Received: 23 December 2020 | Revised: 29 March 2021 | Accepted: 6 April 2021

DOI: 10.1049/qtc2.12009

IET Quantum Communication

The Institution of Engineering and Technology WILEY

CASE STUDY

Advances in quantum secure direct communication

Piotr Zawadzki

Department of Telecommunications and Teleinformatics, Silesian University of Technology, Gliwice, Poland

Correspondence

Piotr Zawadzki, Department of Telecommunications and Teleinformatics, Silesian University of Technology, Gliwice, Poland.
Email: Piotr.Zawadzki@polsl.pl

Abstract

The practical implementation of quantum secure direct communication (QSDC) will undoubtedly be a milestone in the development of quantum cryptography. Research is in its final phase and focuses on developing secure protocols that consider realistic constraints and are feasible within the current state of technology. Three well-known protocols ae compared, Ping-Pong, Two-Step and Deng-Long, in the context of the level of security offered and the challenges related to their implementation. This work explains how the evolution of QSDC protocols from a purely quantum formulation to hybrid classical-quantum solutions based on the Wyner wiretap channel model can solve most problems encountered. The work aims to inform scientists in other fields of quantum information processing about the latest advances in QSDC. The attached appendix introduces basic concepts for readers unfamiliar with this research area.

1 | INTRODUCTION

The purpose of information protection is the unique assignment of confidentiality and authenticity attributes. These attributes can be verified by the recipient. They adequately imply that the wrong entities have not obtained access to the message and that it comes from the appropriate source. Three basic paradigms of confidentiality provision have been identified: (1) symmetric algorithms using shared keys [1], (2) asymmetric algorithms using public key–private key pairs [2] and (3) errors (noise) accompanying information transmission [3]. The first two paradigms have been developed intensively since they were proposed. Results of these studies are described in a synthetic form in many textbooks on classical cryptography [4, 5]. The third paradigm is the foundation of modern quantum cryptography.

The idea of information processing based on the laws of quantum mechanics is not as new as it may seem. Back in the 1970s, Steven Wiesner, a Columbia University student, proposed a quantum cryptocurrency system and a method for encoding information in non-orthogonal quantum states. Unfortunately, the manuscript describing the properties of the system was rejected by many journals and was published later in 1983 [6], after Benioff's [7] and Feynman's [8] papers, which called for the construction of quantum computers. At that time, quantum cryptography was considered an interesting niche of research but with no serious impact on the existing communication infrastructure. The real impetus to research in this field was given a decade later by Shor's paper [9]. It demonstrated that asymmetric algorithms (the foundation of Internet security) can be efficiently broken using a hypothetical quantum computer and thus undermined a security paradigm based on computational complexity. Since then, we have observed increasing interest in research in new cryptographic primitives that exploit the quantum properties of matter to protect against that new threat.

Quantum cryptography is a well-developed branch of cryptography, that provides primitives whose security is based on the laws of physics. It offers a few primitives that provide quantum-assisted confidentiality of transmitted information. They can be categorized according to the mechanism of confidentiality provision and the method of cryptographic key handling. (1) Quantum key distribution (QKD) protocols do not ensure confidentiality [10, 11] as a standalone tool. They deliver private and random key material to both peers of the link that can be subsequently used for classical encryption. However, unconditional security is attainable only when QKD is used jointly with a classical one-time pad (OTP) cipher. QKD protocols are inherently non-deterministic because both parties contribute to the randomization of the key and neither can predict the key resulting from the protocol execution. (2) Functional characteristics of the deterministic QKD (DQKD) protocols [12, 13] are similar. However, this time, the cryptographic key is selected by one of the parties and delivered to the other in deterministically. The privacy of the delivery process is guaranteed by the properties of the quantum communication process. It may be imperfect, because the parties can always refer to the process of privacy amplification for its improvement at the cost of reducing the key length. The resulting key, as in QKD, can be used to parameterize the operation of classical cryptographic algorithms. The unconditional confidentiality is achieved only when OTP is used as a cipher and the parties use a key suitable for that task. (3) Deterministic quantum secure communication (DQSC) protocols [14, 15] may provide confidentiality without referring to classical encryption. The information sender creates a random classical cryptographic key and uses it to encode sensitive information into quantum states that are sent to the recipient. Then, parties verify whether the eavesdropper is on the line using local operations and classical communication. The key that permits decoding of the sensitive message is delivered in an open classical channel when no eavesdropping is detected. (4) Quantum secure direct communication (QSDC) protocols [16] go one step further and eliminate the need for the cryptographic key. The privacy and determinism of communication are ensured by the quantum nature of information carriers. Unlike the DQKD, perfect privacy of communication is ensured in QSDC. From the user's perspective, the sensitive message just enters a QSDC-protected private channel and confidentially travels to the recipient. No key agreement or reference to external ciphers is required. All 'magic' of information protection is handled by the protocol. Moreover, the provided security is independent of the eavesdropper's resources because it is founded on the laws of physics ([17], p. 58). The unconditionally secure QSDC is a stronger cryptographic primitive than all forms of QKD because it can be used to deliver both random keys and sensitive deterministic messages securely.

This review focuses on quantum information processing techniques used in QSDC protocols. Its purpose is not to illustrate the current state of knowledge, but the main ideas behind QSDC and their evolution over time; therefore, the provided bibliography should by no means be considered complete. Some results are referenced in the summary.

