Performance analysis of different multi-user optical passive networks for quantum cryptography applications

P. Curtacci, F. Garzia, R. Cusani, E. Baccarelli
Dipartimento INFOCOM, Università degli Studi “La Sapienza”, 00184 Rome, Italy

ABSTRACT

The performance of four passive optical network topologies in implementing multi-user quantum key distribution is compared, using 3 protocols proposed by quantum cryptography (B92, EPR, SSP). The networks considered are the passive-star network, the optical-ring network based on the Sagnac interferometer, the wavelength-routed network, and the wavelength-addressed bus network . An analysis of the quantum bit-error rate and sifted key rate for each of these topologies is used to determine their suitability for providing quantum key distribution-service to networks of various sizes. The efficiency of the three considered protocols is also determinated.

Keywords : Quantum cryptography, QKD, sifted key rate, QBER, B92, EPR, SSP.

1. INTRODUCTION

The quantum cryptography term represents the set of the techniques which allow two entities, Alice and Bob, to exchange reserved information by means of a quantum channel. A quantum channel is an optical channel governed by the quantum mechanics. The job in cryptographic field of the quantum mechanics allows results impossible to be obtained with the only mathematics. More precisely, talking about quantum key distribution (QKD) is opportune. The quantum channel is used to transmit a sequence of bits, well known only to Alice and Bob and then able to constitute the secret key of a cryptographic system. Therefore the next communications, which are ciphered with such key, can be made on a conventional channel (not quantum). QKD is a method for securely distributing encryption keys that are used for secure communications. These quantum systems are based on the theorem of Heisenberg [1], according to which the measurement of a quantum system generally perturbs it and gives an incomplete piece of information on his state preceding the measurement, and on the quantum no-cloning theorem [2], which forbids the perfect copying of two non-orthogonal quantum states. Therefore the quantum nature of a channel makes sure that any interception is noticed. Hence an eavesdropper, Eve, cannot get any information about the communication without introducing perturbations which would reveal her presence. To share a secret key, Alice and Bob must follow a protocol (BB84, B92, EPR, SSP, etc.). Once developed the procedure requested by the protocol, if any eavesdropper were not noticed, Alice and Bob share a secret key, which exchanged themselves without having to turn to a third reliable part and initially sharing no information, except that the one necessary to authenticate their communications part. The frequency used by Alice and Bob to share the sifted secret key is denominated sifted key rate (R_{SIFT}). To reveal the presence of an eavesdropper, Eve, Alice and Bob monitor the quantum bit error rate (QBER). If the QBER exceeds a certain threshold the made communication is just considered as not safe and therefore the secret key is discarded. The security threshold depends on the used protocol. The QBER and the R_{SIFT} are considered the fundamental parameters to evaluate the performances of a quantum channel. This analysis has already been done for BB84 protocol [3, 4]. The purpose of this paper is to extend the mentioned analysis to other three common protocols that are B92, EPR and SSP.

2. PROTOCOLS

2.1 B92

In an article of 1992 Charles Bennett proposed a new protocol, B92 [5, 8]. Both the transmitter “Alice” and the receiver “Bob” generate an independent random bit sequence. Alice then transmits her random bit sequence to Bob using a clocked sequence of linearly polarized individual photons with polarization angles chosen according to her bit values as given by 0°≡0 and 45°≡1. In each time period, Bob makes a polarization measurement on an incoming photon by orientating the transmission axis of his polarizer according to his bit value as given by -45°≡0 and 90°≡1. It means that Bob will detect only that subset of incoming photons that goes through his polarizer. We refer to these instances as “un-ambiguous” since when they occur, Alice and Bob can be sure that their polarization settings were not orthogonal and, consequently, that their bit values were the same (both 0 or both 1). Conversely, the instances in which Bob receives no photon are referred to as “ambiguous”. In fact, Bob doesn’t receive any photons when these are absorbed by his polarizer. It absorbs all photons that are orthogonal with his axis (when Alice’s and Bob’s bit values are not the same), but it also absorbs, with probability 1/2, some photons that are not orthogonal with his axis (Alice’s and Bob’s bit values are the same). It means that Bob will detect, on average, only 1/4 of incoming photons. Bob then uses an authenticated public channel to inform Alice of the time slots in which he detected bits (1/4 on average), so they can extract a shared bit sequence, the key, from the initial random bit sequence. The B92 protocol is intrinsically less efficient than the given BB84 that, also in ideal conditions (when no bit of the raw key is to be deleted), only 1/4 of the impulses gives a key bits, while with BB84 protocol fraction is 1/2. This inefficiency is the price that Alice and Bob must pay for secrecy.

2.2 Six State Protocol (SSP)

The Six State Protocol (SSP) encodes classical bits in 6 states: the 4 states of BB84 (0°, 90°, +45°, -45°) with the addition of 2 polarization states. Because of the complex nature of his coefficients, Hilbert space 2-dimensional admits also a third base (circular) conjugate to both the rectilinear and diagonal bases:

- $|\overline{\overline{0}}> = (|0°> * \frac{1}{\sqrt{2}} + i\,|90°> * \frac{1}{\sqrt{2}})$ (1)
- $|\overline{\overline{1}}> = (|0°> * \frac{1}{\sqrt{2}} - i\,|90°> * \frac{1}{\sqrt{2}})$ $(i = \sqrt{-1})$

In the SSP the polarization states are assembled in 3 non-orthogonal basis placed along Cartesian axes where: x = rectilinear base (0°, 90°); y = diagonal base (+45°, -45°); z = circular base ($|\overline{\overline{0}}>, |\overline{\overline{1}}>$). Conventionally, one attributes the binary value 0 to states 0°, 45° and $|\overline{\overline{0}}>$ and the value 1 to the other three states. In the first step, Alice sends one photon to Bob choosing at random one of the three bases (x, y, z). Next, Bob measures the incoming photons in one of the three bases, chosen at random. If Alice and Bob both choose the same random basis, then Bob’s measurements will have a deterministic outcome. Conversely, the outcome of his measurement becomes probabilistic. In the second step, Alice and Bob communicate over a public channel to compare the bases in which the bits were encoded and measured. The bits that are sent and measured in different bases are discarded. The remaining bits (on average 1/3 of initial sequence) shared between Alice and Bob form the key. Compared to the other protocols, SSP has the highest symmetry of the bit state space. This symmetry reduces Eve’s optimal information gain for a given error rate QBER. If Eve measures every photon, the QBER is 33%, compared to 25% in the case of the BB84 protocol [1].

