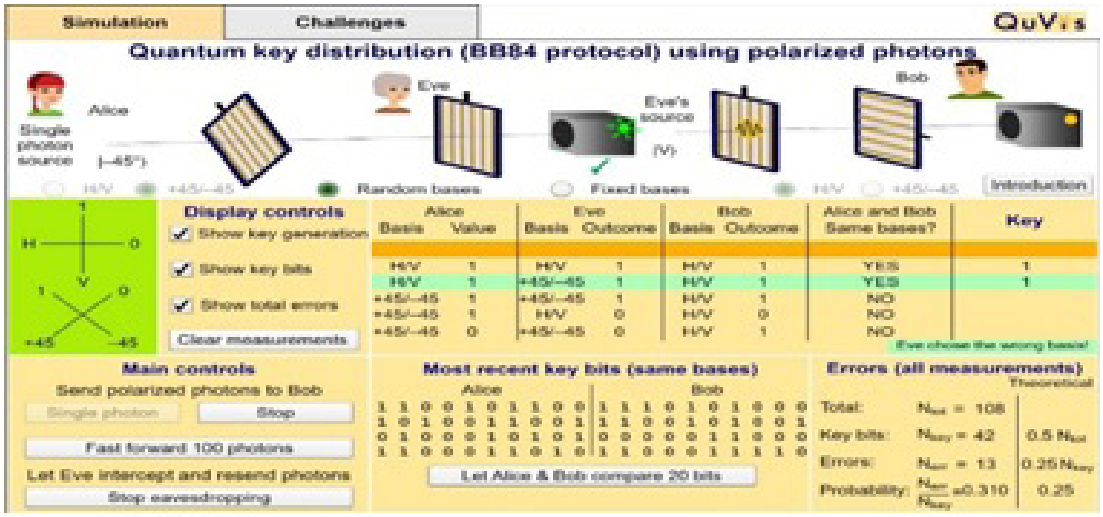


***Figure 5.*** *BB84 Simulation – interception, random selection of the polarization bases*

The theoretical number of key bits should be 1/2 of the total number of generated bits. In this simulation, up to the instantiation time, the ratio between the number of key bits and the total number of generated bits is slightly lower 0.5. On the other hand, the total number of bit errors should be 1/4 of the key bits number. In the experiment, up to the current time, the ratio between the number of bit errors and the key bits number may vary (in the example, it is slightly higher than 0.25).

Several information may be acquired in such experiments.

Figure 6 shows the sequence of outcomes that Bob (the receiver) measures, assuming no eavesdropper presence and action. The right measured values are checked. These are justified by the fact that the transmitter and receiver have the same values whenever their measurements are done in the same basis. The transmitter and receiver's values are perfectly correlated (meaning that the receiver measures the same value as the transmitter sends to him) only when both of them choose the same basis. If they do not use the same measurement basis, then their results are completely uncorrelated (Figure 7).