In QSDC protocols, unlike classical cryptography, the principle of information protection is founded only on the laws of physics, and the encryption process per se does not occur. Furthermore, the transfer of sensitive information is limited to a quantum channel and classical messages, if any, that carry on control data only. QSDC protocols exploit the following non-classical properties of quantum objects: (1) the inability to copy unknown quantum states (no-cloning theorem) [18, 19], (2) the imperfect distinguishability of non-orthogonal quantum states [20], and (3) the inability to determine the state of the entangled system when only its part is accessible for measurement [21]. These concepts may be used alone or in combination in different configurations to ensure security of a communication process. Many QSDC protocols have been proposed in the 20-year history of research. We will further focus on the properties of the three protocols: Ping-Pong (PP) [13], which, as we will see later, cannot be considered a full-blown QSDC solution; and two QSDC protocols, namely, Two-Step (TS) [22] and DL (after the names of its inventors, Deng Fu-Guo and Long Gui Lu, also referred to as Quantum OTP) [23]. The PP engine was chosen because it well illustrates the challenges and pitfalls in designing QSDC communication. Although it was initially developed as a QSDC primitive [24], it is often used to construct DQKD protocols [25, 26]. Selection of the remaining two is motivated by the following reasons: (1) theprotection of information is founded on different techniques, (2) the way these techniques are used is representative of other approaches, (3) they have been thoroughly studied because they have been functioning in the scientific literature for many years and (4) they still evolve in the process of adjusting to existing technical capabilities [26–34]. QSDC protocols use an authenticated classical channel in the process of eavesdropper detection. It is therefore clear that they must operate in combination with other protocols, perhaps quantum, which provide thus authentication of control data.

No unconditionally secure QSDC and QKD protocols that could be implemented in practice have been developed so far. Shortcomings of available techniques for processing quantum objects are the main obstacle to achieving this goal. The lack of reliable and long-term quantum memory is particularly challenging. Two general approaches to solve the problem have been adopted. In the first, unconditionally secure protocols are modelled. Then, it is verified to what degree adjustment of the model to existing technical capabilities affects the security of the protocol. In the second approach, the capabilities of communicating parties are limited to feasible operations already at the design stage, and the security is maximized within that framework. Both of these trends, combined with the constant development of technology, will probably lead to the construction of unconditionally secure and feasible QSDC protocols [33, 34].

This article is organized as follows. The next section introduces typical QSDC protocols and compares their security profiles in the perfect setting. Then, the idealized model is critically discussed and the impact of previously disregarded errors and losses on the provided security is highlighted. This is followed by Section 3, which discusses how to obtain secure protocols in an imperfect quantum channel setting. The final conclusions are contained in Section 4. The main text is supplemented by additional material that explains the applied notation and introduces useful information for readers who are not familiar with the specifics of quantum operations on qubits.

2 | QUANTUM SECURE DIRECT COMMUNICATION IN PERFECT CHANNELS

The following description uses standard personification rules for parties involved in implementing the cryptographic protocol: Alice is the sender of the information, Bob acts as the recipient, and Eve is an attacker who attempts to access sensitive information in an unauthorized manner. Alice and Bob use classical and quantum communication channels. The quantum channel is: (a) open: Eve has unrestricted access to it; (b) ideal: any transmission errors or loss results only from Eve's hostile activities. The classical channel is authenticated; therefore, Eve can see the control messages but she cannot modify their content.

2.1 | Protocol PP

The PP protocol was proposed by Boström et al. in 2002 [13]. It employs the sequential processing of quantum states.

PP.1: Distribution of information carriers.

(a) *Bob: Preparation of entangled state*. Bob produces an Einstein-Podolsky-Rosen (EPR) pair of the form $|\beta_{00} = \frac{1}{\sqrt{2}}(|0_\mathrm{A}\rangle|0_\mathrm{B}\rangle + |1_\mathrm{A}\rangle|1_\mathrm{B}\rangle)$. He keeps qubit B for himself and sends qubit A to Alice.
(b) Alice randomly decides whether to verify the authenticity of the received qubit (point PP.1c) or to encode the message (point PP.2).
(c) *Alice: Test measurement*. Alice measures the observable $[Z]$ on the received qubit in randomly selected cycles of protocol. The measurement results in the collapse of the EPR pair. The system state after measurement depends on the received outcome.

outcome	+1	−1
Observable		
$[Z]$	$|0_\mathrm{A}\rangle|0_\mathrm{B}\rangle$	$|1_\mathrm{A}\rangle|1_\mathrm{B}\rangle$

Alice asks Bob to measure the same observable on his qubit.

(d) *Bob: Verification of entanglement*. Bob also measures $[Z]$ on his qubit. He should receive the same outcome as Alice. This is a direct consequence of the collapse induced by her measurement. Then, Bob sends the resulting value back to Alice.
(e) *Alice: Check for the correlation*. Alice compares results of her measurements with Bob's outcomes. The lack of expected correlation is a sign of Eve's interference in the entanglement distribution process. Upon such an event, Alice terminates the protocol. Otherwise, she returns back to point PP.1a.

PP.2: Transmission of sensitive information.

(a) *Alice: Information coding*. Alice encodes one classical bit $m \in \{0, 1\}$ of the message by doing nothing or by applying the gate $[Z]$ to her qubit of the EPR pair, respectively. This operation effectively changes the state $|\psi_\mathrm{AB}\rangle$ of the system shared by Alice and Bob:

$$|\psi_\mathrm{AB}\rangle(m) = [Z]_\mathrm{A}^m|\beta_{00}\rangle = |\beta_{m0}\rangle \tag{1}$$

where $|\beta_{mn}\rangle = 2^{-1/2}\left(|0_\mathrm{A}\rangle|n_\mathrm{B}\rangle + (-1)^m|0_\mathrm{A}\rangle|\bar{n}_\mathrm{B}\rangle\right)$ and bar over n denotes the negation of the classical bit.

(b) *Bob: sensitive information decoding*. Bob is able to decode the information by discriminating the $|\beta_{00}\rangle$ and $|\beta_{10}\rangle$ states.

