Quantum key secure communication protocol via enhanced superdense coding

Mario Mastriani

Received: 27 April 2021 / Accepted: 14 October 2022 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In this study, an improvement, and a generalization to more than two bits of the superdense coding protocol are presented. Based on both innovations, a novel quantum key secure communication protocol is developed, which uses an N-bit key, optical multiplexers and demultiplexers, and quantum repeaters, which work thanks to entanglement swapping. In this way, the new protocol allows the simultaneous transmission of N-bits encrypted through optical channels. This study incorporates implementations on two platforms: the Quirk simulator, and the 16-qubits Melbourne processor of the IBM Q Experience program. Errors in terms of the number of quantum repeaters are studied. Finally, this study is completed by analyzing the advantages of the optical link, with which the protocol works, versus the commonly used electromagnetic link for quantum communication between submerged submarines in the presence of a third party that acts as an eavesdropper.

Keywords Quantum entanglement · Quantum Internet · Quantum repeaters · Quantum teleportation

1 Introduction
Currently, information security implies, one way or another, the use of techniques based on principles of quantum mechanics. Below we will mention the most relevant of all of them:

Quantum key distribution (QKD) protocols. They base their entire operation on the use of polarized (Bennett and Brassard 1984; Zhang and Ni 2020) or entangled photons (Ekert 1991; Kish et al. 2020), being the manipulation of the key its flank of greater exposure to the attack of an eavesdropper, which compromises their efficiency in real life applications. This eventual weakness comes in the form of four security loopholes which are related to: (1) the exposure of the key in the quantum channel (QCh) or distribution channel, (2) the transfer of the key from said channel to the sender terminals, (3) the transfer of the key from the same channel to the receiver terminals, and (4) the free availability of the public channel through which the encrypted message or ciphertext travels. These loopholes are
commonly ignored in both communication terminals, which generates a serious security problem due to the daily advance of eavesdropping techniques.

Quantum no-key protocol (Nguyen and Kim 2020; Kak 2005). This protocol is divided into three stages, where each one has its own key, consisting of unitary transforms applied to the message transferred at each stage. Its main differences with a QKD protocol, e.g. Bennett-Brassard (BB84) (1984), consists in that here both the keys and the message always remain quantum, and that at each stage the flow of communication has an opposite direction to the previous one.

Deterministic secure quantum communication (DSQC) (Elsayed 1904; Qaisar et al. 2017) protocol. This quantum protocol uses a key to encrypt each classical bit of a deterministic message thanks to two photons. In the same way, as in the case of quantum cryptography techniques based on QKD, DSQC protocol can work with entangled or polarized photons, using a unidirectional quantum channel, and a classical channel (Elsayed 1904; Qaisar et al. 2017). Besides, as a sine qua non condition, in DSQC the information must be preprocessed by photons before encoding it in order to avoid unnecessary exposure of parts of the message in the channel in the presence of an eventual eavesdropper. Whether or not such presence is detected, the same protocol will be the vehicle to send the key by which the message will be decrypted.

Quantum secure direct communication (QSDC) protocol (Long and Liu 2002; Deng and Long 2004; Zou et al. 2020a; Zhou et al. 2020; Xie 2020; Chen et al. 2018; Zou and Qiu 2014; Yan et al. 2020; Wang et al. 2006; Wei et al. 2012; Qi et al. 2019). It was created in 2000 by Prof. Gui-Lu Long from the Department of Physics of Tsinghua University. This protocol eliminates the four loopholes mentioned above in relation to the key management in QKD, therefore, it constitutes the greatest expression of quantum cryptography, being QSDC the best quantum technique for secure communications currently in use. In fact, QSDC exploits the attributes of the entanglement (Audretsch 2007; Jaeger 2009; Horodecki et al. 2007) for the development of long-distance quantum communication (Cariolaro 2015; Dieks 1982; NIST 2014; Yu et al. 2014) like no other. Consequently, it can directly transmit secure information through quantum channels without keys (Deng and Long 2004). In particular, the simplified version of QSDC, presented in this work, is extremely ductile when we try to extend their range via any kind of quantum repeaters (Sangouard et al. 2011; Hasegawa et al. 2019; Munro et al. 2015; Ruihong and Ying 1237; Razavi et al. 2009), whether we use lines of optical fiber or if necessary, satellite quantum repeaters (Boone et al. 2015; Mastriani and Iyengar 2020).

Post-quantum cryptography (PQC) (Chen 2016; Crockett et al. 2019; Wang et al. 2018). Among the most important post-quantum primitives, we have lattice-based cryptography and code-based cryptography. Elliptic curves cryptography (Yoneyama 2019), in general, is not able to resist quantum computers, and indeed post-quantum schemes based on elliptic curves rely on isogenies between super-singular elliptic curves. Furthermore, normally post-quantum schemes do not surpass the Rivest–Shamir–Adleman (RSA) algorithm (Rivest et al. 1978) in terms of key size: code-based schemes have rather large keys, while lattice-based schemes are characterized by smaller keys but, in general, RSA with the same (classical) security level has keys way smaller.

Consequently, after having studied the pros and cons of the two most used techniques in Quantum Cryptography: QKD (Bennett and Brassard 1984; Zhang and Ni 2020; Ekert 1991; Kish et al. 2020), and QSDC (Long and Liu 2002; Deng and Long 2004; Zou et al. 2020a; Zhou et al. 2020; Xie 2020; Chen et al. 2018; Zou and Qiu 2014; Yan et al. 2020; Wang et al. 2006; Wei et al. 2012; Qi et al. 2019), we present here an alternative to both techniques without their respective defects called Quantum Key Secure Communication.
(QKSC) protocol, which is extremely robust and easy to implement in both optical (Furusawa and Loock 2011) and superconductor (IBM Q Experience 2020; Rigetti 2020; D-Wave 2020; Braket 2020) platforms. However, we resort here to the 16-qubits Melbourne IBM quantum processor (IBM Q Experience 2020), and Quirk simulator (Algorithmic Assertions 2020), without losing generality in the number of qubits, which theoretically can be extended into an infinite number, or at the origin of the implementation platform (IBM Q Experience 2020; Rigetti 2020; D-Wave 2020; Braket 2020).

Showing up next, the main tool necessary to implement the QKSC protocol, i.e., an enhanced version of the Super-dense Coding protocol (Bennett et al. 1993; Nielsen and Chuang 2004) is developed in Sect. 2. QKSC protocol is explained in Sect. 3. Implementations of the novel on the 16-qubits Melbourne IBM quantum processor (IBM Q Experience 2020), and Quirk simulator (Algorithmic Assertions 2020) are presented in Sect. 4 with a complete section about the analysis of the outcomes. Finally, Sect. 5 provides the conclusions.

2 Enhanced super-dense coding protocol

All the keys used in the cryptographic protocols mentioned in Sect. 1 are expressed in bits or in their quantum counterparts, which arise from the two poles of the Bloch’s sphere (Nielsen and Chuang 2004; Kaye et al. 2004; Stolze and Suter 2007) and which are called Computational Basis States (CBS). These CBS can be expressed in several ways:

\[
\text{North pole} = \text{Spin up} = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \text{and}
\]

\[
\text{South pole} = \text{Spin down} = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.
\]  

QKD protocols such as Bennett and Brassard’s (1984) (BB84) also use qubits of the type:

\[
|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \text{and} \quad |-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),
\]

where \(H\) is the Hadamard gate (Nielsen and Chuang 2004; Kaye et al. 2004; Stolze and Suter 2007). QKSC uses classic bits and the famous Bell bases (Nielsen and Chuang 2004; Kaye et al. 2004; Stolze and Suter 2007):

\[
|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\beta_{00}\rangle, \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv |\beta_{10}\rangle,
\]

\[
|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv |\beta_{01}\rangle, \quad \text{and} \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv |\beta_{11}\rangle.
\]  

In fact, the type of qubits used to be transmitted securely thanks to the QKSC protocol will be exclusively the bases of Eq. (4) and their extension to Greenberger–Horne–Zeilinger (GHZ) states (Nielsen and Chuang 2004). Specifically, the QKSC protocol is based on the use of an enhanced version of the Super-dense Coding technique (Bennett et al. 1993;
Nielsen and Chuang (2004), which will be analyzed below along with the original protocol. Figure 1 shows three versions of such protocol, where:

(a) Represents the original protocol (Bennett et al. 1993), such that:

- In $t_0$, we have two ancillas $|0\rangle$ in q[0] and q[1], and both classical bits $\{b_0, b_1\}$ to be transmitted in a secure way, where the simple lines represent quantum wire, i.e., lines that transport qubits, while the double lines have to do with classic wires, i.e., lines that transport classic bits,
- In $t_1$, both Bell states $|\beta_{\text{in}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are available in q[0] and q[1],
- Between $t_2$ and $t_1$, both classic bits $\{b_0, b_1\}$ are incorporated to the quantum circuit via a pair of Controlled-Pauli’s gates (Controlled-X, CNOT or CX; and Controlled-Z, or CZ) (Nielsen and Chuang 2004; Kaye et al. 2004; Stolze and Suter 2007) applied on the qubit q[0], and
- Between $t_3$ and $t_2$, an unitary transform is applied on qubits q[0] and q[1] which is formed by a CNOT and a Hadamard (H) gate (Nielsen and Chuang 2004), besides
both quantum measurements (Busch et al. 2016; Schlosshauer 2005) are carried out, in order to obtain the transmitted classic bits \( \{b_0, b_1\} \) from the recovered CBS allocated in \( q[0] \) and \( q[1] \).

(b) Represents the enhanced protocol, such that:
- In \( t_0 \), we have two ancillas \( |0 \rangle \) in \( q[0] \) and \( q[1] \), and both classic bits \( \{b_0, b_1\} \) to be transmitted in a secure way, exactly the same as the original protocol case,
- In \( t_1 \), both Bell states \( |\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \) are available in \( q[0] \) and \( q[1] \), in the same way as in the original protocol,
- Between \( t_2 \) and \( t_1 \), the difference among the original protocol and the novel appears, since the CZ gate is applied to qubit \( q[1] \), while the CNOT gate is applied to qubit \( q[0] \), and
- Between \( t_3 \) and \( t_2 \), the same unitary transform based on a CNOT and a Hadamard (H) gate (Nielsen and Chuang 2004) is applied on qubits \( q[0] \) and \( q[1] \). Besides both quantum measurements (Busch et al. 2016; Schlosshauer 2005) are carried out, in order to obtain the transmitted classic bits \( \{b_0, b_1\} \) from the recovered CBS allocated in \( q[0] \) and \( q[1] \). However, both in the novel and in the original protocol the outputs lose the original order of the classic bits transmitted when they are recovered, as shown in Fig. 1b. So we turn to the next modified version of the improved protocol.