2.3 EPR

The protocols described up to now foresee that Alice sends the photons to Bob, where the state of the photon codifies the value of the bit to be transmitted. In the EPR protocol [7], each of the two parts receives a particle belonging to a couple, produced by a third source. Ekert (1991) has devised a quantum protocol based on the properties of quantum correlated particles. Einstein, Podolsky and Rosen (EPR) [9] point out an interesting phenomenon in quantum mechanics. According to their theory, the EPR effect occurs when a pair of quantum mechanically correlated photons, called the entangled photons, is emitted from a source. The entanglement may arise out of conservation of angular momentum. As a result, each photon is in an undefined polarization. Yet, the two photons always give opposite polarizations when measured along the same basis. Since EPR pairs can be pairs of particles separated at great distances, this leads to what appears to be a paradoxical “action at a distance”. It is possible to create a pair of photons (each of which we label below with the subscripts A and B, respectively), with the correlated linear polarizations [10]. This correlation is given by the following expression and represents the polarization state of the pair (entangled state):

$$\Psi(A,B)= (|0°>_A |90°>_B - |90°>_A |0°>_B) * \frac{1}{\sqrt{2}} \qquad (2)$$

Einstein (1935) then states that such quantum correlation phenomena could be a strong indication that quantum mechanics is incomplete and that there exist “hidden variables”, inaccessible to experiments, which explain such “action at a distance”. Bell [11] gave a means for actually testing for locally hidden variable (LHV) theories. He proved that all such LHV theories must satisfy the Bell inequality. Quantum mechanics has been shown to violate the inequality. The EPR quantum protocol is a 3 state protocol that uses Bell’s inequality to detect the presence or absence of Eve as a hidden variable. We now describe a simplified version of this protocol in terms of the polarization states of an EPR photon pair. An EPR pair is created at the source. One photon of the constructed EPR pair is sent to Alice, the other to

Bob. Alice and Bob use the same bases to prepare and measure their particles. A similar setup, but with Bob's bases rotated by 45° [12], can be used to test the violation of Bell inequality, that it's used to detect the presence or absence of Eve. Alice records his measured bit. On the other hand, Bob records the complement of his measured bit. This procedure is repeated for as many EPR pairs as needed. Alice and Bob carry on a discussion over a public channel to determine the correct bases they used for measurement. Each of them then separates its respective bit sequences into two sub-sequences. One subsequence, called raw key, consists of those bits at which they used the same basis for measurement. The other subsequence, called rejected key, consists of all the remaining bits. Unlike the BB84 and B92 protocols, the EPR protocol, instead of discarding rejected key, actually uses it to detect Eve's presence. Alice and Bob now carry on a discussion over a public channel comparing their respective rejected keys to determine whether or not Bell's inequality is satisfied. If it is, Eve's presence is detected. If not, then Eve is absent. In this way the probability that they choose the same basis is reduced from 1/2 to 2/9 [1], but at the same time as they establish a key they collect enough data to test Bell inequality .

3. TOPOLOGIES OF THE MULTI-USER QKD NETWORKS

The first experimental implementation of QKD occurred during the October 1989 in Montreal University, when encryption keys were transmitted through 30 cm of air using polarization-encoded photons. It was shown that the use of orthogonal states on more than 10 km of optical fibre is impossible, according to the characteristics of the sources available at present [2, 14]. To allow transmissions at distances always longer, it is therefore necessary the use of systems different from the ones used before. In particular, when using an interferometer, we can encode qubits in an interferometric phase state. We explain, as example, the implementation of B92 using an interferometer. Alice encodes the photons with her phase modulator (PM) by randomly choosing one of two phase shifts: 0 and π. She associates 0 with qubit 0, and π/2 with qubit 1. Bob makes his measurement choosing at random between a -π/2 or π phase shift. Only photons with a final phase shift of -π/2 or +π/2 (the difference of Alice's and Bob's phase shifts) can produce a qubit with probability 1/2. Every photon which produces a final phase of 0 or π does not produce any qubit and is deleted. Thus, whenever Bob measures correctly, qubit 0 is routed to Detector 1 (Det1) and qubit 1 to Detector 2 (Det2). Bob then uses an authenticated public channel to inform Alice of the time slots in which he obtained qubit and then they use the shared subset of their initial random bit sequences represented by these time slots as a key. This process creates the sifted key. Now we introduce the four QKD network topologies to be compared [3]. These networks phase-encode the qubits in optical fiber interferometers. The optical-ring network uses a Sagnac interferometer; all other topologies are implemented with unbalanced Mach–Zehnder interferometers (MZIs). The unbalanced MZI is a modification of the standard MZI with improved interference stability. This improved stability comes at the expense of a 3-dB loss, since half of the photons transmitted through it are lost in the non-interfering path combinations of the interferometer [1]. This makes networks that use the unbalanced MZIs more lossy, thus lowering their sifted key rate and increasing their QBER. The single-photon sources used in the network topologies and in the calculations are modelled as highly attenuated laser pulses that are typically used in practice and contain an average of 0.1 photon per pulse. The single-photon detectors are also modelled as the response of gated avalanche photodiodes operated in Geiger mode [15]. In general, Alice is defined as the user that provides the qubit information in the four bases, and Bob is defined as the user that chooses between the two non-orthogonal basis sets. For the passive-star (fig. 1), wavelength-routed (fig. 3), and wavelength-addressed bus (fig. 4) topologies, Alice is the network controller. She is equipped with an unbalanced MZI, a pulsed laser source (PLS), a tunable attenuator (TA), and a 4-state PM (Phase Modulator). The users at the receiving end (Bob, Chris, … N-th user) choose between the two non-orthogonal bases. Each one of them has another unbalanced MZI, a two-state PM, and a pair of single-photon detectors (Det1 and Det2). The optical-ring network (fig. 2) is significantly different from the others. Here, Bob is the network controller and services multiple Alices. Bob's setup consists of a laser source, two detectors, a two-state PM, and a circulator. Each Alice possesses only a four-state PM.

