A quantum key distribution scheme based on tripartite entanglement and violation of CHSH inequality

Davide Pastorello*
Department of Mathematics, University of Trento,
Trento Institute for Fundamental Physics and Applications
via Sommarive 14, 38123 Povo (Trento), Italy.

Abstract
Entanglement is a well-known resource in quantum information, in particular it can be exploited for quantum key distribution (QKD). In this paper we define a two-way QKD scheme employing GHZ-type states of three qubits obtaining an extension of the standard E91 protocol with a significant increasing of the number of shared bits. Eavesdropping attacks can be detected measuring violation of the CHSH inequality and the secret key rate can be estimated in a device-independent scenario.

Keywords: Quantum key distribution, entanglement, Bell’s inequalities

1 Introduction
Quantum processes can be used to distribute a secret key (a random bit-string) in order to use it as a one-time pad for secure communications [6, 11]. Quantum key distribution (QKD) over a quantum channel prevents effective eavesdropping attacks exploiting principles of Quantum Mechanics. An eavesdropper cannot clone an unknown quantum state (no-cloning theorem [18]) thus he extracts information performing measurement processes, the quantum effects of these measurements can be detected showing that the communication channel is not secure. One of the most celebrated QKD scheme is the E91 protocol [13] which exploits quantum correlations of entangled states to share a private key and uses a measure of the violation of Bell inequalities to check if an eavesdropping occured over the quantum channel.

This paper is devoted to define and analyze a modification of standard E91 protocol based on preparation and processing of tripartite entangled states. The main idea is defining a two-way protocol where Bob transmits a half of an entangled state to Alice who entangles the received state with a third part, as an encoding operation, before re-sending it to Bob. Then he performs a decoding to read the information communicated by Alice, after the decoding operation the clients share a maximally entangled state which can be used to implement a standard E91 protocol as a subroutine. The classical postprocessing is equivalent to that of E91 protocol, so the security analysis is similar. The advantage w.r.t. to the standard E91 protocol (which can be described as a one-way protocol) is the doubled length of the secret key at the same cost of transmitted qubits. Even if an eavesdropper, Eve, can attack each signal twice, we observe that any Eve’s strategy produces a destruction of quantum correlations which can be taken under

*d.pastorello@unitn.it
control by the violation of CHSH inequality. In particular the effect of noise on the secret key rate can be evaluated in terms of such a violation.

In the next section we recall some basic features of quantum systems that are relevant in the present discussion, in particular we refer to finite-dimensional case. In the third section there is a short review on Bell’s inequalities, their physical meaning and relative application in quantum key distribution (E91 protocol). In the fourth section we describe the proposed QKD scheme as a two-way extension of the standard E91 protocol based on tripartite entanglement. In the fifth section we analyze the robustness of the protocol against eavesdropping like intercept/re-send attacks from a qualitative viewpoint. We show that the security of the protocol is based on the violation of CHSH inequality and entanglement monogamy. In the sixth section we remark that an estimation of the secret key rate can be computed in a device-independent scenario after applying a prescription to purify two-way QKD protocols. In the last section there are conclusions and an overview on open issues about the security proof. A technical observation about the entanglement class of the considered states is given in appendix.

2 Preliminaries and notations

According to standard formulation of Quantum Mechanics, a complex vector space $H$ with inner product $\langle \cdot | \cdot \rangle$ (a Hilbert space) is associated to any quantum system. If $\dim H = 2$ then the considered quantum system is called qubit.

Let $\mathcal{B}(H)$ be the space of linear operators on $H$, the set of physical states of the considered quantum system is defined as:

$$\mathcal{S}(H) := \{ \rho \in \mathcal{B}(H) : \rho \geq 0, \text{tr}\rho = 1 \}. \quad (1)$$

$\mathcal{S}(H)$ is convex in $\mathcal{B}(H)$ and its extremal elements, called pure states, are the rank-1 orthogonal projectors in $H$, a non-pure state is called mixed state. Since a pure state $\rho$ can be written as $\rho = |\psi\rangle \langle \psi|$ for some unit vector $|\psi\rangle \in H$, then pure states can be represented by equivalence classes of unit vectors where the equivalence relation between $|\psi\rangle$ and $|\psi'\rangle$ is defined by $|\psi\rangle \sim |\psi'\rangle$ iff $|\psi\rangle = e^{i\theta}|\psi'\rangle$ for some $\theta \in \mathbb{R}$. Therefore two unit vectors differing by a multiplicative phase factor describe the same pure state.