(c) Represents the modified enhanced protocol, such that:
- In \( t_0 \), it is identical to the two previous versions,
- In \( t_1 \), it is identical to the two previous versions,
- Between \( t_2 \) and \( t_1 \), it is identical to the last version,
- Between \( t_3 \) and \( t_2 \), a beam-splitter, formed by a CNOT gate in \( q[0] \) and a Hadamard gate in \( q[1] \), is flipped respect to the last version, in order to obtain the transmitted classic bits \( \{b_0, b_1\} \) from the recovered CBS allocated in \( q[0] \) and \( q[1] \) in the correct order. See Fig. 1c.

In this study, we will use the version (c) of Fig. 1, because it constitutes a primal stage of the QKSC protocol, which will be described in the next section. In practice, we will use symbols or samples (of a signal) coded with several classic bits (not just two), therefore, it is important to have a previous example of the aforementioned enhanced protocol for a greater number of bits to be transmitted safely, which is not possible with the original super-dense coding (Bennett et al. 1993; Nielsen and Chuang 2004) protocol, since it only supports two. Figure 2 shows a generalization of the enhanced super-dense coding protocol of Fig. 1(c) for 4 classic bits \( \{b_0, b_1, b_2, b_3\} \) to be transmitted. As we can see, this configuration is a natural extension of the 2 classic bits version, with a single point to highlight, which is between \( t_3 \) and \( t_1 \). The passage between the protocol of Fig. 1c for 2 bits and that of Fig. 2 for 4 bits consists in increasing the number of CNOT gates used as the number of classic bits to be transmitted increases, while the CZ gate is only applied to the most significant qubit in both versions, in fact, \( q[1] \) for Fig. 1c and \( q[3] \) for Fig. 2.

Table 1 summarizes the time slot for Figs. 1 and 2, where, \( I_{N \times N} \) means identity matrix of \( N \)-by-\( N \) elements, \( \otimes \) is the Kronecker product (Nielsen and Chuang 2004), and \( |GHZ_4\rangle = (|0000\rangle + |1111\rangle) / \sqrt{2} \) is a Greenberger-Horne-Zeilinger state for four entangled particles (Nielsen and Chuang 2004; Kaye et al. 2004; Stolze and Suter 2007).
Finally, Fig. 2 as a natural extension of Fig. 1c, where the number of classical bits to be teleported can be extended unlimitedly.

### 3 Quantum key secure communication (QKSC) protocol

All cryptographic configurations based on QKD protocols (Bennett and Brassard 1984; Zhang and Ni 2020; Ekert 1991; Kish et al. 2020), like that of Fig. 3a, work with three types of channels:

- **Quantum channel (QCh),** in red in Fig. 3a, which results from the distribution of polarized (Bennett and Brassard 1984; Zhang and Ni 2020) or entangled (Ekert 1991; Kish et al. 2020) photons, which are generated by an emitter (which we will call Alice), and sent through from this quantum channel (QCh) to a receiver (which we will call Bob).

- **Public or classical channel (PCh),** in black in Fig. 3a, which is used to complete tasks related to the key distribution, e.g., key sifting and distillation (Cao et al. 2017) in the case of the BB84 protocol (Bennett and Brassard 1984). The sifting task essentially consists of a process where the bits are eliminated, both from the sender and the receiver, which do not have an exact correlation between them. So when this task is done, the sender and the receiver share a key of the same length known as the sifted key (QuRep 2020). An eavesdropper cannot reconstruct the key from the information exposed in the channel during this task, since the errors related to said key have to do with the intervention of the eavesdropper and not with the key itself. As a consequence of this, a second process called key distillation is launched. Basically, the process known as key distillation is composed of two stages: (a) in the first stage all the errors of the key are corrected by means of a classic procedure (QuRep 2020), while (b) in the second one the key is conveniently reduced by means of a procedure known as privacy amplification so that the eavesdropper does not have the necessary information.
Table 1  
Time slot of Figs. 1 and 2

| Time | Figure |
|------|--------|
| 0    | ![Diagram](image1) |
| 1    | ![Diagram](image2) |
| 2    | ![Diagram](image3) |
| 3    | ![Diagram](image4) |

**Example:**
- **Time 0:**
  - \( b_0, b_1 \in \{0, 1\} \)
  - \( q[0] = q[1] = 0 \)
- **Time 1:**
  - \( b_0, b_1 \in \{0, 1\} \)
  - \( q[0] = q[1] = 0 \)
  - \( q[0] = q[1] = 0 \)
- **Time 2:**
  - \( b_0, b_1, b_2, b_3 \in \{0, 1\} \)
  - \( q[0], q[1], q[2], q[3] \)
  - \( q[0], q[1] = b_0, q[2], q[3] = b_3 \)

Note: The diagrams and detailed mathematical expressions are not included in the text but are referenced as `image1`, `image2`, `image3`, and `image4`. The table is a simplification of the more complex table presented in the document.
• Data or insecure channel (DCh), in light blue in Fig. 3a, is the weakest link in the chain and is the natural medium through where the encrypted message or ciphertext travels, which arises from applying the distributed key to the unencrypted original message or plaintext. As in the previous case, this channel is also public and classic in nature.
Instead, quantum secure direct communication (QSDC) protocols (Long and Liu 2002; Deng and Long 2004; Zou et al. 2020a; Zhou et al. 2020; Xie 2020; Chen et al. 2018; Zou and Qiu 2014; Yan et al. 2020; Wang et al. 2006; Wei et al. 2012; Qi et al. 2019), Fig. 3b, uses a classical channel for authentication to verify a correct mutual authentication between Alice and Bob, and a quantum channel with two branches (forward and backward) to complete the transmission of the message. Formally, QSDC does not work with a ciphertext like QKD, however, we allowed ourselves to call the coded message that travels thanks to the quantum channel ciphertext in order to establish a better comparison between QSDC and QKD of Fig. 3a and b, respectively. In fact, there are excellent previous examples of QSDC protocols using GHZ states (Wang et al. 2005; Gao et al. 2020), however all of them without a key.

Like all quantum secure direct communication (QSDC) protocols (Long and Liu 2002; Deng and Long 2004; Zou et al. 2020a; Zhou et al. 2020; Xie 2020; Chen et al. 2018; Zou and Qiu 2014; Yan et al. 2020; Wang et al. 2006; Wei et al. 2012; Qi et al. 2019), the configuration of the QKSC protocol of Fig. 3c proposed in this work uses an authenticated public channel or service channel in order to regularly verify the integrity of the transmitted data between Alice and Bob (Pan et al. 2020a), and a quantum channel QCh as a transport agent for the encrypted message, for which, prima facie, no key is generated or distributed, and the message is encoded in Bell bases like those seen in Eq. (4) which are generated and encoded in the sender (Alice) and travel through the quantum channel QCh to the receiver (Bob) where they are decoded, as part of the process to recover the message, which in this case will be symbols of a text or samples of a signal. At this point, the most noticeable difference between QSDC and QKSC is that the former uses a two-branch quantum channel, while the latter works with a single-branch quantum channel, i.e., the forward branch. In fact, the mere fact of eliminating a branch of the quantum channel remarkably simplifies the practical implementation of QKSC versus QSDC, and this is precisely the second most newsworthy difference between them: the simplicity of implementation of QKSC versus QSDC, both in superconducting quantum computers and on optical circuits. Specifically, QKSC can interchangeably work with symbols coded, for example, in American Standard Code for Information Interchange (ASCII) code (ASCII code 2020), where every symbol is coded in 8 bits; or work with signal samples coded in a pulse-code modulation (PCM) codification (Faruque 2015) with \( n \) bits-per-sample (bps). In all cases these are binary and classic bits to be transmitted from Alice (sender) to Bob (receiver) using the QKSC protocol.

For transmissions over long distances, using lines of optical fiber or satellite links, QKSC will require, like any other quantum cryptography protocol, the use of quantum repeaters between Alice (sender) and Bob (receiver), as can be seen in Fig. 4, which shows the block diagram of the QKSC protocol, where Alice incorporates \( n \) ancillas of the type \( |0\rangle \) and the symbol (or sample) coded in \( n \) classic bits. At the output of this block, there is a quantum channel (QCh) which consists of a single wire because this block incorporates a multiplexer at its output. The diagram continues with a number of quantum repeaters, which depends on the type of link used, i.e., by lines of optical fiber or satellite link and the distance to be covered with the communication system. Each quantum repeater incorporates a multiplexer-demultiplexer pair, hence these blocks exclusively work with a single wire. Finally, Bob receives the coded information from the only wire that constitutes the quantum channel (QCh) and after a measurement he recovers the classic \( n \) bits of the transmitted symbol (or sample) B.

In principle, this protocol uses a single channel, the QCh, however, faced with the possibility of losing photons due to:

\[ \text{Springer} \]
• Problems in their transmission through lines of optical fiber or through spatial transmission via satellite links, or by
• Attacks by an eavesdropper of the photon-number splitting attack (Huttner et al. 1995; Brassard et al. 2000) type,

it may be necessary to use an authenticated public channel or a service channel in order to regularly verify the integrity of the transmitted data. However, since QKSC works essentially on the basis of entanglement, any method of evaluating an attack based on the measurement of entanglement can be used, in the same way as QKD protocols based on entangled photons (Ekert 1991; Kish et al. 2020). On the other hand, the current use of single photon sources can aid in the detection of certain types of attacks, such as, photon-number splitting attack (Huttner et al. 1995; Brassard et al. 2000). Later, in the security analysis subsection, we will develop our own policy to preserve the integrity of the information transmitted against any type of attack.