3.1 Passive-Star Network

The topology of the passive-star QKD network is shown in figure 1. A passive-star QKD network was first demonstrated by Townsend to connect four users over 5.4 km of optical fiber [16]. This topology is an extension of the two-user system, with Alice linked to receivers through a 1xN splitter. Due to the indivisible nature of the photon, each photon is randomly routed to a single user by the 1xN splitter. This topology can be easily implemented but suffers from the effective loss induced by the 1 splitter, which reduces the probability of photons reaching the detectors of any particular user. This reduction scales inversely as the number of users on the network. For example, a three-user network having a 1x2 splitter reduces the probability that a photon will reach the desired receiver by half and consequently acts as a 3 dB attenuator. A 17-user network containing a 1x16 splitter operates effectively like a 12 dB attenuator, and so on. Although this drawback can be partially mitigated by higher initial qubit rates, the routing of the photons to each user is inherently non-deterministic. For example, the mean detection rate at each user after a 1xN splitter is 1/Nth of the detection rate of a single Bob without the 1xN splitter. However, since the routing of photons to each user through the 1xN splitter is random, at any given time, some users will receive photons at a rate above the mean detection rate of 1/Nth, and some users will receive photons at a rate below the mean detection rate. This non-deterministic detection rate will constrain the design of secure quantum networks by limiting the amount of information that can be securely encrypted.

3.2 Optical-Ring Network based on Sagnac Interferometer

Figure 2 shows the schematic diagram of the optical-ring network topology. A two-user QKD system based on the optical fiber Sagnac interferometer has been demonstrated by Nishioka et al. [3]. This topology is significantly different from the topologies based on the unbalanced MZIs: the single-photon pulse enters the Sagnac interferometer through an optical circulator. This pulse splits into two parts in the 50/50 coupler, and each part travels around the Sagnac loop in clockwise (CW) and counter clockwise (CCW) directions, respectively. Any user on the loop that is communicating with Bob modulates the pulse travelling in the CW direction. Bob modulates the pulse travelling in the CCW direction. The position of Bob's PM is important since the pulse that it modulates must be returning from its round trip in the loop in order to prevent any information about Bob's modulation choice from travelling through the loop. A timing and control mechanism must also be established so that only one Alice can modulate the photon at a time. Upon travelling around the loop, the pulses interfere in the coupler and enter one of two photon detectors. Photons enter Detector 1 (Det1 in fig. 2) when they experience a phase shift between the CW and CCW pulses inside the Sagnac interferometer. On the other hand, they enter Detector 2 (Det2 in fig. 2) when they experience a 2π phase shift between the CW and CCW pulses inside the Sagnac interferometer. The Sagnac interferometer has the advantage of being free from thermal fluctuations since the counter propagating pulses pass through the exact same fiber paths inside the loop. Another potential advantage is that each user on the network, except Bob, contains only a single-PM and no photon detectors. This can simplify any deployment of a secure ring network using the Sagnac because Bob is the only user that requires the single-photon detectors.

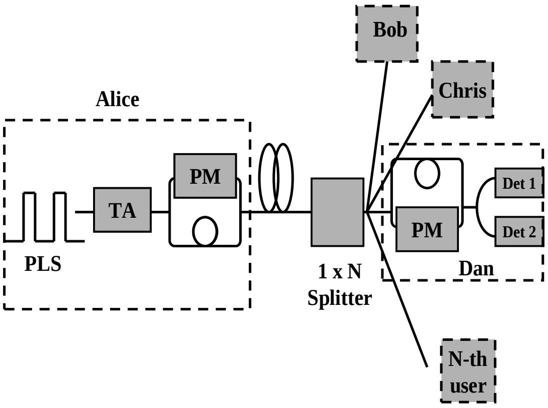

Fig. 1: Passive-star multi-user QKD network.

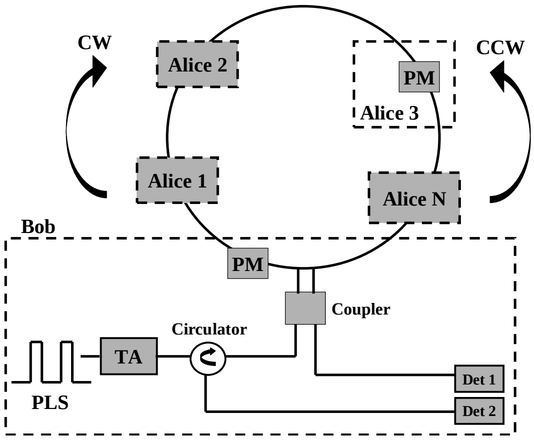

Fig. 2: Optical-ring multi-user QKD network.