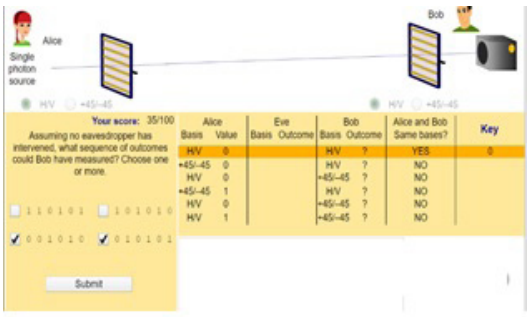

***Figure 6.*** *BB84 Simulation – the right outcomes measured by the legitimate receiver*

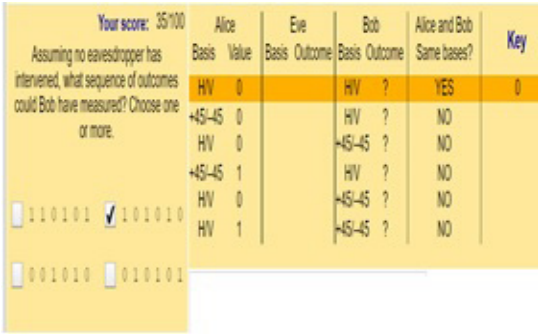

***Figure 7.*** *BB84 Simulation – incorrect selection of the receiver outcomes*

The 2nd case is shown for the *BB84 protocol application with ½ spin particles* (like electrons or, generally referred, fermions). The physical realization of the qubits is based on the quantum state of ½ spin particles and not on the photon's polarization state. A secured key is generated using individual ½ spin particles sent from transmitter to receiver. The transmitter prepares each particle with a spin state that can be: spin-up (associated to the binary value 1) or spin-down (corresponding to the value 0). This operation is performed along one of the orthogonal axes X or Z. The transmitter (Alice) sends the prepared particles to the receiver (Bob). The receiver has a Stern-Gerlach apparatus (SGA) – a region with non-uniform magnetic field which is aligned along to a certain axis (X or Z). The ½ spin particles separate into 2 streams with different deflections, one in the positive direction of the given axis (providing an outcome of value 1) and the other in the negative direction of the axis (ensuring an outcome of value 0). Each SGA device can be oriented along one of the two axes (X, Z). The quantum states for this simulation scenario are as following, depending on the orientation of SGA:

- for the orientation along the vertical axis (Z-direction): the orthogonal spin states $|\uparrow\rangle$ (value 1) and $|\downarrow\rangle$ (value 0);
- for the orientation along the horizontal axis (X-direction): the orthogonal spin states $|+\rangle$ (value 1) and $|-\rangle$ (value 0).

According to BB84 protocol, the transmitter and receiver independently record the basis (the orientation of SGA: X or Z) and the values for each particle (1 or 0). They know that their outcomes are perfectly correlated meaning that if the transmitter sends a certain binary value (1 or 0), then the receiver measures the same value (1 or 0, respectively), only if they select the same basis (the same alignment orientation for their SGA devices). After the measurements phase completion, both entities publicly share the selected basis used for their measurements, but not the underlying information (binary values). They only preserve the values obtained for the cases with the same selected basis and these bits are included in the secret cryptographic key. The errors checking is done by exchanging a small number of bits that will be later removed from the final key material. The simulations are shown in Figures 8, 9 and 10, without and with interception, respectively, and also without and with bits comparison. For these sub-cases the simulation is shown only for the random orientations of SGA (therefore, randomly selected measurement bases ensure the security of the process). The protocol operations for the secret key generation are quite similar.

In the sub-case with interception (Figure 10), one can see the errors that are generated by the wrong choosing of the attacker's measurement basis. The measurement basis is the SGA orientation and not the photon polarization, as in the 1st case.

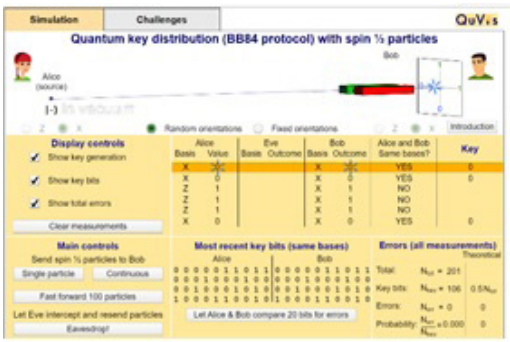


***Figure 8.*** *BB84 Simulation with ½ spin particles –no interception, random selection of the measurement bases (orientation)*

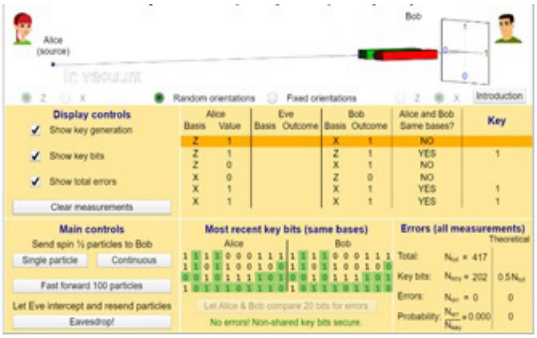


***Figure 9.*** *BB84 Simulation with ½ spin particles – no interception, random selection of the measurement bases, bits comparison*


***Figure 10.*** *BB84 Simulation with ½ spin particles – with interception, random selection of the measurement bases*

### *b) B92 Protocol*

Another QKD protocol based on Heisenberg's uncertainty principle and the photons polarization state is B92. This protocol was proposed by Charles Bennet in 1992, as a simplified version of the original protocol BB84 (Anghel, 2012). This protocol uses only 2 photons polarization non-orthogonal states instead of 4 states as in the 1st QKD protocol (BB84). BB84 protocol used 4 states for the information encoding, having 2 states for each of the 2 bases. In B92, the encoding is as following: 0 as $0^0$ in linear basis, 1 as $45^0$ in diagonal basis. The main protocol operations are quite similar.