Time evolution of an isolated system is described by a continuous one-parameter group of unitary operators $\{U(t)\}_{t \in \mathbb{R}^+}$ acting on states. If $\rho_1$ is the state of the system at time $t_1$ and $\rho_2$ is the state of the system at time $t_2 > t_1$ then:

$$\rho_2 = U(t_2 - t_1)\rho_1 U^* (t_2 - t_1). \quad (2)$$

A measurement process on a quantum system is described by a collection of positive operators $\{E_k\}$ satisfying $\sum_k E_k = I_H$ called positive operator-valued measures (POVM), the index $k$ runs in the set of all possible outcomes of the measurement, so it is a real number. The probability to measure $k$ when the system is in the state $\rho$ is:

$$p_\rho(k) = \text{tr}(E_k \rho). \quad (3)$$

If we consider a pure state $|\psi\rangle$ then above probability is simply given by $p_\psi(k) = \langle \psi | E_k |\psi\rangle$.

A special class of POVMs is that of projective valued measures (PVMs) whose elements are orthogonal projectors $P_k$, i.e. operators on $H$ satisfying $P_k^* = P_k$ and $P_k^2 = P_k$. In this case if the measurement is performed when the state of the system is $\rho \in \mathcal{S}(H)$ and it produces the outcome $k$ then the state of the system after the measurement is:

$$\rho' = \frac{P_k \rho P_k}{\text{tr}(P_k \rho)}, \quad (4)$$

\[1\]We adopt Dirac formalism: A unit vector of the Hilbert space is denoted by the ket $|\psi\rangle$, a vector of dual space is denoted by the bra $\langle \psi|$, the inner product of two vectors is denoted by $\langle \psi|\phi\rangle$, the outer product by $|\psi\rangle\langle\phi|$. 

2
and a selfadjoint operator on $H$, called *observable*, can be defined:

$$A := \sum_k kP_k,$$

so the possible outcomes of the measurement described by the PVM $\{P_k\}$ are the eigenvalues of $A$. If the state of the system is $\rho \in \mathcal{S}(H)$ then the *expectation value* of $A$ is

$$\langle A \rangle_\rho = \sum_k k p_\rho(k) = \text{tr}(A \rho).$$

Another fundamental quantum feature is the following: If a quantum system is composed by two subsystems $A$ and $B$ that are respectively described in Hilbert spaces $H_A$ and $H_B$, then the composite system is described in the Hilbert space tensor product $H_A \otimes H_B$.

Quantum systems, in particular qubits, can be exploited as information storages and physical operations on them can be used for processing and transmitting information. Let $H$ be a 2-dimensional Hilbert space and $(|0\rangle, |1\rangle)$ be an orthonormal basis of $H$ that can be identified as the standard basis of $\mathbb{C}^2$. In the following we call $(|0\rangle, |1\rangle)$ the *computational basis* of $H$. One can assume the vectors $|0\rangle$ and $|1\rangle$ physically represent the eigenstates of a reference observable, e.g. the rectilinear polarization of a photon described by the Pauli matrix $\sigma_z$. Another basis of $H$ is given by $(|+\rangle, |−\rangle)$ with $|+\rangle := 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|−\rangle := 1/\sqrt{2}(|0\rangle − |1\rangle)$, the vectors $|+\rangle, |−\rangle$ can be physically interpreted as the eigenstates of circular polarization of a photon for instance.

**Definition 1** Let $H$ be a 2-dimensional Hilbert space and $n \in \mathbb{N}$. The Hilbert space $H^\otimes n$ is called *n-qubit register* and any unitary operator acting on $H^\otimes n$ is called *n-qubit quantum gate*.