Figure 5 shows the internal constitution of Alice’s and Bob’s modules as an example of a symbol B coded in four bits \{b_0, b_1, b_2, b_3\}. Alice’s module begins, from left to right of Fig. 5a, with four ancillas \(|0\rangle\) in qubits \{q[0], q[1], q[2], q[3]\}, which feed a generating source of a GHZ_4 state (Audretsch 2007; Jaeger 2009; Horodecki et al. 2007):

\[\text{Fig. 4} \quad \text{Block diagram of the QKSC protocol, where Alice (sender) works with \(n\) ancillas of the \(|0\rangle\) type, and every symbol B (or sample) is coded in \(n\) classic bits. At the output of Alice, there is a single wire due to the internal use of a multiplexer. Each quantum repeater has its own multiplexer-demultiplexer pair. Bob (receiver) has a demultiplexer after which it performs a measurement that allows the transmitted symbol (or sample) B to be recovered.}\]

\[\text{Fig. 5} \quad \text{Internal representation of Alice’s and Bob’s modules, as an example of four bits to be transmitted, where a consists of four ancillas of the \(|0\rangle\) type in \{q[3], q[2], q[1], q[0]\}, an H (Hadamard) and three CNOTs gates that generate a GHZ_4 state, one Controlled-Z and three CNOTs gates that allow incorporating the four bits \{b_3, b_2, b_1, b_0\} of symbol (or sample) in this module, and one multiplexer (MX) which is a submodule that converts the parallel set of photons (yellow circles) to serial; and b consists of a demultiplexer (DX), i.e., a submodule that converts the serial set of photons to parallel, with three flipped CNOTs and one H gates, and four quantum measurement constituted in practice by single photon detectors, thanks to which the four transmitted bits \{b_3, b_2, b_1, b_0\} of a symbol or sample B, are recovered.}\]
Quantum key secure communication protocol via enhanced…

Until a few years ago, it was experimentally challenging to construct optical multiplexers (MX) and demultiplexers (DX) in the single photon level, however, today there are several successful examples of their implementations (Li et al. 2018; Meyer-Scott et al. 2020; Carpenter et al. 2013; Elshaari et al. 2017; Lenzini et al. 2017). However, QKSC is preserved by a dynamic key present at both ends of the communication system, which allows it to successfully use MX/DX pairs at the multi-photon level (Pan et al. 2020b), and still be immune to attacks by an eavesdropper of the photon-number splitting attack (Huttner et al. 1995; Brassard et al. 2000) type.

The four outputs of the GHZ$_4$ state source are intercepted for three CNOT gates, and a Controlled-Z (CZ) gate in their more significant qubit $q[3]$. This encodes each wire of the GHZ$_4$ state with its corresponding bit of a B symbol. This will be seen in detail in a later section called implementation on two quantum platforms. Then, a multiplexer (MX) converts a parallel flow of photons to a series one, which are represented as little yellow circles. On the other hand, Fig. 5b shows Bob’s module, which begins with a demultiplexer (DX) that converts a series flow of photons to a parallel one. Then, Bob applies a measurement module like that of Fig. 2 between times $t_2$ and $t_3$. This makes it possible to recover the four bits $\{b_0, b_1, b_2, b_3\}$ of a transmitted symbol B.

Figure 6a shows a parallel configuration of a quantum repeater that uses entanglement swapping (ES) in each photon, see Fig. 6b. Entanglement swapping (Żukowski et al. 1993; Pan et al. 1998; Jennewein et al. 2001; Tsujimoto et al. 2018; Jin et al. 2015; Schmid et al. 2009; Riedmatten et al. 2005) is the most frequently used technique in quantum communications (Cariolaro 2015; Dieks 1982; NIST 2014; Yu et al. 2014) for the construction of quantum repeaters (Sangouard et al. 2011; Hasegawa et al. 2019; Munro et al. 2015; Ruihong and Ying 1237; Razavi et al. 2009). In Fig. 6a, the photons’ stream enters to the demultiplexer (DX), which allows the photons to separate in a parallel configuration. Then, each photon enters to an ES module, which extends the range of the link. We can accumulate several ESs, one after the other, within each quantum repeater, or use repeaters of a single ES per qubit and use several quantum repeaters along the link in order to multiply the link range. Finally, all the photons that come out of each ES go to a multiplexer (MX) which aligns them in the quantum channel (QCh).

$$GHZ_4 = \frac{1}{\sqrt{2}} (|0000\rangle + |1111\rangle).$$ (5)
In Fig. 6b, it is possible to see in detail the interior of each ES. Besides, it is also possible to use a configuration that uses a single ES for all four photons at the same time, i.e., a serial configuration like that of Fig. 6c (Sangouard et al. 2011; Hasegawa et al. 2019; Munro et al. 2015; Ruihong and Ying 1237; Razavi et al. 2009), which is applied directly on the quantum channel (QCh) without the need to separate each photon as in the configuration of Fig. 6a thanks to a multiplexer-demultiplexer pair.

Regarding which is the best configuration of quantum repeater: if the parallel of Fig. 6a, or the series of Fig. 6c; this is still a matter of investigation, since it is exclusively a topic linked to the implementation of the repeaters, which depends on the communication system design factors associated with the distance to be covered and the type of repeaters selected, which are based on lines of optical fiber, or via space link. In the case that the distribution of entangled photons takes place thanks to lines of optical fiber, it is necessary to use repeaters every 50 km due to the losses in the fiber, an attenuation in the material, and a propagation speed \(v\) equal to 2/3 of the speed of light \(c\), while satellite repeaters can cover greater distances at a speed \(v = c\), with less attenuation and losses than in the case of optical fiber except for relative environmental aspects to the ground-sky link, i.e., clouds that can disrupt the distribution of entangled photons.

QKSC can interchangeably use any of the quantum repeater configurations mentioned in Fig. 6. Besides, it can even use a more direct family which is presented here as an alternative version, and that is shown in Fig. 7. The configurations of Fig. 7 work according to a completely different criterion than those in Fig. 6. These techniques base their operation on two main characteristics:

(a) Old photons which come in and new ones which come out, and
(b) They only work forward, i.e., there are no quantum repeaters in the middle of the quantum channel (QCh) distributing entangled photons back and forth in order to use the transitivity of entanglement swapping (Zukowski et al. 1993; Pan et al. 1998; Jennewein et al. 2001; Tsujimoto et al. 2018; Jin et al. 2015; Schmid et al. 2009; Riedmatten et al. 2005).

The configurations shown in Fig. 7 are exclusively parallel, where the photons that come from the demultiplexer (DX), and at the same time from the quantum channel (QCh), interact with \(GHZ_4\) states and after a measurement process new photons are obtained with the same attributes with which they went out from Alice’s module. Versions of Fig. 7a, c, and e are perfectly interchangeable between them, while Fig. 7b, d, and f are their equivalent and simplified versions, respectively. In fact, in a later section called implementation on two quantum platforms, we will use the simplified version of Fig. 7b in order to simplify implementations on both platforms. Finally, a multiplexer converts the organization of the resulting photons from a parallel to a series configuration, so that they continue their journey on the quantum channel.

To summarize, the quantum repeater scheme proposed in Fig. 7 represents a relay mechanism of old photons for new ones, exclusively forward, in which, as in the case of the quantum repeaters (Sangouard et al. 2011; Hasegawa et al. 2019; Munro et al. 2015; Ruihong and Ying 1237; Razavi et al. 2009) commonly used in practice such as those from Fig. 6, it will require quantum memories (Pastawski 2012) for its optical implementation in order to compensate for differences in the arrival time of each photon.
3.1 QKSC protocol

Based on Fig. 4, we can define this protocol as a procedure for the case where the quantum channel is a line of optical fiber, where we can analyze the status of the quantum channel at the beginning and end of each module:
where \( \text{range} \) is the distance between sender and receiver, \( QCh(t) \) is the quantum channel status in each time, \( B(t) \) is the symbol to be transmitted in each time, \( n \) is the size of the symbol \( B \), i.e., the number of bits to be transmitted, \( O_{\text{Alice}} \) is the Alice’s oracle, subscript QR means quantum repeaters, \( O_{\text{QR}} \) is the QR’s oracle, \( O_{\text{Bob}} \) is the Bob’s oracle, \( t \) is the time, \( r \) is the accumulator associated with the number of quantum repeaters, and 50 km represents the distance between modules in case of working with lines of optical fiber.

As we can see, the procedure described above is simple, however, we need to take into account an important detail, which consists of the inside of Alice’s module, in which case, we have to generate \( \text{GHZ}_n \) states. If \( n \) is a large number, the implementation of Alice’s module may seem a complicated task in practice. However, through a configuration as in the work of Prof. Pan (Li 2020) group, which generates \( \text{GHZ}_4 \) states, we can extend this to a general case of \( \text{GHZ}_{2^k} \) (\( k \) is the level of splitting) states from a single-photon source and an optical demultiplexer. This implies a pulse laser with a central wavelength around 893 nm excites the quantum dot resonantly through a fiber-coupled confocal microscope system, polarizing beam-splitter, half- and quarter-wave plates, Pockels cell, and mirrors for its implementation. In Fig. 8a, a quantum circuitry interpretation of this configuration is presented, while Fig. 8b–e, are extensions of the mentioned configuration for the case of \( \text{GHZ}_8 \) is developed through four equivalent quantum circuits.

Finally, all this simplicity could be transferred to the work of an eavesdropper, even working with sources that generate the minimum necessary amount of photons, which apparently would protect the configuration of a photon-number splitting attack (Huttner et al. 1995; Brassard et al. 2000), for which we must do a more exhaustive analysis of security.

### 3.2 Security analysis

Since QKSC bases its entire operation on entangled photons, it is possible to consider measures to prevent the negative effects of the intervention of eavesdroppers of the type:

(a) Entanglement measurement as in the case of Ekert 91 (E91) protocol (Ekert 1991),

(b) The use of the exact, minimum and necessary number of photons in order to prevent interventions like photon-number splitting attacks (Huttner et al. 1995; Brassard et al. 2000).
Fig. 8 Circuitry interpretation of $\text{GHZ}_k^4$ ($k$ is the level of splitting) states generation from a single-photon source and an optical demultiplexer, where: a is the representation of the example of $\text{GHZ}_4$ presented in the paper of Prof. Pan (Li 2020) group, while from b to e are representing, with the same criterion, four equivalent versions of $\text{GHZ}_8$. 
However, if we consider the transmission losses either in lines of optical fibers, or via a space link, we will find that in order to prevent an attack we expose ourselves to the loss of critical photons, thus compromising the integrity of the message, therefore, QKSC contemplates the possibility of using a multiple-photon source accompanied by a key $K$, that is shared between Alice (sender) and Bob (receiver), and that should only be transmitted the first time via:

(i) A manual procedure, i.e., in a pre-arranged way, or
(ii) Through the use of a QKD protocol, either polarized (Bennett and Brassard 1984; Zhang and Ni 2020), or entangled (Ekert 1991; Kish et al. 2020) photons.

QKSC protocol itself transmits its next keys, starting, inclusive, with the second key. In Fig. 9, a generic block diagram using a key on Alice (sender) and Bob (receiver) is established.