### *The process description*

The transmitter randomly prepares the photons using the polarization state either horizontal – $0^0$ orientation (bit value 0) or diagonal $+45^0$ orientation (bit value 1). The transmitter sends the polarized photon to the receiver. The receiver has a polarization analyser and a single photon detector. For each measurement, the receiver randomly set the analyser aligned to an orthogonal direction with respect to the transmitter direction ($90^0$ or $-45^0$, respectively). The transmitter notifies the intended receiver every time when sending a polarized photon. When the receiver detects this photon, the true polarization state is already known and, therefore, the receiver also knows the bit value (0 or 1) sent by the transmitter (Figure 11).

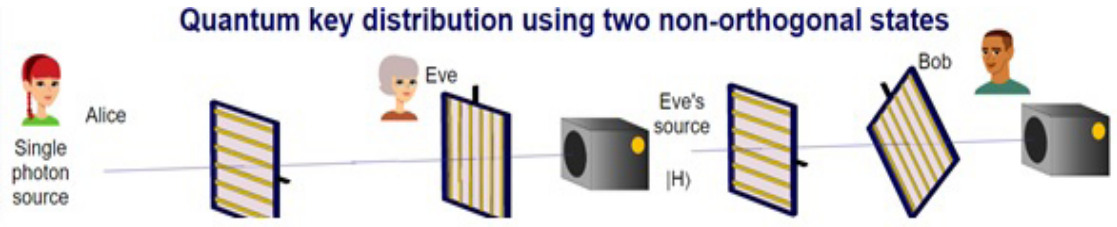


***Figure 11.*** *The setting for the B92 QKD protocol*

For example, if the intended receiver (Bob) detects a polarized photon while measuring along the 90º direction (SGA alignment), then he knows the +45º true polarization state sent by the transmitter (Alice) and, therefore, the true bit value is 1. The assigned bit value is 1 for the detections with 90º, while, for the detections with -45º, the assigned bit value is 0. If the receiver does not detect the photon, there will be no certainty about which state the transmitter sent. The transmitter and receiver will only preserve those measured cases in which the receiver detected a polarized photon. The generated key is the sequence of the corresponding bits. The two entities (transmitter Alice and receiver Bob) publicly communicate to find out the detected photons. The error checking is then done by exchanging of a small number of bits that later are discarded. The simulation sub-cases (with and without interception and also with and without the comparison of the last 20 bits for errors) are shown in Figures 12, 13, 14 (considering only random polarization basis selection).

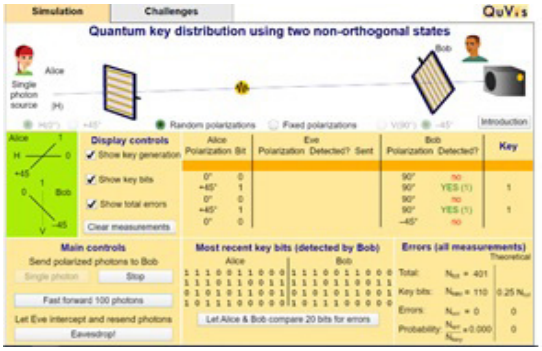


***Figure 12.*** *B92 Simulation – no interception, random selection of the polarization bases*

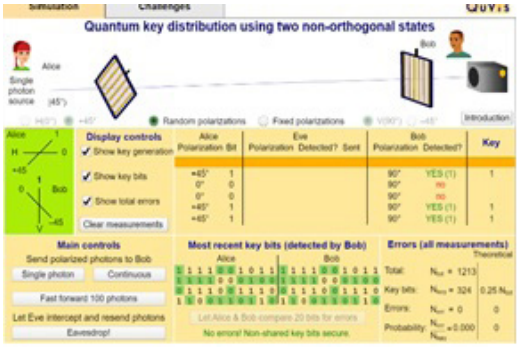


***Figure 13.*** *B92 Simulation – no interception, random selection of the polarization bases, bits comparison for error checking*

In Figure 14, one can see a case in which the entire key should be discarded, because of the detected eavesdropping action.