The *Hadamard gate* $H$ is a 1-qubit quantum gate defined w.r.t. the computational basis by $H|0\rangle := |+\rangle$ and $H|1\rangle := |−\rangle$ and it is denoted by the symbol:

$$\includegraphics{hadamard_gate.png}$$

The Hilbert space of a qubit pair is $H \otimes H$, with dim $H = 2$, an orthonormal basis of $H \otimes H$ is $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$, where $|00\rangle \equiv |0\rangle \otimes |0\rangle$, that we call *computational basis* of $H \otimes H$. A remarkable 2-qubit gate is the *CNOT gate* $\Lambda$ that is defined in the computational basis by:

$$\Lambda|00\rangle := |00\rangle \quad \Lambda|01\rangle := |01\rangle \quad \Lambda|10\rangle := |11\rangle \quad \Lambda|11\rangle := |10\rangle,$$

i.e. $\Lambda$ acts as the identity when the first qubit is in $|0\rangle$ and acts as a bit-flip on the second qubit when first qubit is in $|1\rangle$. The CNOT gate is denoted by the symbol:

$$\includegraphics{cnot_gate.png}$$

CNOT gate can be used to define another useful element of a quantum circuit, the *SWAP gate*:

$$\includegraphics{swap_gate.png}$$

that switches the input qubits. In the fourth section we define a quantum circuit to entangle three qubits for our QKD purpose.
3 CHSH inequality and standard E91 protocol

Let us briefly recall the notions of entanglement, violation of Bell’s inequalities and E91 protocol. Since composite quantum systems are described in tensor product Hilbert spaces, the definition of quantum state itself implies that there is a class of quantum states containing non-classical correlations that are inherently non-local.

**Definition 2** Let \( \rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B) \) be a state of a composite quantum system. \( \rho \) is said to be **separable** if it can be written as:

\[
\rho = \sum_i \lambda_i \rho_i^A \otimes \rho_i^B
\]  

(10)

with \( \rho_i^A \in \mathcal{S}(\mathcal{H}_A), \rho_i^B \in \mathcal{S}(\mathcal{H}_B), \lambda_i \geq 0 \) and \( \sum_i \lambda_i = 1 \). Otherwise it is called **entangled**.

Entanglement can be interpreted as a non-local property: Consider the entangled pure state of a qubit pair identified by the vector \( |\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\varphi\rangle) \in \mathcal{H}_A \otimes \mathcal{H}_B \), if one performs the PVM-measurement \( \{\{0\} \otimes |\psi\rangle, |1\rangle \otimes |\varphi\rangle\} \) on the first qubit then the state of the second qubit collapses in \( |\psi\rangle \) or in \( |\varphi\rangle \) according to the outcome of the local measurement, this phenomenon occurs even if the qubits are spacelike separated (EPR paradox [12]). However this non-local feature cannot be used for communications faster than light (no-communication theorem [15]).

In order to elucidate the content of Bell theorem [4], let us briefly discuss the notion of local hidden variable theory based on the assumption of local realism. Let us adopt the term local realism in reference to a pair of properties that a general physical theory can present:

i) **Principle of locality**: If two events are outside their respective light cones then there is no causal connection among them.

ii) **Counterfactual-definiteness**: The values of physical quantities are definite and unaffected by any measurement process.

Consider a bipartite quantum system composed by a subsystem \( A \) and a subsystem \( B \), suppose to perform local measurements on \( A \) and \( B \) obtaining correlated outcomes when they are spatially separated. Invoking local realism we are assuming that local measurements are independent and do not perturb the systems. So the probability to measure value \( k \in \mathbb{R} \) by a POVM measurement \( E \) on the system \( A \) and value \( l \in \mathbb{R} \) by a POVM measurement \( D \) on the system \( B \) can be generally expressed by:

\[
p(E, k; D, l) = \int_X F_E(k, x)F_D(l, x)d\mu(x),
\]  

(11)

where \((X, \mu)\) is a measure space, \( x \mapsto F_E(k, x) \) and \( x \mapsto F_D(l, x) \) are measurable functions associated to POVMs \( E \) and \( D \). The product \( F_E(k, x)F_D(l, x) \) is the probability to obtain value \( k \in \mathbb{R} \) by the measurement process \( E \) on the first subsystem and value \( l \in \mathbb{R} \) by the measurement process \( D \) on the second subsystem for a fixed value of the parameter \( x \), called hidden variable, encoding correlations between subsystems.