2.2 | Protocol TS

Protocol TS was proposed by Deng et al. in 2003 [22]. It differs from the PP protocol in two aspects: (1) parties encode information in a computational and dual base, and (2) qubits are processed in blocks. Its operation can be summarized as follows:

TS.1: Distribution of information carriers.

(a) *Alice: Preparation of entangled states*. Alice prepares a sequence of EPR pairs $S = \{|\beta_{00}\rangle\}_{k=1}^N$ from which she extracts two qubit sequences, S_A and S_B, composed of A and B qubits of the pairs, respectively. She stores the S_A sequence in quantum memory and sends sequence S_B to Bob.
(b) *Bob: Test measurement*. Bob stores the received sequence in quantum memory. He measures observables randomly selected from set $\{[Z], [X]\}$ on some randomly selected subset of sequence S_B. The possible measurement outcomes and postmeasurement states are summarized next.

Result	+1	−1
Observable		
$[Z]$	$|0_\mathrm{A}\rangle|0_\mathrm{B}\rangle$	$|1_\mathrm{A}\rangle|1_\mathrm{B}\rangle$
$[X]$	$|+_\mathrm{A}\rangle|+_\mathrm{B}\rangle$	$|-_\mathrm{A}\rangle|-_\mathrm{B}\rangle$

Bob informs Alice about the positions of the measured qubits, selected observables, and received outcomes.

(c) *Alice: Entanglement verification*. Alice measures observables specified by Bob on corresponding positions of the possessed S_A sequence. Her outcomes should be in perfect correlation with the outcomes reported by Bob. Any deviation from the predictions in step TS.1b is a sign of a mounted attack. Alice informs Bob about a positive verification or interrupts the protocol.

(d) *Alice and Bob: Shortening of the sequence.* Alice and Bob remove the used qubits from sequences S_A and S_B, respectively.

TS.2: Transmission of sensitive information.

(a) *Alice: Information coding.* Alice encodes a pair of classical bits $p = (b_0, b_1)$ on each EPR pair using the transformation

$$|\psi_{AB}\rangle(p) = [Z]_A^{b_0}[X]_A^{b_1}|\beta_{00}\rangle = |\beta_{b_0,b_1}\rangle \tag{2}$$

applied to elements of sequence S_A. She encodes random bits on some pairs and message bits on the remaining ones. Alice then sends the qubits of the S_A sequence to Bob.

(b) *Bob: Storage.* Bob stores received qubits in quantum memory.
(c) *Alice: Publication of test data.* Alice publishes positions of pairs that carried random information and the values of encoded random bits.
(d) *Bob: Test measurement.* Bob makes Bell's measurement on positions of S published by Alice. The resulting outcomes allow him to check for errors in the transmission of sensitive information. Their presence is a sign of Eve's interference, so the remaining sensitive information cannot be trusted.
(e) *Bob: Decoding sensitive information.* Bob makes Bell's measurement on the remaining pairs. The outcomes are translated into classical bits (b_0, b_1) according to rule (2) described in TS.2a.

2.3 | Protocol DL

Protocol DL was proposed by Deng et al. in 2004 [23]. It uses non-orthogonal quantum states to ensure the confidentiality of the transmission and employs processing qubits in blocks. It can be summarized in the following points:

DL.1: Distribution of information carriers.

(a) *Bob. Preparation of information carriers.* Bob prepares and stores two random sequences of classical bits, $\{b_l\}_{l=1}^{N}$ and $\{v_l\}_{l=1}^{N}$. They are used to form sequence S of qubits $|\phi_l\rangle = [H]^{b_l}|v_l\rangle$, where $[H]$ denotes a Hadamard gate. In other words, Bob prepares sequence S composed of qubits $|\phi_l\rangle$ in states randomly selected from the set $\{\ |0\rangle, |1\rangle, |+\rangle, |-\rangle\ \}$. He sends this sequence to Alice.
(b) *Alice: Test measurement.* Alice stores the received qubits in quantum memory. She measures an observable randomly selected from set $\{[Z], [X]\}$ on a randomly selected subset of qubits. Then, she sends to Bob the positions in sequence selected for testing, the type of measured observables and the obtained outcomes.
(c) *Bob: Test measurements.* Roughly half of Alice's choices are consistent with Bob's preparation base. On these positions, Alice's outcomes v_l' should be deterministic and consistent with value v_l used by Bob at the preparation step. Deviation from this rule is a sign of Eve's interference and forces interruption of the protocol. Bob informs Alice that there are no errors. Otherwise, the protocol is interrupted.
(d) *Alice and Bob: Shortening of the sequence.* The parties remove test entries from the stored sequences: Alice's is quantum and Bob's is classical.

DL.2: Transmission of sensitive information.

(a) *Alice: Information encoding.* Alice encodes one bit c_l of classical information on each stored qubit by applying ('1') or not ('0') transformation $j[Y] = [Z][X] = |0\rangle\langle 1| - |1\rangle\langle 0|$ to the remaining qubits of sequence S:

$$|\psi_l\rangle = (j[Y])^{c_l}|\phi_l\rangle \tag{3}$$

This operation effectively flips the qubit independent of the preparation base.

$$j[Y]|0\rangle = |1\rangle \qquad j[Y]|1\rangle = |0\rangle \tag{4a}$$

$$j[Y]|+\rangle = |-\rangle \qquad j[Y]|-\rangle = |+\rangle \tag{4b}$$

where global phase has been skipped. The resulting sequence can be expressed as:

$$|\psi_l\rangle = [H]^{b_l}|v_l \oplus c_l\rangle \tag{5}$$

Alice encodes random bits on the selected positions. The rest of the sequence carries sensitive information. The modified sequence is sent back to Bob.