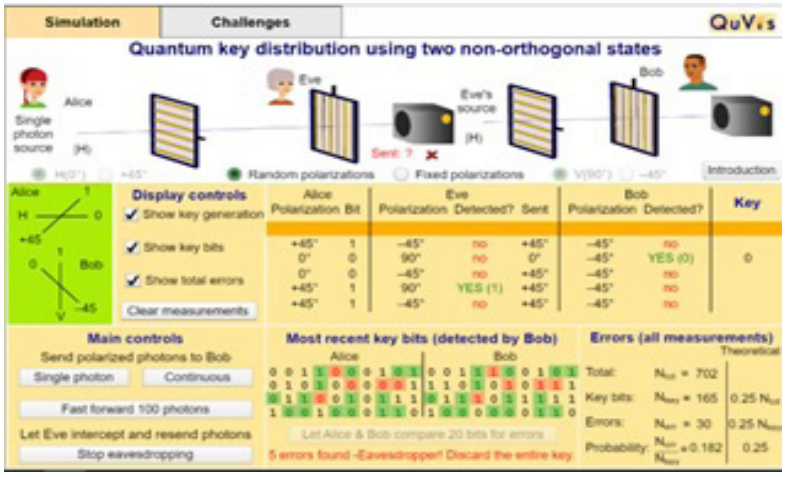


***Figure 14.*** *B92 Simulation – with interception, random selection of the polarization bases, bits comparison for error checking*

## Quantum Entanglement-based QKD protocols

The 2nd major category of QKD protocols uses the Quantum Entanglement feature in order to detect the passive attacks. This property means the quantum correlation between the particles such as changing a quantum state of the 1st particle will immediately change the stare of the other one. Quantum Entanglement is an essential property in quantum domain, with major relevance for different applications in Quantum Computing. Among QE-based QKD protocols one can mention E91 and BBM92 protocols.

*a) E91 Protocol*

This protocol was proposed by Eckert in 1991 (Anghel, 2012; Gisin, 1997; Treiber, 2009). Its design and operation exploit the Quantum Entanglement (QE) of the photons (qubits). The QKD protocol uses entangled photons pairs that can be generated either by the transmitter, or by the receiver or by a 3rd party. The entangled paired photons distribution is made so that each of the two legitimate entities has one photon from each pair. Eckert described a model with a channel and a single source that emits pairs of entangled particles – polarized photons (Haitjema, 2007). Each of the two entities part of the data communication randomly selects a measurement base. The transmitter A and receiver B clearly communicate the polarization bases they use in their measurements. The presence of an attacker E can be detected by examining those photons for which entities A and B have chosen different polarization bases for measurement. The major difference in comparison with the BB84 protocol is that the E91 protocol explicitly uses the quantum entanglement feature, the specific operations being defined at the level of polarized and entangled photon pairs (quantum correlated), while the BB84 protocol explicitly uses the polarization state of a single photon.

Despite the difference in how the principles of quantum mechanics are applied to secure key distribution (individual polarized photons or entangled pairs of polarized photons), the BB84 and E91 protocols are quite similar. Bennett and Brassard showed that any version derived from the original protocol proposed in 1984 can be adapted to include a source of entangled photons, removing the role of data transmitter A as a source of polarized photons (Haitjema, 2007).

*b) BBM92 Protocol*

The BBM92 protocol derived from the original BB84 protocol by Bennett, Brassard and Mermin, in 1992, is based on entangled photon pairs, thus exploiting the QE property. The major difference in comparison with the E91 protocol is that it uses only two polarization states instead of 4. The BBM92 protocol uses pairs of polarized entangled photons to transmit non-orthogonal quantum signals, instead of the approach based on the polarization state of single photons (the BB84 protocol).

*The process description*

The generation of the secret key is done using a source that emits pairs of entangled ½ spin particles. The two particles in a pair are emitted with opposite spin components. Each particle in the pair is transmitted through a Stern-Gerlach apparatus (SGA) which consists of a region of non-uniform magnetic field aligned along a given axis. For ½ spin particles, the particles separate into two discrete strings, one with deflection in the positive direction (output 1) and one with deflection in the negative direction (output 0). Each SGA device can be oriented along two orthogonal axes, X and Z. The transmitter and receiver perform measurements independently and record the basis (X or Z) and measurement result (0 or 1) for each pair. Due to QE, the two entities know that their results are perfectly anticorrelated (if Alice measures 1 then Bob measures 0 and vice versa), when both SGA devices are oriented along the same axis. After the measurements are completed, the two entities publicly share the bases used for each measurement (but not the results of the measurements) and retain only those results for which their bases are the same. Finally, the transmitter and receiver exchange a small