**Definition 3** A quantum state \( \rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B) \) admits a hidden variable model if for all POVMs \( E = \{E_k\}_k \subset \mathcal{B}(\mathcal{H}_A) \) and \( D = \{D_l\}_l \subset \mathcal{B}(\mathcal{H}_B) \) there exists a measure space \((X, \mu)\) and measurable functions \( x \mapsto F_E(k, x) \) and \( x \mapsto F_D(l, x) \) such that:

\[
\text{tr}(\rho(E_k \otimes D_l)) = \int_X F_E(k, x)F_D(l, x)d\mu(x).
\]  

(12)

for any \( k \) and \( l \).
The above definition provides a class of states of a composite quantum system such that introducing a fictitious variable $x$ quantum correlations can be treated as classical correlations in presence of local realism. The set of states admitting a hidden variable model is non-empty, in particular it contains all separable states.

**Proposition 4** Any separable state $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ admits a hidden variable model.

Proof. If $\rho$ is separable then we have the convex combination:

$$\rho = \sum_{i=1}^{n} \lambda_i \rho_i^{(A)} \otimes \rho_i^{(B)}$$

with $\rho_i^{(A)} \in \mathcal{S}(\mathcal{H}_A), \rho_i^{(B)} \in \mathcal{S}(\mathcal{H}_B)$. Let be $X := \{1, 2, 3, ..., n\}$ and $\mu(\{i\}) := \lambda_i$. For all POVMs $\{E_k\}_k \in \mathfrak{B}(\mathcal{H}_A)$ and $\{D_l\}_l \in \mathfrak{B}(\mathcal{H}_B)$ let us define:

$$F_E(k, x) := \rho_x^{(A)}(E_k) \ \ , \ \ F_D(l, x) := \rho_x^{(B)}(D_l),$$

obtaining the hidden variable model. \qed

Within a hidden variable model, correlation functions obey to a set of constraints called **Bell’s inequalities**. In particular we consider the **CHSH-inequality** (Clauser, Horne, Shimony, Holt [17]) to formulate the Bell theorem:

**Theorem 5** If a state $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ admits a hidden variable model then it satisfies CHSH-inequality:

$$|\mathrm{tr}[\rho(A \otimes (B - B'))] + \mathrm{tr}[\rho(A' \otimes (B + B'))]| \leq 2,$$

for all $A, A' \in \mathfrak{B}(\mathcal{H}_A)$ such that $-I_{\mathcal{H}_A} \leq A, A' \leq I_{\mathcal{H}_A}$ and for all $B, B' \in \mathfrak{B}(\mathcal{H}_B)$ such that $-I_{\mathcal{H}_B} \leq B, B' \leq I_{\mathcal{H}_B}$.

We have that the violation of CHSH inequality is a sufficient condition for the entanglement of a state, on the contrary there are entangled states admitting a hidden variable model [16].

A remarkable example of CHSH violation is the following: Consider the Pauli matrices $\sigma_x$ and $\sigma_z$ and define the hermitian operators in $\mathfrak{B}(\mathbb{C}^2)$: $A := \sigma_x, A' := \sigma_z, B := \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), B' := \frac{1}{\sqrt{2}}(-\sigma_x + \sigma_z)$. Consider the unit vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$|\Phi \rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

i.e. an entangled pure state of a qubit pair. We can calculate the left-hand term of (13) where $\rho = |\Phi \rangle \langle \Phi |$, obtaining by direct inspection:

$$|\langle \Phi | A \otimes (B - B') \Phi \rangle + \langle \Phi | A' \otimes (B + B') \Phi \rangle| = 2\sqrt{2},$$

then CHSH inequality is violated. More precisely (14) is a maximally entangled state and (15) is the maximum violation of CHSH inequality (experimentally measured for the first time by Aspect et al. in 1982 [2]).

The E91 protocol [13] is based on the production of a qubit pair in the maximally entangled pure state (14) by Alice. Then she sends one qubit of the pair to Bob [2]. Alice measures one of the following observables on her qubit:

$$A_1 = \sigma_x, \quad A_2 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \quad A_3 = \sigma_z,$$

\(^{2}The entangled qubit pair can be produced by an external source (including an eavesdropper) sending one qubit to Alice and the other one to Bob.
on the other side Bob measures one of the following observables on his qubit:

\[
B_1 = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) \quad B_2 = \sigma_z \quad B_3 = \frac{1}{\sqrt{2}}(-\sigma_x + \sigma_z).
\]  

(17)

If qubits are polarized photons or spin-$\frac{1}{2}$ particles then different measurement processes correspond to different orientation angles of Alice and Bob’s analyzers. If Alice and Bob perform the same measurement process then their outcomes coincide.