(b) *Bob: Information decoding.* Upon received qubits $|\psi_l\rangle$, Bob measures observable compatible with the preparation base: $[Z]$ for $b_l = 0$ and $[X]$ for $b_l = 1$. That way, he receives a sequence $\{v_l''\}$ of classical bits. The bits encoded by Alice are retrieved with xor operation $c_l' = v_l \oplus v_l''$, where $\{v_l\}$ is the sequence used at preparation stage DL.1a.
(c) *Alice: Publication of test data.* Alice publishes the positions and value of random bits.
(d) *Bob: Received data validation.* Bob compares the results of his measurements with the values received from Alice. That way, Bob can assess whether Eve modified the states of qubits carrying sensitive information.

2.4 | Analysis

Eve's goal is to access confidential information sent in an open quantum channel. The lack of cryptographic keys allows Eve to cut through a quantum channel, set up a man-in-the-middle) attack (also referred to as intercept-resend in quantum cryptography) and consequently impersonate legitimate parties. That is why, to verify the reliability of the quantum media, Alice and Bob perform a series of probabilistic tests that employ local measurements and classical communication. The authenticity of control messages is a necessary condition for ensuring the security of QSDC communication. It is assumed *a priori* because the methods of its provision are not within the scope of QSDC.

There are two stages of communication in the QSDC protocol: (1) the distribution of quantum carriers; and (2) the encoding, transmission, and decoding of classical information. Attacks that target only the second stage of the well-designed protocol have no chance of success; for each protocol under consideration, measurements of carriers lead to a set of equally likely results. The only form of Eve's interference at this stage may be the replacement of qubits in the quantum channel, which will result in decoding of the random message. PP does not include protection against this type of Eve's activity; it is assumed that errors will be detected at the link layer. TS and DL, on the other hand, have built-in denial of service tests already in the physical layer.

Eve may also try to access information encoded in quantum states by entangling a system that she controls with information carriers at the distribution stage. Introduced entanglement causes that Alice's and/or Bob's local operations to affect the state of the Eve's system. Attacks of this type that span multiple protocol cycles are called coherent. The attack is called individual or incoherent when coupling is applied to every signal particle independently. As a rule, Eve is subject to restrictions imposed only by the laws of quantum mechanics, and she is allowed to use any quantum operation. In the context of security analysis, the Stinespring's dilation theorem [35] is of prime importance. It states that any quantum operation in system A can be thought as composed of the following operations: (1) tensoring with a second system B twice the size of the system A, and (2) a unitary transformation defined on a composite system. Thus, any quantum operation can be thought of as a narrowing of unitary evolution on a larger (dilated) system. System B to which system A is coupled is usually called the ancilla of A. For the protocols under consideration, any individual attack can therefore be modelled as a unitary operation in a space of three qubits: one signal qubit and two additional ones that are controlled by Eve.

Of course, the introduction of entanglement inevitably modifies the system used to transmit confidential information. Such actions will manifest themselves as transmission errors or losses. Therefore, the protocol design should include tests that detect changes in the communication system leading to potential information leakage. In turn, the attackers aim to access protected information in a way that is undetectable by these tests.

Ensuring the proper design of the distribution stage is crucial for the security of QSDC protocols. Alice and Bob make local measurements of distributed qubits and use an authenticated classical communication channel to verify the expected correlation of their states. These measurements, according to the laws of quantum mechanics, are destructive and probabilistic; a single test detects Eve's interference with a certain probability. Therefore, only a series of tests on a sufficiently large sample of states can convince Alice and Bob of the authenticity of the remaining carriers.

If there an entangling operation exists that is undetectable by correlation tests while providing a nonzero information gain to Eve, the protocol is considered broken. Mathematically, this issue can be described as the selection of map $[U_{\mathrm{AE}}]$ coefficients:

$$|0_{\mathrm{A}}\rangle|\phi_{\mathrm{E}}\rangle \overset{[U_{\mathrm{AE}}]}{\to} u_{00}|0_{\mathrm{A}}\rangle|00_{\mathrm{E}}\rangle + u_{01}|1_{\mathrm{A}}\rangle|01_{\mathrm{E}}\rangle \tag{6a}$$

$$|1_{\mathrm{A}}\rangle|\phi_{\mathrm{E}}\rangle \overset{[U_{\mathrm{AE}}]}{\to} u_{10}|0_{\mathrm{A}}\rangle|10_{\mathrm{E}}\rangle + u_{11}|1_{\mathrm{A}}\rangle|11_{\mathrm{E}}\rangle \tag{6b}$$

where $|\phi_{\mathrm{E}}\rangle$ is the initial state of the ancilla, and states $|\mu\nu_{\mathrm{E}}\rangle$ are used to distinguish between coding operations performed by Alice. The coefficients $u_{\mu\nu}$ are not independent because operation $[U_{\mathrm{AE}}]$ has to be unitary. When test measurements are performed only in a computational base, as is the case in the PP protocol, the probability of Eve being detected is $e = |u_{01}|^2 = |u_{10}|^2$, and therefore its activity will remain hidden with probability $D = 1 - e = \ |u_{00}|^2 = |u_{11}|^2$. In general, the relation that describes a trade-off between Eve's risk of being detected and her gaining information depends on the protocol design. It is particularly simple (Boström and Felbinger, Equation 12) for a PP protocol:

$$I_{\mathrm{E}} = -e\log_2 e - D\log_2 D = h(e) \tag{7}$$

where $h(\cdot)$ denotes Shannon's entropy of the binary source. In other words, Eve must take the risk of being detected with probability e to gain non-zero information I_E. Protocols with this property are called robust, and all protocols under consideration belong to this class. Similar formulae can be derived for sequential versions (block length $N = 1$) of TS and DL protocols [32]:

$$I_{\mathrm{E}} = \begin{cases} 2h(e/2) & \text{TS} \\ h(e) & \text{DL} \end{cases} \tag{8}$$

under the assumption that bit-flip and phase-flip errors contribute equally to the errors observed at the carrier's distribution stage.