As we can see, scheme of Fig. 9 is similar to that of Fig. 4, where the intervention of the key $K$ only affects Alice’s and Bob’s modules, and not to quantum repeaters.
Figure 10 shows the internal representation of Alice’s and Bob’s modules with the intervention of a key $K \{k_3, k_2, k_1, k_0\}$, as an example of four bits to be transmitted $\{b_3, b_2, b_1, b_0\}$, where the only difference with the modules of Fig. 5 consists in the incorporation of the key $K \{k_3, k_2, k_1, k_0\}$ on Alice’s and Bob’s qubits $\{q[3], q[2], q[1], q[0]\}$. This incorporation is via three CNOTs, and one Controlled-Z gate on the most significant qubit $q[3]$ of both modules. Moreover, in the case of Alice’s module the key $K$ is incorporated after the symbol $B$ and before the multiplexer (MX), in the case of Bob’s module, the key $K$ is incorporated after the demultiplexer (DX) and before the measurement that Bob must take to retrieve the transmitted symbol $B$.

The example of Fig. 10 is extensive to symbols and keys of any size, with the sole exception of the number of qubits supported by the host platform. In this work, we will implement the QKSC protocol in the section called implementation on two quantum platforms, where said platforms will be Quirk simulator (Algorithmic Assertions 2020), of 16 qubits, and a 16-qubits IBM Q processor (IBM Q Experience 2020), called Melbourne, which has the highest number of qubits of free access in the IBM Q series non-Premium quantum processor family. Therefore, these platforms will condition our ability to test the protocol with large symbols and keys, e.g., for 1024, 2048, 4096 or more bits. Furthermore, in real implementations carried out through optical circuits (Furusawa and Loock 2011), the use of quantum memories (Pastawski 2012) should be considered, both in the sender and in the receiver. For example, on the receiver’s side it is necessary to keep the current key until the symbol to be decrypted arrives.

Finally, the optical implementation of the QKSC protocol, i.e., Alice’s and Bob’s modules, and the details about the constitution of optical quantum repeaters based on Bell state measurement (BSM) modules, quantum memories, and photon detectors are outside the scope of this study, however, it is important to take into account recent experiments carried out by Prof. Pan’s group, in which optical quantum repeaters are implemented without the use of quantum memories (Li et al. 2019).

### 3.3 QKSC protocol with a static key

Based on Fig. 9, we can define a version of this protocol as a procedure that uses a key for the case where the quantum channel is a line of optical fiber. We can analyze the status of the quantum channel at the beginning and end of each module as in the keyless case:

\[
\begin{align*}
  t &= 0, \quad QCh(t) = |0\rangle^{\otimes n}, \\
  t &= t + 1, \quad QCh(t) = O_{Alice}[B(t), K, |0\rangle^{\otimes n}], \\
  t &= t + 1, \\
  r &= 0, \\
  \text{while}(\text{range}-50\text{ km}) > r, \\
  &\{ \\
  &\quad QCh(t) = O_{QR}[QCh(t - 1)], \\
  &\quad r = r + 50\text{ km}, \\
  &\quad t = t + 1, \\
  \} \text{end while}, \\
  B(t) &\leftarrow QCh(t) = O_{Bob}[QCh(t - 1), K].
\end{align*}
\]
where $K$ is an $n$ bits shared key, which is previously distributed between Alice and Bob thanks to any QKD protocol (Bennett and Brassard 1984; Zhang and Ni 2020; Ekert 1991; Kish et al. 2020), any other QSDC protocol (Long and Liu 2002; Deng and Long 2004; Zou et al. 2020a; Zhou et al. 2020; Xie 2020; Chen et al. 2018; Zou and Qiu 2014; Yan et al. 2020; Wei et al. 2006; Qi et al. 2019), or manually, i.e., pre-arranged. After that, any new innovation of the key will be via QKSC itself using the last key to protect the transmission. Finally, in the procedure described above, the only modules impacted by the key are those of Alice and Bob, since the quantum repeaters are identical to those used in the keyless version of this procedure.

### 3.4 QKSC protocol with a dynamic key

Based again on Fig. 9, we can define a new version of this protocol as a procedure that uses a dynamic key for the case where the quantum channel is a line of optical fiber. Then, we need to define what criteria we will base on to dynamically evolve the key, for which we highlight the best way to do it among an innumerable number of them. The first key $K(0)$ is generated thanks to a QRNG, distributed manually, via any QKD protocol (Bennett and Brassard 1984; Zhang and Ni 2020; Ekert 1991; Kish et al. 2020), or via any other QSDC protocol (Long and Liu 2002; Deng and Long 2004; Zou et al. 2020a; Zhou et al. 2020; Xie 2020; Chen et al. 2018; Zou and Qiu 2014; Yan et al. 2020; Wei et al. 2006; Qi et al. 2019), while from the second one onwards, the current key $K(t)$ is calculated from an XOR operation between the previous symbol $B(t−1)$ and the previous key $K(t−1)$, i.e., $K(t) = B(t−1) \lor K(t−1)$, that is, the complete scheme is a conditional of the type:

$$
\begin{align*}
\text{if } t &= 0, \\
K(t) &= K(0), \\
\text{else} \\
K(t) &= B(t−1) \lor K(t−1), \\
\text{end if}.
\end{align*}
$$

Reviewing the four dynamic key proposals mentioned above, we can see that we have gone from the highest to the lowest in the exposure of the key in the channel, since in the first option each key generated must be distributed and therefore exposed in the channel, while in the case of the last option, the exposure is minimal because the first key is distributed only, while from that moment on the key is dynamically and independently updated in a synchronized and simultaneous way in both Alice’s and Bob’s side without the need of any transmission. Therefore, based on the fourth option, we will modify the QKSC protocol with the inclusion of the dynamic key:
$$t = 0, \ QCh(t) = |0\rangle^{\otimes n},$$

$$t = t + 1, \ QCh(t) = O_{Alice}[B(t), K(t), |0\rangle^{\otimes n}],$$

$$t = t + 1,$$

$$r = 0,$$

while\(\text{range}-50\ km > r,$$

$$\{\$$

$$QCh(t) = O_{QCh}[QCh(t - 1)],$$

$$r = r + 50\ km,$$

$$t = t + 1,$$

$$\} \text{ end while,}$$

$$B(t) \leftarrow QCh(t) = O_{Bob}[QCh(t - 1), K(t - 1)].$$

Moreover, since experiments indicate that the key does not introduce noise, we can use it permanently, even in a broader security context. Finally, for both static and dynamic keys (ignoring the presence of MX/DX) the Oracle and outcomes of Alice and Bob will be:

$$O_{Alice} = O_{Alice,2} \ O_{Alice,1}$$

$$O_{Alice,1} = (X^h_0 \otimes I^{8 \times 8})(I^{2 \times 2} \otimes X^h_1 \otimes I^{4 \times 4})(I^{4 \times 4} \otimes X^h_2 \otimes I^{2 \times 2})(I^{8 \times 8} \otimes Z^b_3)$$

$$O_{Alice,2} = (X^h_0 \otimes I^{8 \times 8})(I^{2 \times 2} \otimes X^h_1 \otimes I^{4 \times 4})(I^{4 \times 4} \otimes X^h_2 \otimes I^{2 \times 2})(I^{8 \times 8} \otimes Z^b_3)$$

$$\{q[0], q[1], q[2], q[3]\} = QCh = O_{Alice}|GHZ_4\rangle$$

$$O_{Bob} = O_{Bob,2} \ O_{Bob,1}$$

$$O_{Bob,1} = (X^h_0 \otimes I^{8 \times 8})(I^{2 \times 2} \otimes X^h_1 \otimes I^{4 \times 4})(I^{4 \times 4} \otimes X^h_2 \otimes I^{2 \times 2})(I^{8 \times 8} \otimes Z^b_3)$$

$$O_{Bob,2} = (I^{8 \times 8} \otimes H)(I^{4 \times 4} \otimes CX^\text{flipped})(I^{4 \times 4} \otimes SW)(I^{2 \times 2} \otimes CX^\text{flipped} \otimes I^{2 \times 2})$$

$$\{q[0], q[1], q[2], q[3]\} = O_{Bob} \ QCh = \{b_0, b_1, b_2, b_3\}$$

where $CX^\text{flipped}$ is a flipped CNOT gate (control and target qubit are reversed), and SW is a SWAP gate.

### 4 Implementation on two quantum platforms

In this section, we will carry out a series of experiments without and with the use of a key previously distributed between Alice’s and Bob’s modules. In all cases, we will work with three-bit symbols for reasons of limitation in the number of qubits supported by the two platforms on which we will carry out the aforementioned implementations: Quirk simulator (Algorithmic Assertions 2020), and 16-qubits Melbourne IBM Q processor (IBM Q Experience 2020). Quirk was chosen for being the most powerful non-commercial platform in terms of its visual expression and the number of metrics it uses to evaluate the outcomes of the experiments, while in the case of Melbourne, in addition to being the non-Premium processor with the greatest number of qubits of the IBM Q (IBM Q Experience 2020) family, which implies greater decoherence and errors compared to the series of
Premium processors from the same company, it is a physical machine which will allow us to analyze the performance of the novel in a real environment. On the other hand, in all the experiments, we will compare the results obtained with Melbourne and the IBM Q simulator (IBM Q Experience 2020), which delivers identical results to Qiskit (IBM Q Experience 2020), in order to check the deterioration introduced in Melbourne by decoherence (Schlosshauer 2005), and different types of errors like bit-flip, phase-flip, and bit-phase-flip (Korotkov 2017).

Finally, all the implementations in this section will have the following points in common:

- it is not possible to implement both the multiplexer (MX) and the demultiplexer (DX), for reasons related to their construction and operation, so their implementations will be exclusively in charge of an optical version,
- the symbol $B = \{b_2 = 0, b_1 = 1, b_0 = 1\}$ to be transmitted will be the same in all experiments, and
- the GHZ base will be the same in all cases, that is,

$$GHZ_3 = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle).$$

\[ (6) \]

4.1 Keyless with only one quantum repeater

Figure 11 shows an implementation of QKSC protocol on Quirk simulator (Algorithmic Assertions 2020) transmitting the mentioned symbol B. Alice’s side first stage consists in the symbol preparation where we can build CBS as $|1\rangle$ thanks to NOT gates (i.e., Pauli’s inverter X) after the ancillas $|0\rangle$. Then, we use quantum measurements to obtain the bits of the symbol $B$ from their respective CBS of Eqs.(1 and 2). The second stage is reserved for the $GHZ_3$ state generation, like that of Eq. (6). The third and last stage of Alice’s side inserts the elements of symbol $B = \{b_2 = 0, b_1 = 1, b_0 = 1\}$ as control bits in two CNOT

![Fig. 11 QKSC implementation on Quirk simulator, keyless, and with only one quantum repeater](image-url)
gates and one Controlled-Z gate, while the GHZ$_3$ states enter the same gates but at their target qubits.