Let us summarize E91 protocol as follows:

**Step 1**: A pair of entangled qubits is produced by Alice. She sends a qubit of the entangled pair to Bob. Alice measures observable $A_i$ with $i \in \{1,2,3\}$ on her qubit. Bob measures observable $B_j$ with $j \in \{1,2,3\}$ on his qubit. The procedure is repeated $N$ times.

**Step 2**: Alice and Bob declare on a classical public channel what observable they have measured on each qubit. They store the outcomes produced measuring the same observable obtaining two perfectly correlated bit string (sifted key) of length $n \simeq \frac{N}{3}$.

**Step 3**: Alice and Bob declare on a classical public channel the outcomes produced by different measurements in order to calculate:

\[
S := \langle \Phi | A_1 \otimes (B_2 - B_3) \Phi \rangle + \langle \Phi | A_3 \otimes (B_2 + B_3) \Phi \rangle.
\]  

(18)

At the end of the round the maximum violation of CHSH inequality is expected $S = 2\sqrt{2}$. If the experimental value is $S < 2\sqrt{2}$ then some measurement process in the middle of quantum transmission has altered the state of entangled pairs destroying the quantum correlation, hence an eavesdropping attack has been detected. However a sifted key may be not discarded even if $S < 2\sqrt{2}$, since an estimation of Eve’s information in post-processing could show that the survived quantum correlations allowed to produced an acceptable secret key. In this regards see section 6 where some estimations are sketched for the two-way protocol. On the other hand the extreme case $S \leq 2$ entails the erasure of any quantum correlation.

Obviously a classical authentication protocol must be implemented over the classical channel in order to ensure that the right person is at the end of the line.

### 4 The proposed QKD protocol

According to definition 2 a pure state $|\phi\rangle\langle \phi| \in \mathcal{S}(H_A \otimes H_B)$ is separable if and only if $|\phi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ with $|\psi_A\rangle \in H_A$ and $|\psi_B\rangle \in H_B$. More generally: Let $\{H_1,...,H_n\}$ be a family of finite-dimensional Hilbert spaces. A pure state, represented by $|\phi\rangle \in H_1 \otimes \cdots \otimes H_n$, is separable if and only if $|\phi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ with $|\psi_i\rangle \in H_i$ for $i = 1,...,n$. Otherwise if $|\phi\rangle$ is not a product vector then the corresponding pure state is entangled.

For instance a pure state of three qubits can be separable like $|010\rangle$, 2-entangled like $|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes |1\rangle$ or 3-entangled like $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. More precisely pure states of three qubits $a,b,c$ are divided in six entanglement classes: One class of separable states ($a-b-c$), three classes of 2-entangled states ($a-bc$, $b-ac$, $c-ab$) and two classes of 3-entangled states. These classes correspond to the orbits of the group $GL(2,\mathbb{C})^{\otimes 3}$ [9]. Representative elements of inequivalent classes of genuine tripartite entangled states of three qubits are:

\[
|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad \text{and} \quad |W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle).
\]  

(19)

In this section we propose a QKD protocol where an entangled state of GHZ-type is prepared and processed in order to implement an improved version of E91 protocol which is capable of a superdense key distribution, i.e. the length of the sifted key is double at the same cost of
standard E91 protocol in terms of the transmitted qubits number.
Consider the Hilbert space $H \otimes H$ of a qubit pair, an orthonormal basis can be defined by means of the Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

representing the maximally entangled states of two qubits.

Let $\Sigma : H \otimes H \to H \otimes H$ be a quantum gate defined in the computational basis as follows:

$$\Sigma|00\rangle := |\Phi^+\rangle, \quad \Sigma|11\rangle := |\Phi^-\rangle, \quad \Sigma|10\rangle := |\Psi^+\rangle, \quad \Sigma|01\rangle := |\Psi^-\rangle.$$ (21)

The corresponding graphical representation is:

(22)

The simplest quantum gate to construct Bell states is

(23)

whose action on the computational basis is $|00\rangle \mapsto |\Phi^+\rangle$, $|11\rangle \mapsto |\Psi^-\rangle$, $|10\rangle \mapsto |\Phi^-\rangle$ and $|01\rangle \mapsto |\Psi^+\rangle$.