3.3 Wavelength-Routed Network

The schematic diagram of the wavelength-routed network topology is depicted in figure 3. This topology is implemented with unbalanced MZIs and it is very similar in layout to the star network. The greater difference is that Alice has the ability to control which user receives the photons by employing a wavelength-routing scheme. Alice is equipped with a wavelength tunable pulsed laser source (PLS) and the receivers are assigned their own wavelength channel. Alice transmits to a particular user by tuning her source to that user's wavelength and the photons are routed via an arrayed waveguide grating (AWG). The advantage of this topology is that the insertion loss of the AWG is approximately uniform regardless of the number of channels. Theoretically, the number of users that this kind of network support is limited only by the channel spacing of the AWG and the bandwidth of the fiber. In addition, the single-photon detectors must be sensitive for the entire range of frequencies used in the network. This is not a problem since avalanche-photodiode (APD)-based single-photon detectors respond to a much broader spectrum than the band of wavelengths used in multi-wavelength networks.

3.4 Wavelength-Addressed Bus Network

The wavelength-addressed bus network is also based on the unbalanced MZI setup and it is shown in figure 4. Like the wavelength-routed network, this network also allows Alice to route her photons to a desired user by tuning the photons to a desired wavelength. In such a system, Alice is equipped with a tunable PLS, and each receiver is assigned their own wavelength channel. Alice selects an intended receiver by tuning her source to that user's wavelength and transmits the encoded photons along the bus. The receivers are connected to the bus line through a fiber Bragg grating (G), which allows them to retrieve only the photons intended for them. These gratings are designed to reflect photons of a specific wavelength to a given user and transmit all others. The network accommodates multiple users by placing several fiber Bragg gratings in series along the bus. One of the merits of this topology is that it can be easily expanded to accommodate more users by simply tapping the bus and inserting a suitable grating.

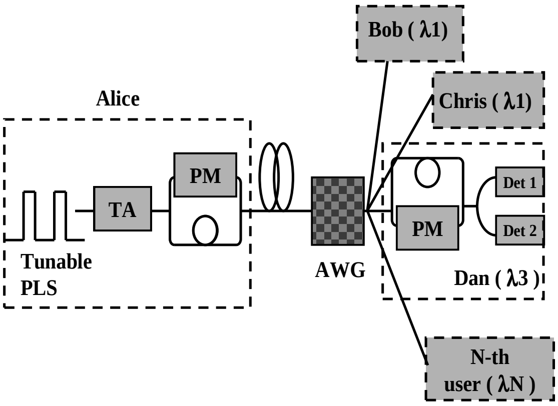

Fig. 3: Wavelength-routed multi-user QKD network

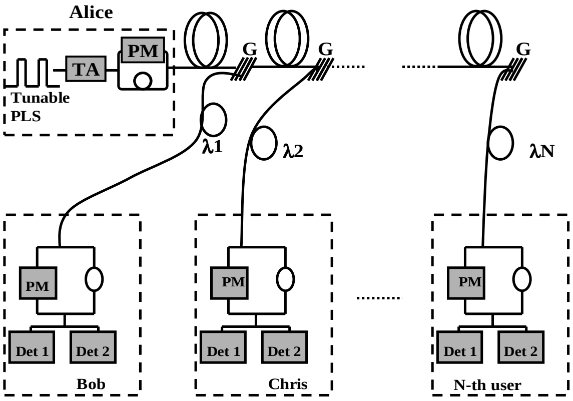

Fig. 4: Wavelength-addressed bus multi-user QKD network.

4. SECURITY THRESHOLD

Due to the principles of quantum mechanics described above, it is impossible for the spy Eve to gain perfect knowledge of the quantum state sent from Alice to Bob. Hence an eavesdropper, Eve, cannot get any information about the communication without introducing perturbations which would reveal her presence. We always have some detector noise, misalignments of detectors and so on. It should be pointed out that we cannot even in principle distinguish errors due to noise from errors due to eavesdropping activity. We therefore assume that all errors are due to eavesdropping. Nevertheless, she can acquire some knowledge. From an information theoretic point of view, the natural measure of "knowledge" about some signal is the Shannon information. It is measured in bits and can be defined for any two parties, the sender of the signal and the observer (receiver). In general terms, the knowledge of the observer consists of obtained measurement results and any additional gathered knowledge, like the announced basis of signals in the SSP protocol. The QBER, which is indicative of the security and post-error-correction net key rate, is useful for assessing the performance of the network. High QBER values in QKD systems lower the net key rate during the error correction stage of the protocol [1]. In addition, high QBER allows an eavesdropper to gain more information about the transmitted keys at the expense of the legitimate receiver. It has been shown that for QBERs above a security threshold, an eavesdropper can actually gain more information than the legitimate receiver. If this happens, it is not possible to use any privacy-amplification technique. Therefore, when designing a QKD network, it is necessary to ensure that the baseline QBER is below this security threshold so that privacy amplification strategies may be used to eliminate any knowledge gained by Eve [1]. For QBERs under this threshold ($QBER_T$), the Shannon information between Alice and Bob (I_{AB}) is higher than that in Eva's possession (I_E). For QBERs over the threshold, Eve has more information than Alice and Bob:

$$\mathrm{QBER} < \mathrm{QBER}_T \qquad I_{AB} > I_E \qquad (3)$$
$$\mathrm{QBER} > \mathrm{QBER}_T \qquad I_{AB} < I_E$$

Bounds on the obtainable Shannon information for eavesdropping on single bits can be found in the literature for different protocols. Fuchs et al. give bounds for the EPR [17] and the B92 protocol [18]. A bound for the Six State

Protocol was also obtained [19]. These bounds are illustrated in figure 5, 6, 7 for each of used protocol. Note the trade-off between Eve's information gain and the disturbance she causes: more information for Eve means higher error rate for Bob. For reasonably low error rates Eve's maximal information is smallest in the six-state protocol, as it uses the biggest ensemble of input states. Furthermore comparing Eva's Shannon Information with the Shannon information between Alice and Bob; we are able to determinate the threshold for the QBER for each of the used protocols.