The second module belongs to the only quantum repeater implemented in this experiment, which corresponds to the simplified version of Fig. 7b but for three qubits and not including the multiplexer (MX) or the demultiplexer (DX) used in said figure.

Finally, in the third module Bob makes the measurement after two flipped CNOTs and one Hadamard (H) gates, obtaining the same bits that were generated in Alice’s first module. We must remember that Quirk simulator is an ideal environment without decoherence or noise, which only allows us to evaluate the logical feasibility of the protocol. Therefore, for a more realistic evaluation about the operation of the QKSC protocol on a physical machine we must resort to a platform like 16-qubits Melbourne IBM Q processor (IBM Q Experience 2020), where Fig. 12 shows its connectivity map, with the single-qubit U2 and CNOT error rates in detail.

In Fig. 13, an implementation of the QKSC protocol on the IBM Q platform is presented, where the fundamental differences with the implementation on Quirk simulator are the following:

**Fig. 12** Connectivity map of the 16-qubits Melbourne IBM Q processor (IBM Q Experience 2020), with the single-qubit U2 and CNOT error rates in detail

**Fig. 13** QKSC implementation on IBM Q, keyless, and with only one quantum repeater
• We have eliminated the measurements of the first stage of Alice’s side, which converted CBS into their respective bits, so as not to dilate the histograms of Fig. 15, which corresponds to the execution on Melbourne processor, so as not to complicate the reading of their outcomes, and
• we implement the Controlled-Z gate of the most significant qubit of the third stage of Alice’s module thanks to one CNOT gate, and two H gates (before and after the target qubit of the CNOT gate).

As in Quirk, the metrics to the right of Fig. 13, i.e., circles in gray and/or blue, show that the upper three qubits (to be transmitted) and the lower three (transmitted) coincide, which indicates they have been transmitted successfully.

Figures 14 and 15 show the outcomes of Fig. 13 when its circuits is ran on the IBM Q simulator and 16-qubits Melbourne quantum processor, respectively. In both cases, with 8192 shots and fairshare as the run mode. However, while Fig. 14 shows 100% of probability in $b_2b_1b_0 = 110$, Fig. 15 has 71.241% of probability in $b_2b_1b_0 = MM0$, and 28.759% of probability in $b_2b_1b_0 = MM1$, where M is a meta-symbol that represents 0 and 1, at the same time. This important dispersion in the outcomes of the 16-qubits Melbourne IBM Q processor compared to those obtained with the IBM Q simulator is a direct consequence of decoherence (Schlosshauer 2005) and the aforementioned flip errors (Li et al. 2019) present in Melbourne processor.

### 4.2 Keyless, with two quantum repeaters

Figures 16 and 17 show the implementation of the QKSC protocol on Quirk simulator, and IBM Q, respectively, without a key, and with two quantum repeaters. In both implementations, the coincidence between the bits to be transmitted, i.e., those higher qubits corresponding to Alice’s first stage, and those received in the lower qubits on Bob’s side, is total. In Quirk, the verification is automatic thanks to its clear visual metrics, while in IBM
Q the circles on Bob’s side mean: $b_2b_1b_0 \equiv \text{blue-blue-gray} \equiv 110$, which are the correct outcomes.

As in the previous experiment, with a single quantum repeater, Fig. 18 shows the results presented by the IBM Q simulator, which are perfect with a 100% probability at $b_2b_1b_0 = 110$, and 0% for the rest of CBS. The problem arises when we analyze the outcomes delivered by the 16-qubit Melbourne IBM Q processor, which corresponds to less than 60% effectiveness, i.e., 59.497%, with more than 40% error. This increase in error with respect to the previous experiment has to do with the number of CNOT gates incorporated when adding the second quantum repeater, which adds bit flip errors (Korotkov 2017), deteriorating the quality of outcomes.

4.3 Key, and only one quantum repeater

In Figs. 19 and 20 the implementations of the QKSC protocol are represented with a key and one quantum repeater only, for Quirk simulator (Algorithmic Assertions 2020), and IBM Q (Experience 2020), respectively, where the symbol B is the same used in the last experiments, i.e., $b_2b_1b_0 = 110$, while the key K will be $k_2k_1k_0 = 101$. As in the previous cases, the metrics of both platforms indicate the success of the transmission, with 100% effectiveness. However, we must evaluate the impact of decoherence and flip type errors thanks to the intervention of more gates of the CNOT and Controlled-Z type in the Alice’s (sender), and Bob’s (receiver) modules on a physical platform like 16-qubits Melbourne IBM Q.

In Fig. 21, it is possible to see an identical performance to those obtained in the implementations of Figs. 14 and 18 for the keyless cases with one and two quantum repeaters, respectively. On the other hand, Fig. 22 shows the outcomes obtained in the IBM Q Melbourne processor, in which the impact of decoherence and flip errors is evident. However,
Fig. 16 QKSC implementation on Quirk simulator, keyless, and with two quantum repeaters
Fig. 17 QKSC implementation on IBM Q, keyless, and with two quantum repeaters
the values of Fig. 22 resemble those of Fig. 15 (keyless with only one quantum repeater), being much higher in performance than those of Fig. 23 (keyless with two quantum repeaters). This establishes the suspicion that the key does not seem to be responsible for the drop in the performance, but rather the quantum repeaters, for which we must carry out a final experiment with a key and two quantum repeaters to confirm this hypothesis.

4.4 Key, and two quantum repeaters

This configuration is represented with a performance of 100% in Figs. 24 and 25 on Quirk simulator (Algorithmic Assertions 2020), and IBM Q (IBM Q Experience 2020), respectively. Therefore, the important thing is to verify the hypothesis about who is responsible for the drop in performance on the Melbourne processor.

Figure 26 does not help in the verification of the pending hypothesis because, like Figs. 14, 18 and 21, it shows the exact outcomes that would be expected for this case, i.e., with a probability of 100% at $b_2b_1b_0=110$. Instead, Fig. 27 shows that the hypothesis is correct given the high level of decoherence in its outcomes. In fact, if the previous experiments were not available and the only information at hand were the outcomes of this figure, an exact conclusion about the performance of the QKSC protocol could not be drawn. However, we must gather all the evidence from the four experiments in an integrative scheme to evaluate the situation more clearly in a comparative way and draw conclusions about who the responsible for the poor performance in the Melbourne IBM Q processor implementation is and why.

4.5 Analysis of outcomes

The four previous experiments are summarized in Table 2 and Fig. 28, where the outcomes were grouped according to the use or not use of a key, for one or two quantum repeaters,
Fig. 19 QKSC implementation on Quirk simulator, with key, and only one quantum repeater
Fig. 20  QKSC implementation on IBM Q, with key, and only one quantum repeater.
on the IBM Q simulator or Melbourne. In particular, Fig. 28 highlights the errors in red, showing that the responsible for them is the second quantum repeater and not the key. This is mainly due to the fact that each quantum repeater involves a large number of CNOT gates, which introduce bit flip errors to which Melbourne is extremely sensitive.

4.6 QKD vs QKSC in a real context

In Fig. 29, we can observe a comparative analysis in the use of QKD and QKSC protocols in a real and conspicuous case (Mastriani et al. 2021) of secure quantum communication. Alice (A) and Bob (B) are in two allied submarines, trying to communicate between each other through a quantum satellite. The submarines are submerged and are connected to their respective buoys on the surface, Alice in red and Bob in blue, using resistant cables to the elements of the environment. Eve’s not-ally submarine (E) with its respective black buoy is submerged, silent and pre-existing to the arrival of Alice’s submarine in the area. All the buoys are tiny in real life but exaggerated in size in Fig. 29 and just barely rise above the surface of the sea. Eve’s submarine is far enough away so as not to be detected by Alice’s sonar, and close enough to be under the coverage area, in pink in Fig. 29a, due to the electromagnetic radiation of the classic channels (PCh: Public, and DCh: Data) that Alice and Bob will use to share a key via a QKD protocol and transmit encrypted information using that key.

As we have seen in Fig. 3a, QKD protocols require three channels: Quantum (QCh), public (PCh), and data (DCh) channels in order to distribute a key, and send the encrypted message based on that key. Obviously, if we were to use a QKD-based cryptographic system to communicate to Alice’s and Bob’s submarines, we would have to resort to a configuration like the one in Fig. 29a, where the orange rays represent the polarized or entangled photons required by the QKD protocol, while the rays in gray represent the classic PCh and DCh channels. On the other hand, as we mentioned in the first section, the QKD protocols have four loopholes related to the excessive exposure of the key in the channels, which is
consistent with the problem posed in Fig. 29a. Therefore, we must consider an alternative based on the best tools available, using a CubeSat of 6 units developed by CIS-FIU (School of Computing and Information Sciences 2020), with a low Earth orbit (LEO) at an altitude of 500 km with several minutes of presence between both allied submarines. This platform uses a double telescope to make focus on both allied submarines at the same time.
Fig. 24  QKSC implementation on Quirk simulator, with key and two quantum repeaters
Fig. 25 QKSC implementation on IBM Q, with key and two quantum repeaters
with a footprint of 200 m on each one. Based on this platform it is possible to use a cryptographic protocol with fewer channels like QKSC, which results in a simplification of the Cubesat and the buoys associated with each submarine. Thus, the combination established between the aforementioned Cubesat and the QKSC protocol (with a dynamic key like the one explained above) seems to be the ideal solution, although several alternatives arise taking into account the transmission of the first key, and the reduced footprint generated by that Cubesat:

(a) the first key is not transmitted, but was pre-agreed before the submarines set sail,
(b) the first key is transmitted directly to both allied submarines thanks to a multi-photon source (Pan et al. 2020b) and without any protocol, emphasizing the little footprint,
(c) similar to the previous case but using a single-photon source (Zou et al. 2020b; Li and Long 2020; Hu et al. 2016),
(d) the first key is transmitted via a QKD protocol using a multi-photon source (Pan et al. 2020b), emphasizing the little footprint again, or
(e) similar to the previous case but using a single-photon source (Zou et al. 2020b; Li and Long 2020; Hu et al. 2016).