However $\Sigma$ admits an elementary property that we are going to apply.

**Proposition 6** Let $\Omega : H^\otimes 3 \to H^\otimes 3$ be the quantum gate defined as $\Omega := (I \otimes \Sigma)(\Sigma \otimes I)$. Therefore $\Omega(|\psi\rangle \otimes |\Phi^+\rangle) = |\Phi^+\rangle \otimes |\psi\rangle$ for any $|\psi\rangle \in H$.

Proof. Consider $|\psi\rangle \in H$ decomposed on the computational basis $|\psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{C}$. One can explicitly calculate the action of $\Omega$ on $|0\rangle \otimes |\Phi^+\rangle$ and $|1\rangle \otimes |\Phi^+\rangle$:

$$\Omega(|0\rangle \otimes |\Phi^+\rangle) = (I \otimes \Sigma)(\Sigma \otimes I) \left[ \frac{1}{\sqrt{2}}(|000\rangle + |011\rangle) \right] =$$

$$= (I \otimes \Sigma) \left[ \frac{1}{2}(|000\rangle + |110\rangle + |011\rangle - |101\rangle) \right] = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = |\Phi^+\rangle \otimes |0\rangle.$$

$$\Omega(|1\rangle \otimes |\Phi^+\rangle) = (I \otimes \Sigma)(\Sigma \otimes I) \left[ \frac{1}{\sqrt{2}}(|100\rangle + |111\rangle) \right] =$$

$$= (I \otimes \Sigma) \left[ \frac{1}{2}(|101\rangle + |100\rangle + |001\rangle - |111\rangle) \right] = \frac{1}{\sqrt{2}}(|001\rangle + |111\rangle) = |\Phi^+\rangle \otimes |1\rangle.$$

Hence $\Omega(|\psi\rangle \otimes |\Phi^+\rangle) = |\Phi^+\rangle \otimes |\psi\rangle$ by linearity. \qed
Considering three qubits where two are maximally entangled, the action of $\Omega$ transfers the state of the first qubit to the third one entangling the other two. In particular the action of $\Sigma \otimes I$ creates a state where entanglement is distributed over all qubits. So we can assume to encrypt the state $|\psi\rangle$ in a 3-entangled state by application of $\Sigma \otimes I$ then one can apply $I \otimes \Sigma$ to decrypt $|\psi\rangle$. Since two qubits remain entangled they can be used to check the presence of eavesdroppers implementing an additional ordinary E91 protocol.

Suppose a client, Bob, prepares a qubit pair in the state $|\Phi^+\rangle_{bc} \in H_b \otimes H_c$ sending the qubit $b$ to Alice and keeping the qubit $c$ in his hands. Meanwhile Alice prepares a qubit in the state $|x\rangle_a \in H_a$ giving rise to the tripartite quantum state $|\epsilon_x\rangle_{abc} := |x\rangle_a \otimes |\Phi^+\rangle_{bc} \in H_a \otimes H_b \otimes H_c$, where $x = 0, 1$.

Let $A_1, A_2, A_3, B_1, B_2, B_3$ be the observables defined in (16) and (17), a QKD protocol can be realized as follows:

**Step 1** Alice and Bob share a quantum state $|\epsilon_x\rangle_{abc} = |x\rangle_a \otimes |\Phi^+\rangle_{bc}$, with $x = 0, 1$ (the qubit pair $ab$ in Alice’s lab and qubit $c$ in Bob’s lab), by means of the transmission of the qubit $b$. Then Alice performs the local operation described by $\Sigma$ generating the following tripartite entangled state:

$$
(\Sigma \otimes I)|\epsilon_x\rangle_{abc} = \begin{cases} 
\frac{1}{2}(|000\rangle_{abc} + |110\rangle_{abc} + |011\rangle_{abc} - |101\rangle_{abc}) & \text{if } x = 0 \\
\frac{1}{2}(|010\rangle_{abc} + |100\rangle_{abc} + |001\rangle_{abc} - |111\rangle_{abc}) & \text{if } x = 1
\end{cases}
$$

**Step 2** Alice sends the qubit $b$ to Bob. He processes the pair $bc$ with gate $\Sigma$.

**Step 3** Alice measures the observable $A_j$, with $j \in \{1, 2, 3\}$, on the qubit $a$. Bob measures the observable $B_j$ with $j \in \{1, 2, 3\}$ on the qubit $b$ and measures the observable $B_2$ on the qubit $c$ obtaining the outcome $x$. The value $x$ is stored as a bit of the secret key. The procedure is repeated $N$ times.