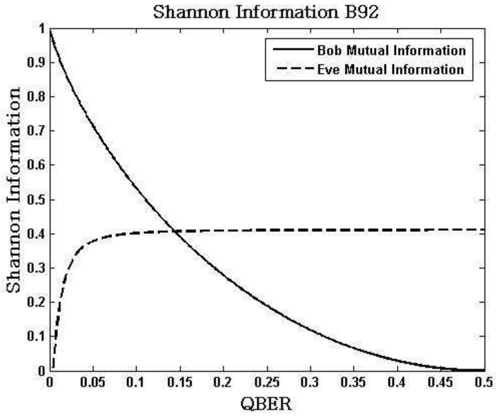

Fig. 5: Shannon Information with B92 protocol

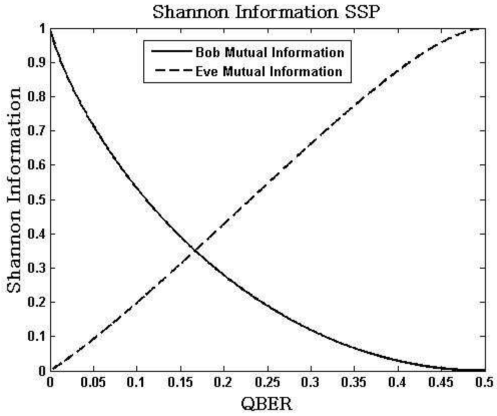

Fig. 6 : Shannon Information with SSP

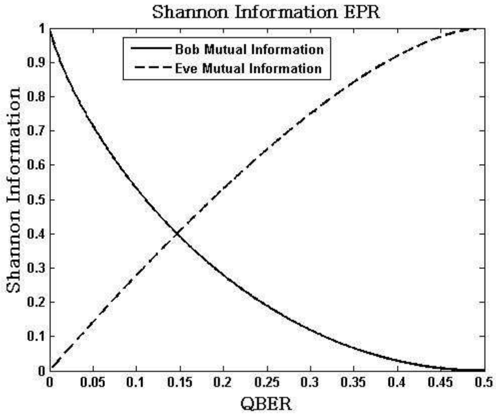

Fig. 7 : Shannon Information with EPR protocol

5. KEY PARAMETERS IN QKD

QBER and R_{SIFT} are two parameters used to measure the performance of network topologies which offer QKD service. The QBER and sifted key rate equations that are used in the simulations are illustrated in this section. More detailed discussions on the physical principles underlying these equations are provided in references [1 - 20]. The sifted keys are those keys shared by Alice and Bob when they make compatible basis choices [20]:

$R_{SIFT} = q\ R_{RAW}$ (4)

$R_{RAW} = f_{REP}\ \mu\ t_{LINK}\ \eta$ (raw key rate) (5)

where q depends on protocol (for example, in BB84 protocol q = 1/2 because half the time Alice and Bob bases are not compatible), f_{REP} is the repetition frequency, μ is the average number of photons per pulse, t_{LINK} is the transmission coefficient of the link and η is Bob's detection efficiency. The transmission coefficient is related to the loss l_F (in dB per km) and length L (in km) of the fiber, the loss due to the number of users l_N(N) (dB), and the topology selected, by:

$t_{LINK} = 10^{-(l_F L + l_N(N) + l_T)/10}$ (6)

The topology choice introduces a topology loss constant l_T (in dB) that is an overhead of loss involved in working with a particular topology. This quantity is constant regardless of a network's fiber length and number of users. The topology loss has 4 components: end-user losses arising from losses in the receiver's interferometer, routing loss caused by the device that selects the user that receives the photon, the non-interfering path combination loss in the unbalanced MZIs (for those topologies that use them), and miscellaneous losses, such as those caused by connectors and splices. The QBER is defined as the number of wrong bits to the total number of received bits and it is normally in the order of a few percent. In the following we will use it expressed as a function of rates [1]:

$$QBER = \frac{R_{error}}{R_{SIFT} + R_{error}} \approx \frac{R_{error}}{R_{SIFT}} \qquad (7)$$

One can distinguish three different contributions to R_{ERROR}. The first one arises because of photons ending up in the wrong detector, due to imperfect interference or polarization contrast. The rate R_{OPT} is given by the product of the sifted key rate and the probability P_{OPT} of a photon going in the wrong detector:

$$R_{OPT} = R_{SIFT}\, P_{OPT} \qquad (8)$$

This contribution can be considered, for a given set-up, as an intrinsic error rate indicating the suitability to use it for QKD. Imperfect phase matching in the interferometers results in reduced fringe visibilities that lead to an increased probability of routing photons to the wrong detectors. The probability of this type of error P_{OPT} is related to the fringe visibility (V) by:

$$P_{OPT} = \frac{1-V}{2} \qquad (9)$$

The second contribution, R_{DARK}, arises from the detector dark counts (or from remaining environmental stray light in free space setups). This rate is independent of the bit rate and depends only on the characteristic of the photon counter [15]. Of course, only dark counts falling in a short time window when a photon is expected give rise to errors:

$$R_{DARK} = k\, f_{REP}\, P_{DARK} \qquad (10)$$

where P_{DARK} is the probability of registering a dark count per time-window and per detector. K factor is related to the fact that a dark count has a k% chance to happen with Alice and Bob having chosen incompatible bases (thus eliminated during sifting). Finally, error counts can arise from uncorrelated photons, because of imperfect photon sources:

$$R_{ACC} = \frac{1}{2} f_{REP}\, \mu\, t_{LINK}\, \eta\, P_{ACC} \qquad (11)$$

This factor appears only in systems based on entangled photons, where the photons belonging to different pairs but arriving in the same time window are not necessarily in the same state. The quantity P_{ACC} is the probability to find a second pair within the time window, knowing that a first one was created. The QBER can now be expressed as follows:

$$QBER = \frac{R_{OPT} + R_{DARK} + R_{ACC}}{R_{SIFT}} \qquad (12)$$

6. PARAMETER VALUES

The results are based on calculations assuming the following parameter values, which are held constant for each topology [1, 15, 16, 21, 22] :