Based on these tools, we would be in a configuration like that of Fig. 29b, where the security would be total, since the exposure of the key and the message would be practically null, since it is impossible for Eve’s submarine and buoy not to be detected being at a distance of less than half a kilometer from Alice’s submarine and buoy.

4.7 Non-distributable key sharing in QKSC

Below, an example of how to generate synchronized keys at both ends of the QKSC protocol, without resorting to a distribution of the keys as in the case of QKD, is presented. There are several techniques of non-distributable key sharing (NDKS) (Mastriani 2205);
in this case, we will resort to a simple yet extremely robust procedure of NDKS, from the point of view of cybersecurity, based on chaos (Barnett et al. 2015) operators. The selected NDKS procedure proceeds as follows:

1. At the moment of establishing the first link between two points A and B, which generally coincides with the moment of the foundation of both points, and only that time, we share two top-secret parameters \( \{ \lambda \in \mathbb{R}, x_0 \in \mathbb{R} \} \) of a chaos operator called \( f : \mathbb{R} \to \mathbb{R} \), which results,

\[
x_{t+1} = f(x_t) = \lambda x_t (1 - x_t), \tag{7}
\]

where \( \lambda \) is the growth factor (Barnett et al. 2015), with \( \lambda \in [0, 4] \), and \( (1 - x_t) \) is named the limiting factor (Barnett et al. 2015), with \( x_t \in [0, 1] \ \forall t \), and as can we appreciate, Eq. (7) has an iterative nature.

2. We need to establish the period of the orbit (Barnett et al. 2015), i.e., the number of times we recursively apply the selected operator, or the level of composite operators, e.g., 2, 4, or more times. Therefore, if Eq. (7) corresponds to an orbit of period 1, those of periods 2 and 4 will be, respectively:

\[
x_{t+1} = f^2(x_t) = f \circ f(x_t) = \lambda f(x_t)(1 - f(x_t)), \tag{8}
\]

\[
x_{t+1} = f^4(x_t) = f^2 \circ f^2(x_t) = \lambda (\lambda f(x_t)(1 - f(x_t)))(1 - (\lambda f(x_t)(1 - f(x_t)))) \tag{9},
\]

where each independent variable of the following operator is replaced by the previous operator.

3. Set the size of the keys, e.g., \( N \), for a pair of randomly selected parameters, e.g., \( \{ \lambda = 4, x_0 = 0.01 \} \) shared and involved in a period of a given orbit, for example, 4, i.e., that of Eq. (9), and 100 pieces of a message to be encrypted of \( N \) bits each piece. Then, Fig. 30 results.

We resort to Python (Python Language 2022) because it is a high-level language, which has no limit on the number of decimal places that can be used, and whose only limitation in this regard is found in the processor’s memory. In this way, we obtain 100 numbers from Eq. (9) with \( N \) decimal places each, like those represented in Fig. 30, where the first 10 result:

\[
\begin{align*}
  x_1 &= 0.99898385618784746... \\
  x_2 &= 0.23841808206575010... \\
  x_3 &= 0.90814669199264297... \\
  x_4 &= 0.95478937871686020... \\
  x_5 &= 0.07992833032586151... \\
  x_6 &= 0.98410844673313658... \\
  x_7 &= 0.80957230709414696... \\
  x_8 &= 0.65401754166355985... \\
  x_9 &= 0.35336619198049213... \\
  x_{10} &= 0.47506120805078567...
\end{align*}
\]
4. Finally, we will build a key \( (k_t) \) for each \( x_t \) as follows: taking \( x_1 \) as an example, from its decimal point to the right, we will analyze each decimal of \( x_t \) in such a way that if it is even, the corresponding key, in this case \( k_1 \), will have a 0 (zero) in that position. Instead, if the decimal parsed of \( x_1 \) is odd, \( k_1 \) will have a 1 (one) in that position. Then, the resulting keys in order are:

![Quantum key secure communication protocol via enhanced…](image)

**Fig. 27** IBM Q Melbourne processor. Upper figure: Histogram (measurement probabilities) in terms of computational basis states, with \((16.003 + 11.56 + 15.027 + 10.657\%) = 53.247\%\) of probability in \( b_2b_1b_0 = MM0 \), and \((13.33 + 11.157 + 12.463 + 9.802\%) = 46.752\%\) of probability in \( b_2b_1b_0 = MM1 \), where \( M \) is a meta-symbol that represents 0 and 1, at the same time. The difference of almost 47\% between the simulator and Melbourne processor shows decoherence of the latter for this experiment. Lower figure: Run details of simulator execution, with 8192 shots, and fairshare run mode.

| CBS         | Keyless, 1 QR Simulator | Keyless, 2QRs Simulator | Key, 1 QR Simulator | Key, 2QRs Simulator |
|-------------|-------------------------|-------------------------|---------------------|---------------------|
|             | Melbourne               | Melbourne               | Melbourne           | Melbourne           |
| 110         | 100%                    | 71.241%                 | 100%                | 71.313%             |
| rest        | 0%                      | 28.758%                 | 0%                  | 28.687%             |

*QR* Quantum repeaters, and *CBS* Computational basis states
4.8 QKD vs QKSC, when it comes to installation and maintenance costs

The keys mentioned in Eq. (11) will be present simultaneously at both ends of the channel, at the same time, perfectly synchronized and without the need for any distribution as in the case of the QKD protocols. In other words, with this technology, the channels (classical or quantum) are never used for key distribution. With the same criteria, quantum repeaters are only used to increase the transmission range of the encrypted message, and not for the distribution of keys, saving the time of use of the different channels, saving channels, simplifying the infrastructure, its cost, and maintenance.

Keeping in mind the future quantum Internet (Caleffi et al. 2020, 2018; Chandra et al. 2012; Cacciapuoti et al. 2020a, 2020b; Caleffi and Cacciapuoti 2020; Cuomo et al. 2020; Ferrari et al. 2021; Chakraborty et al. 1907; Wehner et al. 2018; Dür et al. 2017; Kimble...
Quantum key secure communication protocol via enhanced…

Fig. 29 A quantum satellite to communicate Alice (a red buoy on sea in point A) and Bob (a blue buoy on sea in point B). Besides, there is a third ship, the Eve submarine (E), silent, submerged and pre-existing in the Alice’s area. Therefore, two alternatives emerge: a the not ally submarine is at an appropriate distance from Alice’s one, i.e., close enough to be affected by the electro-magnetic shadow associated to the satellite footprint (pink triangular sector), and far enough not to be detected by Alice, thus being able to decode and thus alter the bits of the public and data channels used by the QKD protocol, instead, b using a satellite with a fully optical channel, i.e., quantum channel (QCh), which can focus exclusively on Alice’s buoy for transmission and reception of the entangled photons used by QKSC, the not ally submarine has no chance of altering the communication between Alice and Bob. Otherwise, the orange rays in (a) and (b) represent the entangled photons scattered across the satellite, while the brown rays represent the cables between the buoys and the submarines, which are subjected to great forces of stretching and compression, as well as mechanical degradation due to exposure to the environment. Moreover, in (a), the gray rays represent the electromagnetic links that drives the transmission of the classic bits that Alice needs to rebuild the transmitted keys, via a QKD protocol, and then the message, while the black ray represents the intervention of the not ally submarine in the electromagnetic channel, whereas, in (b) the yellow ray represents the only intervening channel (optical link). They are the Alice’s and Bob’s buoys that reconstruct the transmitted information and emit them to the submarines. Finally, all the elements of the figures are out of proportion in order to make them more visible.

Gyongyosi and Imre 2020, 1905a, 1905b), which will undoubtedly be purely optical, this protocol is ideal to ensure the integrity of the data that travels through it without
having to deal with the problems present in any QKD implementation (Mastriani 2020). In this regard, the National Security Agency (NSA) (2022) highlights the following technical limitations of the QKD protocols:

- Quantum key distribution is only a partial solution,
- Quantum key distribution requires special-purpose equipment,
- Quantum key distribution increases infrastructure costs and insider threat risks,
- Securing and validating quantum key distribution is a significant challenge, and
- Quantum key distribution increases the risk of denial of service.

In response to the observations made by the NSA regarding the practicality and effectiveness of the QKD protocols, QKSC + NDKS does not suffer from a denial of service, since this technology provides for the use of the channel for the transmission of encrypted information when that channel is being shared with the eavesdropper. On the other hand, QKSC + NDKS does not require special-purpose equipment, does not increase the infrastructure costs and insider threat risks, does not require securing and validating quantum key distribution, because the keys are never distributed, and lastly, it is a complete solution, as far as key sharing is concerned, and not partial as is the case of QKD.

Another problem with QKD protocols is what is known as key distillation (Mastriani 2020). This procedure is applied in order to ensure that the key that is finally shared at both ends of the channel is not also shared with an eavesdropper. The problem is that the repeated application of key distillation significantly reduces their size, which implies repeatedly using the QKD protocol in order to finally arrive at a key of satisfactory size. Moreover, if we are talking about a Space-QKD-type configuration through the intervention of a Low-Earth-Orbit (LEO) satellite, such as the 500 km altitude CubeSats (Mastriani 2020), which distributes entangled or polarized photons, the problem is even more aggravated, given that the laser on board the CubeSat (no matter how powerful it may be)

Fig. 30  Chaos operator of Eq. (9) in terms of each instant $t$ (i.e., for each key) with $r=4$, and $x_0=0.01$
cannot compete with the sun in terms of transmittance, regardless of the wavelength (Mastriani 2205) used, which eliminates the possibility of sharing keys through a protocol of QKD during the day. Nor can such distribution be carried out on a cloudy night or in areas of very high contamination and/or atmospheric pollution, which makes the distribution of keys of the desired size an almost insurmountable challenge in a distillation context, since the satellite would have to perform several orbits in order to complete the task of distributing a secure key only among the allowed points. When we say that the CubeSat should make several orbits, we can speak of several days or weeks depending on the region of the planet, the season of the year, the climate, and the level of environmental pollution. As we have seen in the previous subsection, QKSC+NDKS is absolutely immune to any key distribution problem through space, between space and Earth, or through fiber optic lines, since no key is ever distributed.

Based on everything said so far, in the QKD protocols the key is distributed from time to time, while in the case of QKSC+NDKS, the key changes with each portion of the message of a similar size to that of the generated key, that is, we are in the presence of a dynamic encryption system (i.e., a different key for each portion of a message to be encrypted), well above the security performance of the QKD protocols, which exclusively work with static encryption (i.e., the same key for several messages to be encrypted). Finally, a complete study of the problems related to the practical implementation of the QKD protocols can be found in a recent article on NDKS (Mastriani 2205).