The seminal version of PP employs sequential processing of qubits to avoid using quantum memory. In that case, the control tests are randomly interleaved with information cycles. The chance that Eve's attack will remain undetected after N tests is D^N. The probability D^N is relatively high in the initial phase of communication when N is small. It can be said that the confidentiality of the classical bit increases with its position. Therefore, there is a chance that the initial portion of the message will leak out and yet Eve will remain undetected. In the earlier discussion, it was assumed that all qubits were attacked. However, Alice and Bob never know when Eve starts her attack, so no portion of the message is well-protected. On the other hand, Eve never knows which qubits will be used for eavesdropping tests and must risk her presence being revealed. In general, there is trade-off between Eve's information gain and the probability of her detection. Protocols with this property are called quasisecure protocols; they are unsuitable for QSDC tasks, although they may be used as DQKD [26].

Quasisecurity is usually resolved by processing qubits in blocks, as in the efficient-QSDC [16], TS and DL protocols. Alice proceeds to the information transfer stage only after she is sure that Eve is not present for a certain block of carriers. The probability that Eve remains hidden can be arbitrarily minimized by increasing length N of the processed block and the protocol can be considered unconditionally secure. Unfortunately, processing qubits in blocks requires the use of quantum memory. The time when the deployment of quantum memory will be possible is difficult to predict. It was only relatively recently that a laboratory installation of the TS protocol based on the cutting-edge implementation of quantum memory was demonstrated [33].

None of the presented approaches leads to satisfactory solutions; protocols using sequential qubit processing are at most quasisecure whereas processing qubits in blocks cannot be implemented in practice. The joint application of classical information processing in blocks with sequential qubit transmission has been proposed as a solution that combines the advantages of both approaches [29–31]. This issue is discussed next.

3 | QUANTUM SECURE DIRECT COMMUNICATION IN IMPERFECT CHANNELS

The analysis in the previous section assumed communication in a perfect quantum channel. As a result, any erroneous transmission or loss of qubits can be interpreted as a manifestation of Eve's hostile activity. However, the assumption of error-free and lossless transmission of qubits does not stand up to reality. No known methods of qubit transmission can be considered close to that model. The observed error and/or loss rates are much higher than in the classical channels. Unfortunately, errors and losses resulting from natural causes are indistinguishable from errors and losses resulting from the actions of an attacker. Eve is limited only by the laws of physics, so one should assume the pessimistic assumption that she is able to replace the quantum channel used by Alice and Bob with the better one. Security analyses that assume imperfect quantum channels should consider that all observed errors and losses are manifestations of Eve's hostile activity. However, unlike perfect conditions, the execution of the protocol cannot be interrupted after a first error. Alice and Bob simply have to accept the fact that some qubits can be attacked with impunity and tolerate the associated potential leakage of associated information. The QSDC analysis model in real-world channels thus can be summarized as:

1. Alice and Bob communicate using a perfect quantum channel.
2. Eve eavesdrops communication and her activity induces errors both in the distribution of carriers and the information transfer stage.
3. Alice and Bob tolerate invalid transmissions as long as the losses and the error rate does not exceed certain maximum thresholds, lmax and emax, respectively.
4. The carrier degradation associated with Eve's attack also reduces mutual information between Alice and Bob: that is, $I_B(e_{\max}) < I_B(0)$.

The aim of this research is to develop protocols in which the level of security offered is independent of Eve's resources, despite her uncontrolled access to some of the information sent. A similar problem occurs with QKD protocols in which at some point in the key agreement process, the parties have identical random bit sequences, some of which may be known to Eve. In QKD, privacy amplification is the solution to the problem. Alice and Bob perform a series of suitably selected operations on their bit strings and communicate classically to diminish Eve's information to zero. A side effect of this process is shortening and randomization of the shared sequence of bits. Therefore, this procedure cannot be used directly in QSDC protocols for which the deterministic nature of the communication is a fundamental requirement.

A quantum analogue of privacy amplification can be used in protocols founded on quantum entanglement. In the TS protocol, the information can leak when some elements of the S_A and S_B sequences remain entangled with ancilla. Alice and Bob can separate themselves from the system controlled by Eve using the entanglement distillation protocol [36]. As a consequence, Eve loses access to sensitive information. The entanglement distillation efficiency for the TS protocol is $(1 - 2h(e_{\max}/2))$. Unfortunately, the entanglement distillation procedure de facto requires a quantum computer, which for the time being makes it impossible to deploy.

Fortunately, classical preprocessing of sensitive information is a feasible solution to the problem. Hybrid classical and quantum information processing were proposed as early as 1983 [37], even before the appearance of the first QKD protocol [11]. However, in the context of QSDC, such an approach, based on Wyner results [3], was proposed only recently [31, 34, 38]. Wyner proved that classical redundant coding exists enabling confidential communication as long as the secrecy capacity [3, 32, 41]

$$C_S = (1 - l^{(m)}_{\max})I_B - (1 - l^{(c)}_{\max})I_E \tag{9}$$

is positive. Quantities $l^{(c)}_{\max}$ and $l^{(m)}_{\max}$ represent the loss rates for the carrier distribution and information transmission stages, respectively. The presented estimates are valid at the limit of the infinite length of the message. Therefore, further work is carried out to estimate the secrecy capability for more realistic conditions [34].