Pulse repetition rate (f_{REP})	1 MHz	Mean number of photon per pulse (μ)	0.1
Detector efficiency @1310 nm (η)	20%	Detector efficiency @1550 nm (η)	10%
Dark count probability (P_{DARK})	10^{-5}	Fringe visibility (V)	98%

Loss Source	**Star**	**Ring**	**W.Routed**	**Bus**
Topology Loss				
End User Loss (dB)	0.3	0.49	0.3	0.3
Routing Loss (dB)	0.1	0.0	3.0	0.02
Non interfer. path Loss (dB)	3.0	0.0	3.0	3.0
Miscellaneous Loss (dB)	1.0	1.0	1.0	1.0
Total Topology Loss (dB)	4.4	1.49	7.3	4.32
Fiber Loss (dB/Km)	0.35 @ 1310 nm 0.25 @ 1550 nm			
User number Loss (dB)	10log(N)	0.1N	0	0.2(N-1)

Tab.1 : Losses contributing to the transmission coefficient t_{LINK} for the 4 network topologies [3].

The transmission coefficient link t_{LINK} varies from one topology to another. The values used in the simulations that contribute to t_{LINK} are outlined for each topology in table 1. In the table the contributions to the topology losses are also shown; namely, the end-user loss, routing loss, non-interfering path combination loss, and miscellaneous loss. The end-user loss arises from the excess loss in the couplers and PM in the receiver's interferometer. Routing loss is the loss in the device that routes the photons to each user. In the star, wavelength-routed, and bus networks, which are all based on the unbalanced MZI design, a 3 dB loss arises from non-interfering path combinations. The miscellaneous loss represents from losses such as those due to connectors, splices, and imperfections in the network all of which occur in practical optical network setups. Now we are able to analyse the QBER and the R_{SIFT} for every QKD protocol considered previously. The results of QBER for each topology are presented in the following tables that report the maximum distance (Km) supported by every topology for various number of users for QBER< $QBER_T$ and the maximum number of users supported by every topology at different distance for QBER < $QBER_T$. This threshold, previously mentioned in Section IV, is the value below which secure key distribution can be performed on the network. The term "distance" is defined as the total fiber length used in the transmission of the photons. For the optical ring, it is the total length of the Sagnac loop. For all the other topologies, it is the total fiber length spanning Alice and Bob (or Chris, Dan, etc.). Another observation that is made is about the *crossover distance.* This distance (30 km), is the same for all four topologies and determines when it's useful to use the wavelength at the 1550 nm or at 1310 nm. For distances less than 30 km, the sifted key rate values at 1310 nm are always greater than at 1550 nm. The situation reverses for distances beyond 30 km. In fact, at the distance of 30 km, the maximum number of users is the same for both the wavelengths (tab. 2, 4, 6). The system performances at 1310-nm and 1550-nm telecommunications wavelength windows are shown in the following tables. In addition, these results also serve to show a network's sensitivity to expanding the number of users.

7. QBER PERFORMANCE

7.1 B92

As previously explained in Section 2.1, B92 protocol is intrinsically less efficient than the given BB84 that, also in ideal conditions (when no bit of the raw key is to be deleted), only 1/4 of the impulses gives a key bits, while with BB84 protocol this fraction is 1/2. This inefficiency is the price that Alice and Bob must pay for secrecy.

$$R_{SIFT} = \frac{1}{4} R_{RAW} = \frac{1}{4} f_{REP}\, \mu\, t_{LINK}\, \eta \qquad (13)$$

$$R_{OPT} = \frac{1}{4} f_{REP}\, \mu\, t_{LINK}\, \eta\, P_{OPT} \qquad (14)$$

$$R_{DARK} = \frac{1}{2} f_{REP}\, P_{DARK} \qquad (15)$$

Table 2 and table 3 summarize the performance of B92 protocol applied to the four topologies.

7.2 SSP

As previously explained in Section 2.2, the six states constitute 3 bases, hence the probability that Alice and Bob chose the same basis is only of 1/3. This means that to determinate the sifted key, that Alice and Bob can share, an average of 2/3 of the received bits must be discarded. But the symmetry of this protocol greatly simplifies the security analysis and reduces Eve's optimal information gain for a given error rate QBER.

$$R_{SIFT} = \frac{1}{3} R_{RAW} = \frac{1}{3} f_{REP}\, \mu\, t_{LINK}\, \eta \qquad (16)$$

$$R_{OPT} = \frac{1}{3} f_{REP}\, \mu\, t_{LINK}\, \eta\, P_{OPT} \qquad (17)$$

$$R_{DARK} = \frac{2}{3} f_{REP}\, P_{DARK} \qquad (18)$$

Table 4 and table 5 summarize the performance of SSP protocol applied on the four topologies.