5 Conclusions and future works

5.1 Conclusions

There are several versions of Quantum Secure Direct Communication (QSDC) (Cao et al. 2012; Ola et al. 2009; Li et al. 2015; Wen and Long 2007; Xiu et al. 2009) based on the Super-dense Coding protocol (Bennett et al. 1993; Nielsen and Chuang 2004; Kaye et al. 2004; Stolze and Suter 2007). All of them have a formidable performance of transmission, but with a defect which blocked its use. Said defect is the lack of a key in the presence of an eavesdropper on the channel. Taking these results as a reference, we present here a new protocol called QKSC, which is based on an improvement made over the Super-dense Coding protocol with a dynamic key in order to extend its original performance to an unlimited number of bits to be transmitted and preserving the security in the presence of an eavesdropper in the channel. Among the advantages introduced by the novel, we can highlight the following:

• Independently of the use of an authentication channel, which is common in all protocols of Quantum Cryptography, QKSC only adopts one (QCh) of the three (QCh, PCh, DCh) channels used by a QKD-based cryptographic system,
• This is the first protocol of Quantum Cryptography that is presented with a dynamic key, where it changes with the randomness of the message and the previous key,
• It does not transmit the key, i.e., the key is never exposed as it happens in the QKD protocols,
• QKSC protocol is simple to implement, cheap and a low maintenance solution, compared with any QKD protocol,
• This is a complete communication, and data security system,
• Unlike a traditional QSDC system, where part of the data used by the protocol goes back and forth between sender and receiver in order to complete its operation, QKSC is an exclusively forward procedure, i.e., QKSC only uses one of the two branches of the QCh used by a QSDC protocol, however, it is easy to develop a bidirectional version of this protocol based on a practical antecedent such as that of Massa et al. (Massa et al. 1802; Santo and Dakic 1706),
• Key and message are always protected, which is why a multi-photon source can be used to counteract loss of photons in transmission without exposing security to number-photon splitting attacks (Huttner et al. 1995; Brassard et al. 2000), since the novel depends heavily on the permanent distribution of photons, and
• Its use is ideal in command, control, communications, and computers (C4); Intelligence, Surveillance and Reconnaissance (ISR); and Network Operations Center (NOC) systems.

In an optical implementation of the QKSC protocol, if the entire infrastructure was successfully intervened by an eavesdropper, there are would still be the protection via a dynamic key as the last line of defense. In fact, as each message usually occupies several characters or samples, and with each character or sample the keys change, then, during a message the key will change as many times as characters or samples the message has. This causes that any eavesdropper does not have the necessary room nor the time to break a message, in fact, not even a single character or sample. He cannot even perform an easy and efficient off-line intervention, in batch or quasi-batch modalities, such as statistical analysis, pattern recognition, or some disambiguation procedure.

Therefore, QKSC protocol will be protected even from future attacks by quantum computers with very similar criteria to post-quantum cryptography (Chen 2016; Crockett et al. 2019; Wang et al. 2018; Yoneyama 2019). Finally, given that eventually only the first key should be distributed by any of the methods described in Sect. 3, and the rest are generated automatically, and independently, although in a synchronized way both on Alice’s (sender) and Bob’s (receiver) side, we can say that the dynamic key system of the QKSC protocol resembles a virtual procedure of key redistribution.

If QKSC were used without a key but at a single-photon level, and an eavesdropper present on the channel executed a number-photon splitting attack, Bob could detect the alteration in the transmission and notify Alice to stop all transmission. In this way, the integrity of the message would be preserved, but the transmission between allies would be interrupted. On the other hand, if a multi-photon source is used, the detection of the eavesdropper action by Bob would be compromised. This is the reason for the inclusion of a dynamic key, which would preserve the integrity of the message so that the transmission would never be interrupted even if the presence of an eavesdropper on the channel had been confirmed.

The QKSC + NDKS combination generates a key for each portion of the message to be encrypted with a length equal to the key. The encoding of the message is carried out through an XOR operation between each key and the portion of the message to be encrypted. The NDKS technique is extremely sensitive to any change in the parameters \( \{\lambda, x_0\} \), so a small variation in any decimal of them (no matter how small) generates large changes in the generated keys, and therefore in the encoding resulting from the same portion of the message.

Finally, QKSC is the first protocol of Quantum Cryptography with a complete secure information transmission scheme using a dynamic key with a clear projection on the quantum Internet (Caleffi et al. 2020, 2018; Chandra et al. 2012; Cacciapuoti et al. 2020a, 2020b;
Caleffi and Cacciapuoti 2020; Cuomo et al. 2020; Ferrari et al. 2021; Chakraborty et al. 1907; Wehner et al. 2018; Dür et al. 2017; Kimble 2008; Gyongyosi and Imre 2020, 1905a, 1905b).

5.2 Future works

They basically consist of the optical implementation of the QKSC protocol both in the case of lines of optical fibers, as well as in configurations such as those in Fig. 29b.

Acknowledgements M. Mastriani thanks to the staff of Knight Foundation School of Computing and Information Sciences of Florida International University for all their help and support.

Funding This research received no external funding.

Data availability The experimental data that support the findings of this study are available in ResearchGate with the identifier https://doi.org/10.13140/RG.2.2.17197.72165.

Declarations

Competing interests Author declare he has no competing interests.

References

ASCII code, (2020) https://www.ascii-codes.com/cp852.html (last accessed 30 September 2020).
Algorithmic Assertions (2020) https://algassert.com/quirk (last accessed 07 September 2020).
Amazon Braket, (2020) https://aws.amazon.com/braket/ (last accessed 14 September 2020).
Audretsch, J.: Entangled systems: new directions in quantum physics. Wiley-VCH Verlag GmbH & Co., Weinheim, Germany (2007)
Bennett, W., Serletis, A., Serletis, D. Nonlinear and Complex Dynamics in Economics. Macro-Economic Dynamics, vol. 19(8), pp. 1749–1779. Cambridge University Press, Cambridge, (2015).
Bennett, C.H., et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen Channels. Phys. Rev. Lett. 70, 1895 (1993)
Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179. New York (1984)
Boone, K., et al.: Entanglement over global distances via quantum repeaters with satellite links. Phys. Rev. A 91(5), 052325 (2015)
Brassard, G., et al.: Limitations on practical quantum cryptography. Phys. Rev. Lett. 85, 1330–1333 (2000)
Busch, P., Lahti, P., Pellonpää, J.P., Ylinen, K.: Quantum Measurement. Springer, N.Y. (2016)
Cacciapuoti, A.S., Caleffi, M., van Meter, R., Hanzo, L.: When entanglement meets classical communications: quantum teleportation for the quantum internet. IEEE Trans. Commun. 68(6), 3808–3833 (2020b)
Cacciapuoti, A.S., Caleffi, M., Tafuri, F., Cataliotti, F.S., Gherardini, S., Bianchi, G.: The quantum internet: networking challenges in distributed quantum computing. IEEE Netw 34(1), 137–143 (2020a)
Caleffi, M., Cacciapuoti, A.S.: Quantum switch for the quantum internet: noiseless communications through noisy channels. IEEE J. Sel. Areas Commun. 38(3), 575–588 (2020)
Caleffi, M., Cacciapuoti, A.S., Bianchi, G.: Quantum internet: from communication to distributed computing. In: NANOCOM’18: Proceedings of the 5th ACM International Conference on Nanoscale Communication and Computation, Sept. 5–7, Reykjavik, Iceland, pp. 1–4. https://doi.org/10.1145/3233188.3233224 (2018)
Caleffi, M., Chandra, D., Cuomo, D., Hassanpour, S., Cacciapuoti, A.: The rise of the quantum internet. Computer 53(06), 67–72 (2020)
Cao, Z.-W., et al.: Quantum secure direct communication based on quantum dense coding using a class of W-states. J. Optoelectron. Laser 23(6), 1152–1158 (2012)
Cao, Y., et al.: Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Opt. Express 25(22), 26453–26467 (2017)
Cariolaro, G.: Quantum Communications. Springer International Publishing, N.Y. (2015)
Carpenter, J., et al.: Mode multiplexed single-photon and classical channels in a few-mode fiber. OSA Opt.
Express 21(23), 28794 (2013)
Chakraborty, K., Rozpedeky, F., Dahlberg, A., Wehner, S.: Distributed routing in a quantum internet, arXiv
preprint arXiv:1907.11630 (2019).
Chandra, D., Cacciapuoti, S.A., Caleffi, M., Hanzo, L.: noiseless direct quantum communica-tions in the
face of noisy entanglement, arXiv preprint arXiv:2012.11982 (2020).
Chen, L., et al.: Report on Post-Quantum Cryptography. NISTIR 8105, https://doi.org/10.6028/NIST.IR.
8105. (2016)
Chen, S.S., et al.: Three-step three-party quantum secure direct communication. Sci. China Phys. Mech.
Astron. 61, 090312 (2018)
Crockett, E., Paquin, C., Stebila, D.: Prototyping post-quantum and hybrid key exchange and authenticaiton
in TLS and SSH, IACR Cryptology ePrint Archive: Report 2019/858 (2019).
Cuomo, D., Caleffi, M., Cacciapuoti, A.S.: Towards a distributed quantum computing ecosystem. IET
Quantum Commun. 1(1), 3–8 (2020)
Del Santo, F., Dakic, B.: Two-way communication with a single quantum particle, arXiv preprint arXiv:
1706.08144v3 (2018)
Deng, F.G., Long, G.L.: Secure direct communication with a quantum onetime pad. Phys. Rev. A 69,
052319 (2004)
de Riedmatten, H., et al.: Long-distance entanglement swapping from photons separated sources. Phys.
Rev. A 71, 050302 (2005)
Dieks, D.: Communication by EPR devices. Phys. Lett. A 92(6), 271–272 (1982)
Dür, W., Lamprecht, R., Heusler, S.: Towards a quantum internet. Eur. J. Phys. 38, 043001 (2017)
D-Wave, https://www.dwavesys.com/ (last accessed 14 September 2020).
Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67(6), 661–663 (1991)
Elsayed, T.A.: Deterministic secure quantum communication with and without entanglement, arXiv preprint
arXiv:1904.05881 (2019).
Elshaari, A.W., et al.: On-chip single photon filtering and multiplexing in hybrid quantum photonic circuits.
Nat. Commun. 8, 379 (2017)
Faruque, S.: Pulse Code Modulation (PCM). In: Radio Frequency Source Coding Made Easy. SpringerBriefs
in Electrical and Computer Engineering. pp 65–90. Springer, Cham (2015).
Ferrari, D., Cacciapuoti, A.S., Amoretti, M., Caleffi, M.: Compiler design for distributed quantum comput-
ing. IEEE Trans. Quantum Eng. 2, 4100720 (2021). https://doi.org/10.1109/TQE.2021.3053921
Furusawa, A., van Loock, P.: Quantum Teleportation and Entanglement: A Hybrid Approach to Optical
Quantum Information Processing. Wyley-VCH, Weinheim, Germany (2011)
Gao, Z., Li, T., Li, Z.: Deterministic measurement-device-independent quantum secret sharing. Sci. China
Phys. Mech. Astron. 63, 120311 (2020)
Gyongyosi, L., Imre, S.: Entanglement access control for the quantum internet, arXiv preprint arXiv:1905.
00256 (2019)
Gyongyosi, L., Imre, S. Opportunistic entanglement distribution for the quantum internet, arXiv preprint
arXiv:1905b.00258 (2019)
Gyongyosi, L., Imre, S.: Entanglement accessibility measures for the quantum internet. Quantum Inf. Proc.
19, 115 (2020)
Hasegawa, Y., et al.: Experimental time-reversed adaptive Bell measurement towards all-photonic quantum
repeaters. Nat. Commun. 10, 378 (2019)
Horodecki R, et al.: Quantum entanglement. arXiv preprint arXiv:quant-ph/0702225 (2007).
Hu, J.-Y., et al.: Experimental quantum secure direct communication with single photons. Light Sci. Appl.
5, e16144 (2016)
Huttner, B., et al.: Quantum cryptography with coherent states. Phys. Rev. A 51, 1863–1869 (1995)
IBM Q Experience (2020) https://quantum-computing.ibm.com/ (last accessed 14 September 2020).
Jaeger, G.: Entanglement, Information, and the Interpretation of Quantum Mechanics. The Frontiers Collection.
Springer-Verlag, Berlin, Germany (2009)
Jennewein, T., et al.: Experimental nonlocality proof of quantum teleportation and entanglement swapping.
Phys. Rev. Lett. 88, 017903 (2001)
Jin, R.-B., et al.: Highly efficient entanglement swapping and teleportation at telecom wavelength. Sci. Rep.
5, 9333 (2015)
Kak, S.: A Three-Stage Quantum Cryptography Protocol, arXiv preprint arXiv:0503027 (2005)
Kaye, P., Laflamme, R., Mosca, M.: An Introduction to Quantum Computing. Oxford University Press,
Oxford (2004)
Kimble, H.J.: The quantum internet. Nature 453, 1023–1030 (2008)
Kish, S.P., et al.: Quantum Engineering. Design and analysis of random multiple access quantum key distribution. Quantum Eng. e50 (2020).