Wyner's theorem opens up a niche in research because it does not specify the form of the optimal redundant code. However, it is clear that error rates higher than a few percent prohibit confidential communication (Wu et al. [32], Figures 2 and 3). Some initial results in the quest for optimal redundant encoding are available. The sequential version of the DL protocol supplemented with redundant LDPC coding was analysed in Sun et al. [29]. In this mode of operation, the DL protocol does not require quantum memory, which distinguishes it from other alternatives. Unfortunately, the code form was not given and the secrecy ability was not estimated. A system that combines OTP encryption with LDPC encoding was also proposed [31]. The results of computer simulations indicate that this approach provides an increase in secrecy compared with simply applying redundant codes. Work was also undertaken to develop a generic QSDC security analysis framework [38].

4 | SUMMARY

Analyses using the Wyner model show that hybrid QSDC solutions combining the sequential qubit processing paradigm at the physical layer with classical redundant coding at the link layer enable confidential communication. However, Wyner's results only prove the existence of an optimal solution without providing its specific form. The development of redundant codes optimized to maximize confidentiality capacity while maintaining deployable complexity is expected in the near future. Practical implementations of these ideas have been demonstrated as proof-of-concept experiments [39, 40] or field test deployments [41]. However, the theoretical security of the communication model does not guarantee the security of practical implementation. Quantum equipment is still imperfect and susceptible to side-channel attacks (anecdotally, the first QKD installation emitted different sounds when ‘0’ or ‘1’ was sent). In fact, most attacks on quantum protocols exploit the properties of the hardware. These problems will be naturally solved when the hardware becomes more trustworthy, and at present, these loopholes can be overcome by designing relevant protocols. For example, an analysis of the experimental implementation of the DL protocol when the photon source is imperfect can be found in Pan et al. [42]. The concept of device-independent quantum protocols that remain secure even under the assumption of imperfect equipment aims to solve this problem at the system level. Niu et al. [43] and Zhou et al. [44] and references therein discuss state-of-the-art information on the device independence of QSDC protocols.

ORCID

Piotr Zawadzki https://orcid.org/0000-0002-6235-1397

REFERENCES

1. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. 28(4), 656–715 (1949)
2. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inform. Theory. 22(6), 644–654 (1976)
3. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. 54(8), 1355–1387 (1975)
4. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc. (1993)
5. Ferguson, N., Schneier, B., Kohno, T.: Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing (2010)
6. Wiesner, S.: Conjugate coding. SIGACT News. 15(1), 78–88 (1983)
7. Benioff, P.: The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by turing machines. J. Stat. Phys. 22(5), 563–591 (1980)
8. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. 21(6), 467–488 (1982)
9. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997)
10. Bennett, C., Brassard, G.: Quantum cryptography and its application to provably secure key expansion, public-key distribution, and cointossing. In: Proceedings of IEEE International Symposium on Information Theory: Abstracts of Papers, St. Jovite, Canada, pp. 91–99. IEEE (1983)
11. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems and Signal Processing, New York, pp. 175–179. (1984)
12. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. 75, 1239–1243 (1995)
13. Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89(18), 187902 (2002)
14. Shimizu, K., Imoto, N.: Communication channels secured from eavesdropping via transmission of photonic Bell states. Phys. Rev. A. 60, 157–166 (1999)
15. Beige, A., et al.: Secure communication with a publicly known key. Acta Phys. Pol. A. 101(3), 357–368 (2002)
16. Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A. 65, 032302. arXiv preprint quant-ph/0012056, 2000 (2002)
17. You, X., et al.: Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci. China Inf. Sci. 64, 110301 (2020)
18. Dieks, D.: Communication by EPR devices. Phys. Lett. 92(6), 271–272 (1982)
19. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature. 299, 802–803 (1982)
20. Fuchs, C.A., van de Graaf, J.: Cryptographic distinguishability measures for quantum-mechanical states. IEEE Trans. Inform. Theory. 1999;45:1216–1227 (1999)
21. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)
22. Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A. 68(4), 042317 (2003)
23. Deng, F.-G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A. 69, 052319 (2004)
24. Long, G.-L, et al.: Quantum secure direct communication and deterministic secure quantum communication. Front. Phys. China. 2(3), 251–272 (2007)
25. Beaudry N.J., et al.: Security of two-way quantum key distribution. Phys. Rev. A. 88(6), (2013)
26. Chen, H., et al.: Experimental demonstration on the deterministic quantum key distribution based on entangled photons. Sci. Rep. 6(1), 20962 (2016)
27. Utagi, S., Srikanth, R., Banerjee, S.: Ping-pong quantum key distribution with trusted noise: non-Markovian advantage. Quantum Inf. Process. 19(10), 366 (2020)
28. Kiktenko, E.O., et al.: Lightweight authentication for quantum key distribution. IEEE Trans. Inf. Theory. p. 66(10), 6354–6368 (2020)
29. Sun, S., et al.: Design and implementation of a practical quantum secure direct communication system. In: 2018 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. (2018)
30. Pan, D., et al.: Single-photon-memory Two-Step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs. IEEE Access. 8, 121146–121161 (2020)
31. Sun, Z., et al.: Towards practical quantum secure direct communication: a quantum-memory-free protocol and code design. IEEE Trans Commun. 68(9), 5778–5792 (2020)
32. Wu, J., et al.: Security of quantum secure direct communication based on Wyner's wiretap channel theory. Quantum Engineering. 1(4), e26 (2019)
33. Zhang, W., et al.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. 118(22), 220501 (2017)