7. 3 EPR

As previously explained in Section 2.3, in the EPR protocol, each of the two parts (Alice and Bob) receives a particle belonging to a couple, produced by a third source. Because this source is not perfect it could generate uncorrelated photons that provoke error counts (R_{ACC}). The photons belonging to different pairs, not necessarily in the same state, could arrive in the same time window with probability P_{ACC}. Furthermore the EPR protocol, instead of discarding rejected key, actually uses it to detect Eve's presence. By a discussion over a public channel, Alice and Bob compare their respective rejected keys to determine whether or not Bell's inequality is satisfied. If it is, Eve's presence is detected. If not, then Eve is absent. In this way the probability that they choose the same basis is reduced from 1/2 to 2/9 [1], but at the same time, as they establish a key, they collect enough data to test Bell inequality .

$$R_{SIFT} = \frac{2}{9} R_{RAW} = \frac{2}{9} f_{REP}\, \mu\, t_{LINK}\, \eta \qquad (19)$$

$$R_{OPT} = \frac{2}{9} f_{REP}\, \mu\, t_{LINK}\, \eta\, P_{OPT} \qquad (20)$$

$$R_{DARK} = \frac{7}{9} f_{REP}\, P_{DARK} \qquad (21)$$

$$R_{ACC} = \frac{1}{2} f_{REP}\, \mu\, t_{LINK}\, \eta\, P_{ACC} \qquad (22)$$

$$P_{ACC} = \frac{1}{2} \mu^2 = 000.5 \qquad (23)$$

Table 6 and table 7 summarize the performance of SSP protocol applied on the four topologies.

Distance **(Km)**	**Star** **1310nm/1550nm**	**Ring** **1310nm/1550nm**	**W.routed** **1310nm/1550nm**	**Bus** **1310nm/1550nm**
10	32/20	>128 / >128	>128/ >128	76/66
20	14/11	>128 / >128	>128/ >128	59/54
30	6/6	110/110	>128/ >128	41/41
40	2/3	75/85	>128/ >128	24/29
50	1/2	40/60	0/>128	6/16
60	0/1	5/35	0/0	0/4
70	0/0	0/10	0/0	0/0
80	0/0	0/0	0/0	0/0

Tab. 2: B92-protocol. Maximum number of users supported by every topology at different distance for QBER <14%.

Number of **users**	**Star** **1310nm/1550nm**	**Ring** **1310nm/1550nm**	**W.routed** **1310nm/1550nm**	**Bus** **1310nm/1550nm**
20	15/10	55/66	44/50	42/47
40	7/0	50/58	44/50	31/31
60	2/0	44/50	44/50	19/15
80	0/0	38/42	44/50	8/0
100	0/0	32/34	44/50	0/0
120	0/0	27/26	44/50	0/0

Tab. 3 : B92-protocol. Maximum distance (Km) supported by every topology for various number of users for QBER<14%.

Distance **(Km)**	**Star** **1310nm/1550nm**	**Ring** **1310nm/1550nm**	**W.routed** **1310nm/1550nm**	**Bus** **1310nm/1550nm**
10	34/21	>128 / >128	>128 / >128	78/68
20	15/12	>128 / >128	>128 / >128	60/55
30	6/6	113/113	>128 / >128	43/43
40	3/3	78/88	>128 / >128	25/30
50	1/2	43/63	0/ >128	8/18
60	0/1	8/38	0/0	0/5
70	0/0	0/13	0/0	0/0
80	0/0	0/0	0/0	0/0

Tab. 4: SSP - protocol. Maximum number of users supported by every topology at different distance for QBER <17%.

Number of **users**	**Star** **1310nm/1550nm**	**Ring** **1310nm/1550nm**	**W.routed** **1310nm/1550nm**	**Bus** **1310nm/1550nm**
20	16/11	56/67	45/52	43/48
40	8/0	50/59	45/52	31/32
60	3/0	45/51	45/52	20/16
80	0/0	39/43	45/52	9/0
100	0/0	33/35	45/52	1/0
120	0/0	28/27	45/52	0/0

Tab. 5: SSP - protocol. Maximum distance (Km) supported by every topology for various number of users for QBER<17%.

Distance **(Km)**	**Star** **1310nm/1550nm**	**Ring** **1310nm/1550nm**	**W.routed** **1310nm/1550nm**	**Bus** **1310nm/1550nm**
10	3/1	79 / 58	>128/ >128	26/16
20	1/1	44 / 33	0/ 0	8/3
30	0/0	9/9	0/ 0	0/0
40	0/0	0/0	0/0	0/0
50	0/0	0/0	0/0	0/0
60	0/0	0/0	0/0	0/0
70	0/0	0/0	0/0	0/0
80	0/0	0/0	0/0	0/0

Tab. 6: EPR- protocol. Maximum number of users supported by every topology at different distance for QBER <15%.

Number of users	**Star 1310nm/1550nm**	**Ring 1310nm/1550nm**	**W.routed 1310nm/1550nm**	**Bus 1310nm/1550nm**
20	0/0	26/25	15/10	13/7
40	0/0	21/17	15/10	2/0
60	0/0	15/9	15/10	0/0
80	0/0	9/1	15/10	0/0
100	0/0	4/0	15/10	0/0
120	0/0	0/0	15/10	0/0

Tab. 7: EPR - protocol. Maximum distance (Km) supported by every topology for various number of users for QBER<15%.

8. R_{SIFT} PERFORMANCE

As it can be seen from the equations 13, 16, 19, it is possible to obtain the highest R_{SIFT} by Six State Protocol, but the R_{SIFT} performances of the four network topologies are the same for each used protocol. To be able to make more visible the difference between the various topologies, we compare the sifted key rate of each topology as a function of distance for 4, 32, 64, 128 users. We use a rating system ranging from 1–4, where 1 indicates the network topology with the best performance, and 4 indicates the network topology with the worst performance, to summarize the results of the comparison of the sifted key rate performance of the network topologies. This is shown in table 8.

Number of users	**Passive star**	**Optical ring**	**W.routed**	**Bus**
4	4	1	3	2
32	4	1	2	3
64	4	1	1	3
128	3	2	1	4

Tab. 8 : Comparison of the Sifted Key Rate (R_{SIFT}) performance for the 4 network topologies.