Korotkov, A.: Quantum error correction (QEC) (2017) https://intra.ece.ucr.edu/~Korotkov/courses/EE214-QC/QC-7-error-correction.pdf

Python Language (2022) https://www.python.org/ (accessed on 5 March 2022).

Lenzini, F., et al.: Active demultiplexing of single photons from a solid-state source. Laser Photonics Rev. 11, 1600297 (2017)

Li, J., et al.: Quantum secure direct communication based on dense coding and detecting eavesdropping with four-particle genuine entangled state. Entropy 17, 6743–6752 (2015)

Li, Y-H., et al.: All-optical quantum signal demultiplexer. arXiv:quant-ph/1803.00206 (2018).

Li, J.-P.: Multiphoton graph states from a solid-state single-photon source. ACS Photonics 7, 1603–1610 (2020)

Li, T., Long, G.-L.: Quantum secure direct communication based on one-photon Bell-state measurement. New. J. Phys. 22, 063017 (2020)

Li, Z., Zhang, R., Yin, X., et al.: Experimental quantum repeater without quantum memory. Nat. Photonics 13, 644–648 (2019)

Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key distribution scheme. Phys. Rev. A 65, 032302 (2002)

Massa, F., et al.: Experimental two-way communication with one photon, arXiv preprint arXiv:1802.05102 (2019)

Mastriani, M.: Non-distributable key sharing for improving the security in IoT networks, arXiv preprint arXiv:2205.02779 (2022).

Mastriani, M., Iyengar, S.S.: Satellite quantum repeaters for a quantum Internet. Quantum Eng. QUE255 (2020). https://doi.org/10.1002/que2.55

Mastriani, M., Iyengar, S.S., Latesh Kumar, K.J.: Bidirectional teleportation for underwater quantum communications. Quantum Inf. Process. 20, 22 (2021). https://doi.org/10.1007/s11128-020-02970-51

Meyer-Scott, E., Silberhorn, C., Migdall, A.: Single-photon sources: approaching the ideal through multiplexing. Rev. Sci. Instrum. 91, 041101 (2020)

Munro, W.J., Azuma, K., Tamaki, K., Nemoto, K.: Inside quantum repeaters. IEEE J. Sel. Top. Quantum Electron. 21, 6400813 (2015)

Nguyen, D.M., Kim, S.: A novel quantum no-key protocol for many bits transfer with error correction codes advances in science. Technol. Eng. Syst. J. 5(2), 781–785 (2020)

Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2004)

NIST: Quantum Computing and Communication (CreateSpace Independent Publishing Platform, Scotts Valley 2014).

NSA: Quantum key distribution (QKD) and quantum cryptography QC (2022) Available online: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (accessed on 5 March 2022).

Ola, M., et al.: Quantum secure direct communication using entanglement and super dense coding. In: ECRYPT 2009-International Conference on Security and Cryptography, pp.175–181 (2009)

Pan, J.-W., et al.: Experimental entanglement swapping: entangling photons that never interacted. Phys. Rev. Lett. 80, 3891–3894 (1998)

Pan, D., et al.: Experimental free-space quantum secure direct communication and its security analysis. Photonics Res. 8, 1522 (2020b)

Pan, D., Li, K., Ruan, D., Ng, S.X., Hanzo, L.: Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs. IEEE Access 8, 121146 (2020a)

Pastawski, F.: Quantum memory: design and applications, Ph.D. thesis, Munich University (2012) https://d-nb.info/1025224361/34

Qaisar, S. et al.: Practical deterministic secure quantum communication in a lossy channel, Prog. Theor. Exp. Phys. 041A01 (2017).

Qi, R., et al.: Implementation and security analysis of practical quantum secure direct communication. Light Sci. Appl. 8, 22 (2019)

QuRep, (2020) http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/component/content/article/75-distillation/ (last accessed 29 September 2020).

Razavi, M., Piani, M., Lutkenhaus, N.: Quantum repeaters with imperfect memories: cost and scalability, arXiv preprint arXiv:0810.5334 (2009)

Rigetti (2020) https://www.rigetti.com/ (last accessed 14 September 2020).
Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21(2), 120–126 (1978)

Ruihong, Q., Ying, M.: Research progress of quantum repeaters. In: IOP Journal of Physics: Conference Series, vol. 1237, p. 052032 (2019)

Sangouard, N., et al.: Quantum repeaters based on atomic ensembles and linear optics. Rev. Mod. Phys. 83, 33–80 (2011)

Schlosshauer, M.: Decoherence, the measurement problem, and interpretations of quantum mechanics. Rev. Mod. Phys. 76(4), 1267–1305 (2005)

Schmid, C., et al.: Quantum teleportation and entanglement swapping with linear optics logic gates. New J. Phys. 11, 033008 (2009)

School of Computing and Information Sciences (2020) https://www.cis.fiu.edu/ (last accessed 07 September 2020).

Stolze, J., Suter, D.: Quantum Computing: A Short Course from Theory to Experiment. Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim, Germany (2007)

Tsujimoto, Y., et al.: High-fidelity entanglement swapping and generation of three-qubit GHZ state using asynchronous telecom photon pair sources. Sci. Rep. 8, 1446 (2018)

Wang, H.F., et al.: Quantum secure direct communication by using a GHZ state. J. Korean Phys. Soc. 49(2), 459–463 (2006)

Wang, W. et al.: XMSS and Embedded Systems XMSS Hardware Accelerators for RISC-V (2018) https://eprint.iacr.org/2018/1225.pdf

Wang, C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. Opt. Commun. 253, 15–20 (2005)

Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: a vision for the road ahead. Science 362, eaam9288 (2018)

Wei, H., et al.: Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B 21(10), 100308 (2012)

Wen, K., Long, G.L.: One-party Quantum error correcting codes for unbalanced errors: principles and application to quantum dense coding and quantum secure direct communications. arXiv:quant-ph/0609207v2 (2007).

Xie, X.C.: Quantum secure direct communication with an untrusted Charlie using imperfect measurement devices. Sci. China Phys. Mech. Astron. 63, 230361 (2020)

Xiu, X.-M., et al.: Quantum secure direct communication with four-particle genuine entangled state and dense coding. Commun. Theor. Phys. 52(1), 60–62 (2009)

Yan, L., et al.: Quantum secure direct communication protocol with mutual authentication based on single photons and bell states. Computers, Materials & Continua 63(3), 1297–1307 (2020)

Yoneyama, K. Post-Quantum Variants of ISO/IEC Standards: Compact Chosen Ciphertext Secure Key Encapsulation Mechanism from Isogenies (2019) https://eprint.iacr.org/2019/1036.pdf

Yu, X.-T., Zhang, Z.-C., Xu, J.: Distributed wireless quantum communication networks with partially entangled pairs. Chin. Phys. B 23(1), 010303 (2014)

Zhang, Y., Ni, Q.: Design and analysis of random multiple access quantum key distribution. Quantum Eng. 2, e31 (2020)

Zhou, L., Sheng, Y.B., Long, G.L.: Device-independent quantum secure direct communication against collective attacks. Sci. Bull. 65(1), 12–20 (2020)

Zou, Z.R., et al.: Measurement-device-independent quantum secure direct communication. Sci. China Phys. Mech. Astron. 63(3), 230362 (2020a)

Zou, X.F., Qiu, D.W.: Three-step semi-quantum secure direct communication protocol. Sci. China Phys. Mech. Astron. 57(9), 1696–1702 (2014)

Zou, Z.K., Zhou, L., Zhong, W., Sheng, Y.B.: Measurement-device–independent quantum secure communication of multiple degrees of freedom of a single photon. EPL 131, 40005 (2020b)

Żukowski, M., et al.: Event-ready-detectors bell experiment via entanglement swapping. Phys. Rev. Lett. 71, 4287–4290 (1993)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.