34. Yang, W., Schaefer, R.F., Poor, H.V.: Wiretap channels: nonasymptotic fundamental limits. IEEE Trans. Inform. Theory. 65(7), 4069–4093 (2020)
35. Stinespring, W.F.: Positive functions on C*-algebras. Proc. Am. Math. Soc. 6(2), 211 (1955)
36. Lo, H., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science. 283(5410), 2050–2056 (1999)
37. Bennett, C.H., Brassard, G., Breidbart, S., Wiesner, S.: Quantum cryptography, or unforgeable subway tokens. In: Chaum, D., Rivest, R.L., Sherman, A.T., editors. Advances in Cryptology, pp. 267–275. Springer US, Boston, MA (1983)
38. Ye, Z.-D., et al.: Generic security analysis framework for quantum secure direct communication. Front. Phys. 16(2), 21503 (2020)
39. Hu, J.-Y., et al.: Experimental quantum secure direct communication with single photons. Light Sci. Appl. 5(9), e16144 (2016)
40. Zhu, F., et al.: Experimental long-distance quantum secure direct communication. Sci. Bull. 62(22), 1519–1524 (2017)
41. Qi, R., et al.: Implementation and security analysis of practical quantum secure direct communication. Light Sci. Appl. 8(1), 22 (2019)
42. Pan, D., et al.: Experimental free-space quantum secure direct communication and its security analysis. Photon Res. 8(9), 1522–1531 (2020)
43. Niu, P.-H., et al.: Security analysis of measurement-device-independent quantum secure direct communication. Quantum Inf. Process. 19(10), 356 (2020)
44. Zhou, L., Sheng, Y.-B., Long, G.-L.: Device-independent quantum secure direct communication against collective attacks. Sci. Bull. 65(1), 12–20 (2020)

How to cite this article: Zawadzki P. Advances in quantum secure direct communication. *IET Quant. Comm.* 2021;2:54–62. https://doi.org/10.1049/qtc2.12009

A. Supplement

The states of a quantum system with N degrees of freedom are represented by normalized elements of N-dimensional Hilbert vector space over the field of complex numbers. In Dirac notation, these states are denoted by the symbol $|\psi\rangle$, with the state label in parentheses. In a matrix representation, the states $|\psi\rangle$ take the form of column vectors. The vectors $\langle\psi| = (|\psi\rangle)^\dagger$ are obtained by the Hermitian conjugate, which in the matrix representation consists of transposition combined with a complex conjugate items $([A]^\dagger = ([A]^T)^*)$. We write the dot product of vectors as $\langle\psi|\varphi\rangle$, which in the matrix representation is equivalent to multiplying a row vector by a column one. The dot product takes complex values in a generic case, but the norm of the vector $||\psi|| = \langle\psi|\psi\rangle^{1/2}$ is well-defined.

A.1. Qubits

Qubits are represented as the normalized elements of two-dimensional Hilbert space. Let $\{|0\rangle, |1\rangle\}$ be some orthonormal base. We will then refer to this base as the computational base. Any qubit can be represented as $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. The two basic qubit operations are the phase flip $[Z]$ and qubit negation $[X]$:

$$[Z] = |0\rangle\langle 0| - |1\rangle\langle 1|, [Z]|\psi\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|) \times (\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_0|0\rangle - \alpha_1|1\rangle, \tag{10a}$$

$$[X] = |1\rangle\langle 0| + |0\rangle\langle 1|, [X]|\psi\rangle = (|1\rangle\langle 0| + |0\rangle\langle 1|) \times (\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_0|1\rangle + \alpha_1|0\rangle. \tag{10b}$$

Elements of the computational base are the eigenvectors of the phase flip operation $[Z]$ and correspond to the eigenvalues $\{+1, -1\}$. The dual base is formed by the eigenvectors of the negation operation $[X]$. They can be expressed in the computational base as $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. They also correspond to the eigenvalues $\{+1, -1\}$, respectively. Elements of the computational base can be converted into dual base vectors (and vice versa) using the Hadamard operation $[H] = ([Z] + [X])/\sqrt{2}$:

$$|+\rangle = [H]|0\rangle, |-\rangle = [H]|1\rangle. \tag{11}$$

A.2. Observables

Measurable quantities, or observables, are represented by self-adjoint operators $([A]^\dagger = [A])$. Let us denote the eigenstates and eigenvalues of the measured observable $[A]$ as $\{|\lambda_k\rangle\}_{k=1}^N$ and $\{\lambda_k\}_{k=1}^N$, respectively. The eigenstates of any observable form the base of the space, so state $|\psi\rangle$ of the system before measurement can be represented as $|\psi\rangle = \sum_{k=1}^N \langle\lambda_k|\psi\rangle|\lambda_k\rangle$. The measurement causes the measured object to change its state into one of the eigenvectors of the measured observable. The eigenvalue corresponding to this state is the outcome of the measurement. The final state is selected randomly, with the selection probability determined by the length of projection of the state before measurement on the available eigenstates that is $p(\lambda_k) = |\langle\lambda_k|\psi\rangle|^2$. Thus, the measurement of the observable will not change the state of the system only if the system before the measurement is in one of its eigenstates. Observables that commute, that is, $[A][B] = [B][A]$, have a common set of eigenvectors.

A.3. Einstein-Podolsky-Rosen pairs

The Hilbert space representing a system composed of many qubits is a tensor product of spaces representing the components forming the system. Some states of a composite system can be presented as a tensor product of the qubit states forming the system: for example, $|\psi_{\mathrm{AB}}\rangle = |\alpha_{\mathrm{A}}\rangle|\beta_{\mathrm{B}}\rangle$. These states are called separable. States that cannot be decomposed into a tensor product are referred to as entangled states.