9. RESULT DISCUSSION

Passive star network turns out to be the worst net topology because it supports the smallest number of users for any given distance, it is very sensitive to change in the distance and/or in number of the users and it has the lowest $R_{SIFT.}$ Furthermore it requires each user to have their own interferometer and photo-detectors. In this sense, the ring topology is the simpler design, requiring each user to have only one four-state.

Optical ring network is characterized by higher stability against polarization and phase fluctuations than the other three topologies since each pulse travels through the same fiber length in both the CW and CCW directions [23], lowest structure loss (1.49 dB, tab. 2), lowest QBER with less than 64 users, highest R_{SIFT} with less than 64 users; it is also more susceptible to Trojan horse attacks than systems based on the unbalanced MZI [3].

Wavelength network is the most suitable for networks with more than 64 users, because its Sifted key Rate is independent of the number of users on the network, but it may not be the best choice for networks that are not expected to expand beyond 64 users since it has the highest structure loss (7.3 dB)

Wavelength-addressed-bus network is the most favourable for networks with less than 20 users because it can be easily expanded and has moderate structure loss (4.32 dB), but it is unadvisable for networks with large number of users because it has higher per-user loss than the ring network.

It has also been shown that there is a crossover distance (30 Km) that determines the optimum wavelength (1310 or 1550 nm) to use in the QKD network. About QKD analyzed protocol only B92 and SSP turned out the most efficient. The EPR protocol is the less efficient. The difficulty to handle couples of particles without changing their correlation does not allow to obtain high performances. The results obtained at the moment are the least encouraging for all the four net topologies. The maximum reachable distance was of 30 km with 9 user maximum using the Optical-Ring topology. Only for distances shorter than 10 km it is possible to obtain sufficient performances, avoiding always and however the Passive-Star topology. Six State and B92 protocol present praiseworthy results. The B92 is the more used QKD protocol. It allows to reduce the communications needs on public channel. Six State Protocol prevails on everyone because, having a security threshold of 17%, allows to have a high number of users also beyond the 60 km, furthermore it has the fastest Sifted Key Rate.

REFERENCES

1. N. Gisin, et al., *Quantum cryptography*, Rev. Mod. Phys., pp. 1–57, quant-ph/0101098 v2, September 2001
2. W. K. Wootters and W. Zurek, *A single quantum cannot be cloned*, Nature (London), vol. 299, pp. 802–803, 1982
3. P.Kumavor, A. Beal, S. Yelin, E. Donkor, B. Wang, *Comparison of four multi-user quantum key distribution schemes over passive optical networks*, In Journal of lightwave technology, vol 23, n.1, January 2005
4. C. H. Bennett and G. Brassard, *Quantum cryptography: 'Public key distribution and coin tossing*, presented at the IEEE Conf. Computers, Systems Signal Processing, Bangalore, India, 1984
5. C. Bennett, *Quantum cryptography using any two nonorthogonal states*. Phys. Rev. Lett. 68, 3121 ,1992
6. H. Bechmann-Pasquinucci and N. Gisin, *Incoherent and Coherent Eavesdropping in the 6-state Protocol of Quantum Cryptography*, quant-ph/9807041, 1998
7. A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. 67, 661–663, 1991
8. Karen J. Gordon, et al., *A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System*, IEEE Journal of Quantum Electronics Vol 40, No7, July 2004
9. A. Einstein, B. Podolsky and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Physical Review 41, 777, May, 1935
10. Muhammad Musharraf Ishtiaq Khan and Muhammad Sher, *Protocols for Secure Quantum Transmission: A Review of Recent Developments.* Pakistan Journal of Information and Technology 2 (3): 265-276, 2003
11. J. Bell, *On the Einstein, Podolsky, Rosen Paradox.* Physics, 1, 195-200, 1964
12. Dagmar Bruß et al., *Quantum Key Distribution: from Principles to Practicalities,* quant-ph/9901061, 1999
13. C. Bennett, et al., *Experimental quantum cryptography,* Journal of Cryptology, 5, 3-28, 1992
14. A. Muller, J. Breguet and N. Gisin, *Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fiber over more than 1km.* Europhysics Letters, 23, 383-388 ,1993
15. D. Stucki et al., "*Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's*,", arXiv:quant-ph/0 106 007
16. P. D. Townsend, *Quantum cryptography on multi-user optical fiber networks*, *Nature (London)*, vol. 385,1997
17. C. A. Fuchs, et al., *Optimal Eavesdropping in Quantum Cryptography I*, Phys. Rev. A 56, 1163, 1997
18. C. A. Fuchs and A. Peres: *Quantum State Disturbance vs. Information Gain: Uncertainty Relations for Quantum Information*. Phys. Rev. A 53, 2038–2045, 1996
19. D. Bruß: *Optimal eavesdropping in quantum cryptography with six states*. Phys. Rev. Lett. 81, 3018, 1998
20. D. Stucki, et al., "*Quantum key distribution over 67 km with a plug&play system,*" *New J. Phys.*, vol. 4, July, 2002
21. P. A. Hiskett *et al.*, "*Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm,*" *J. Mod. Opt.*, vol. 48, no. 13, pp. 1957–1966, Jul. 2001
22. D. S. Bethune and W. P. Risk, "*Autocompensating quantum cryptography,*" *New J. Phys.*, vol. 4, July, 2002
23. X. Fang and R. O. Claus, "*Polarization-dependent all-fiber wavelength division multiplexer based on a Sagnac interferometer,*" *Opt. Lett.*, vol. 20, no. 20, pp. 2146–2148, October 1995
24. Richard J. Hughes, George L. Morgan and C Glen Peterson, *Practical quantum key distribution over a 48-km optical fiber network.* Physics Division Los Alamos NM 87545
25. T. Nishioka, H. Ishizuka, T. Hasegawa, and J. Abe, "*'Circular type' quantum key distribution," IEEE Photon. Technol. Lett.*, vol. 14, no. 4, pp. 576–578, Apr. 2002.