number of measurement results (which they will later discard) as an error checking step. The simulation cases are depicted in Figures 15 and 16, without and with interception, only with the random selection of the polarization bases for the entangled photons pairs. In the 1st sub-case (Figure 15), there are some bit errors (generated by mismatches between randomly selected bases). However, the error counting is strongly dependent on the number of measurements; a larger number of measurements is required to ensure a reliable error checking operation. The 2nd simulation sub-case (Figure 16) presents the transmission with interception (eavesdropping), random selection of alignment/deflection directions (bases for entangled photon pairs), and bitwise comparison between transmitter (Alice) and receiver (Bob). One can see 5 identified errors in the sequence containing the most recent 20 key bits.


***Figure 15.*** *Simulation BBM92 – no interception, random selection of the bases/alignment axes/ particles deflection*


***Figure 16.*** *Simulation BBM92 – with interception, random selection of the measurement bases / alignment axes/particles deflection, with bit comparisons*

This is why the entire generated key must be discarded. The key bits correspond to the matching of bases/directions of alignment cases. The theoretic number of the generated key bits should be 1/2 of the total number of the generated bits. The real ratio may vary. Also, the theoretical number of bit errors should be 1/4 of the number of key bits. This ratio may also vary, depending on the number of observations. The reliability of the error checking requires a large number of measurements.

## CONCLUSIONS

The QKD protocols provide a reliable security approach for data and communications process. This is due to the fact that they can be applied for use-cases requiring the detection of passive attacks (eavesdropping) which otherwise cannot be detected with conventional security techniques. Several QKD protocols have been defined and already applied during the last 40 years. However, there are still a lot of challenges for their practical application in various use-cases. In this paper, a brief overview of the most important QKD protocols was made. The typical protocols are presented with their most important operational features. The presentation was completed with several simulation cases, showing the secret cryptographic key generation process for protocols belonging to the both categories: single-photon and quantum entanglement-based protocols, respectively. An interesting and important research direction in this field concerns the way in which QKD could be efficiently integrated with conventional security systems, in order to increase the overall security level, in various applications cases.

## REFERENCE LIST


Anghel, C. (2012) *Security of IT and communication systems through quantum cryptography [Securizarea sistemelor informatice şi de comunicații prin criptografia cuantică].* PhD thesis. "Dunărea de Jos" University of Galaţi.

Babeș-Bolyai University. (2022) *Romanian National Strategy for the Development of Capabilities in Quantum Communications – QTSTRAT. Analysis of the existing situation and development trends in the field of quantum communications. [Elaborarea strategiei pentru dezvoltarea capabilităților naționale în domeniul comunicațiilor cuantice – QTSTRAT. Analiza situației existente și a tendințelor de dezvoltare în domeniul comunicațiilor cuantice].* https://qtstrat.granturi.ubbcluj.ro/. Report.

Dhanaraj, R. K., Rajasekar, V., Islam, S. K. H., Balusamy, B. & Hsu, C.-H. (2022) *Quantum Blockchain: An Emerging Cryptographic Paradigm*. Hoboken, New Jersey, U.S.A, WILEY – Scrivener Publishing.

Gisin, N. & Huttner, B. (1997) *Quantum cloning, eavesdropping and Bell's inequality.* Physics Letters A. 228(1-2), 13-21. doi: 10.1016/S0375-9601(97)00083-2.

Haitjema, M. (2007) *A Survey of the Proeminent Quantum Key Distribution Protocols.* http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/.

Treiber, A. (2009) *A fully automated quantum cryptography system based on entanglement for optical fibre networks.* New Journal of Physics. 11, 045013. doi: 10.1088/1367-2630/11/4/045013.

Quantum Computing. (2022) *What is the difference between CV QKD and DV QKD?*. https://quantumcomputing.stackexchange.com/questions/21743/what-is-the-difference-between-cv-qkd-and-dv-qkd. [Accessed 1st September 2023].

University of St Andrews. (n.d.) *The Quantum Mechanics Visualisation Project*. https://www.st-andrews.ac.uk/physics/quvis/.

Wikipedia. (n.d.) *List of quantum key distribution protocols.* https://en.wikipedia.org/wiki/List_of_quantum_key_distribution_protocols. [Accessed 21st August 2023].