A controlled negation gate, $[CX]$, is one of the most common operations on multiqubit systems. It is defined as a

$$[CX]_{\mathrm{AB}} = |0_{\mathrm{A}}\rangle\langle 0_{\mathrm{A}}| \otimes [I]_{\mathrm{B}} + |1_{\mathrm{A}}\rangle\langle 1_{\mathrm{A}}| \otimes [X]_{\mathrm{B}}$$

where the first elements of the tensor product are applied to the control qubit and the identity and negation modify the state of the target qubit. EPR states are pairs of entangled qubits of the form:

$$|\Phi^{+}\rangle = |\beta_{00}\rangle = [CX]_{\mathrm{A\ B}}[H]_{\mathrm{A}}|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle=$$

$$=\frac{|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle + |1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle}{\sqrt{2}} = \frac{|+_{\mathrm{A}}\rangle|+_{\mathrm{B}}\rangle + |-_{\mathrm{A}}\rangle|-_{\mathrm{B}}\rangle}{\sqrt{2}} \tag{12a}$$

$$|\Psi^{+}\rangle = |\beta_{01}\rangle = [CX]_{\mathrm{A\ B}}[H]_{\mathrm{A}}|0_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle=$$

$$=\frac{|0_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle + |1_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle}{\sqrt{2}} = \frac{|+_{\mathrm{A}}\rangle|+_{\mathrm{B}}\rangle - |-_{\mathrm{A}}\rangle|-_{\mathrm{B}}\rangle}{\sqrt{2}} \tag{12b}$$

$$|\Phi^{-}\rangle = |\beta_{10}\rangle = [CX]_{\mathrm{A\ B}}[H]_{\mathrm{A}}|1_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle=$$

$$=\frac{|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle - |1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle}{\sqrt{2}} = \frac{|+_{\mathrm{A}}\rangle|-_{\mathrm{B}}\rangle + |-_{\mathrm{A}}\rangle|+_{\mathrm{B}}\rangle}{\sqrt{2}} \tag{12c}$$

$$|\Psi^{-}\rangle = |\beta_{11}\rangle = [CX]_{\mathrm{A\ B}}[H]_{\mathrm{A}}|1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle=$$

$$=\frac{|0_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle - |1_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle}{\sqrt{2}} = \frac{|-_{\mathrm{A}}\rangle|+_{\mathrm{B}}\rangle - |+_{\mathrm{A}}\rangle|-_{\mathrm{B}}\rangle}{\sqrt{2}} \tag{12d}$$

The EPR pair generation is reversible. The pair identification procedure by application of the inverse operation followed by the query of qubits is called the Bell measurement:

$$[H]_{\mathrm{A}}[CX]_{\mathrm{A\ B}}|\beta_{\mu\nu}\rangle = |\mu_{\mathrm{A}}\rangle|\nu_{\mathrm{B}}\rangle \tag{13}$$

The Bell measurement will return a random value when the measured qubits are not in the EPR state; for example:

$$[H]_{\mathrm{A}}[CX]_{\mathrm{A\ B}}|0_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle = |+_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle \tag{14}$$

EPR pairs form a base in a two-bit state space, and the calculated base elements can be expressed as:

$$|00\rangle \quad =(|\beta_{00}\rangle + |\beta_{10}\rangle)/\sqrt{2} \quad |01\rangle \quad =(|\beta_{01}\rangle + |\beta_{11}\rangle)/\sqrt{2} \tag{15a}$$

$$|10\rangle \quad =(|\beta_{01}\rangle - |\beta_{11}\rangle)/\sqrt{2} \quad |11\rangle \quad =(|\beta_{00}\rangle - |\beta_{10}\rangle)/\sqrt{2} \tag{15b}$$

Access to one of the qubits that make up a pair enables its deterministic transformation into another type of pair:

$$[Z]_{\mathrm{A}}^{\mu}[X]_{\mathrm{A}}^{\nu}|\beta_{m,n}\rangle = (-1)^{m\nu}|\beta_{m\oplus\mu,n\oplus\nu}\rangle \tag{16}$$

where $\oplus$ denotes summation modulo 2.

According to the laws of quantum mechanics, objects spaced apart can be entangled. This property is often used in quantum cryptography. Let Alice and Bob operate in distant locations and share an EPR pair of known type. One may assume that it is in state $|\beta_{00}\rangle$ without a loss of generality. At the cost of destroying the pair, they can agree on a random classical bit. The value of that bit is confidential and it can be used for cryptographic purposes, such as a one-time key in the OTP algorithm. However, to achieve that goal, Alice and Bob have to use the classical communication channel to synchronize their actions. Alice measures $[Z]$ on her qubit and asks Bob to perform the same measurement. She can receive outcomes ± 1 with probability 1/2. Her measurement will result also in a collapse of the shared pair to one of the states, $|0_{\mathrm{A}}\rangle|0_{\mathrm{B}}\rangle$ or $|1_{\mathrm{A}}\rangle|1_{\mathrm{B}}\rangle$. Bob will always get the same result as Alice because of that collapse. This reasoning also applies to $[X]$ because of Equation (12a). For other EPR pairs, the type of correlation may depend on the measured observables, but the determinism of the procedure is still preserved. The shared pair can also be used to transmit two classical bits confidentially by transmitting only one qubit. Alice may encode two classical bits of information by transforming a shared pair into any other type with an operation (16) applied to her qubit. She then sends her half of the pair to Bob, who decodes the information by making Bell measurements. Eve, who may be controlling a quantum channel, cannot do anything to retrieve the information encoded in this way. Regardless of the type of pair after encoding, the measurement of the qubit en route will randomly return values ± 1. Collapse of the pair and the randomization of Bob's outcomes will be a side effect of such activity. Entanglement can therefore be used as a substitute of the encryption key, but this time the confidentiality of information results directly from the laws of physics and the provided security is independent of Eve's resources. Achieving a situation in which legitimate parties share EPR pairs of a known form is a fundamental design problem of entanglement-based QSDC protocols.