**Step 4** Alice and Bob declare over a classical public channel the measured observables recording the outcomes produced by corresponding measurements. These bits give an additional contribution to the secret key.

**Step 5** Alice and Bob declare over a classical public channel the outcomes produced by different measurements in order to compute the test statistics (18) detecting eventual eavesdropping.

![Figure 1. A circuit diagram schematizing the structure of the proposed protocol.](image-url)
attacks.

In Appendix we will remark that the state (24) belongs to the GHZ class by the computation of the Cayley’s hyperdeterminant.

Assuming Steps 1-3 are repeated $N$ times ($2N$ transmitted qubits in total), Alice and Bob share a bit string of length $n \simeq N + \frac{N}{3} = \frac{4N}{3}$. Otherwise adopting the standard E91 protocol described in the previous section Alice and Bob share a key of length $n \simeq \frac{2N}{3}$ by means of the transmission of $2N$ qubits.

The cryptographic scheme can be represented by the quantum circuit diagram of Figure 1: The gate (23), initialized in $|00\rangle$, is inserted on the Bob’s side to produce the maximally entangled state $|\Phi^+\rangle$ that is shared by the clients.

5 Security against eavesdropping: Qualitative analysis

Suppose an eavesdropper (Eve) wants to move an attack in order to gain the private key during the QKD. Let us show that she cannot gain sufficient information to get the sifted key nor keeping hidden her attack. Suppose Eve is able to interept the transmitted qubits over the quantum channel. Let us exclude the case of a man-in-the-middle attack where Eve plays the part of Alice for Bob and viceversa sharing two different private keys with the clients because we are assuming the existence of a standard authentication protocol over the classical channel that is necessary for the sifting phase and the computation of the test statistic (18).

A general eavesdropping strategy is given by performing a measurement on the first transmitted qubit and processing the second one in a suitable way. If Eve intercepts the first qubit and performs the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ then she destroys the entanglement of the pair $bc$ shared by the clients. More in detail, suppose Eve measures the value 0 then Alice receives the qubit $b$ in the pure state $|0\rangle$ (so Bob’s qubit $c$ collapses in $|0\rangle$ as well and Eve can make a copy of this qubit), by the application of the gate $\Sigma$ on the separable state $|x\rangle \otimes |0\rangle$ Alice obtains the state $|\Phi^+\rangle$ if $x = 0$ or the state $|\Psi^+\rangle$ if $x = 1$. Suppose Eve intercepts also the second quantum transmission (from Alice to Bob), since she does not know the value of $x$, her knowledge of the total system is encoded in the following incoherent superposition:

$$\rho_{Eve} = \frac{1}{2} (|\Phi^+0\rangle\langle\Phi^+0| + |\Psi^+0\rangle\langle\Psi^+0|).$$

(25)

If the state of the three qubits is (25) then Eve cannot gain information about the value of $x$ (that is a bit of the key) by means of a single measurement process or any local operation on the qubit pair $bc'$, where $c'$ is her copy of the qubit $c$. However she makes datum $x$ inaccessible to Bob as a minor result, at this stage Eve’s goal is keeping hidden her interference. Therefore suppose Eve does nothing in order to avoid any perturbation of the quantum transmission from Alice to Bob. Assuming $x = 0$ (the case $x = 1$ is analogue), when Bob performs $\Sigma$ on the qubit pair $bc$ then the state of the total system becomes:

$$(I \otimes \Sigma)|\Phi^+0\rangle = \frac{1}{\sqrt{2}} (|0\Phi^+\rangle + |1\Psi^+\rangle),$$

(26)

so when Bob measures the qubit $c$ obtains a randomized value instead of $x = 0$, however the reduced state of the qubit pair $ab$ turns out to be:

$$\rho_{ab} = \frac{1}{2} (|\Phi^+\rangle\langle\Phi^+| + |\Psi^+\rangle\langle\Psi^+|),$$

(27)

that is a separable state, in fact it can be written as a convex combination of separable pure states: $\rho_{ab} = \frac{1}{2}(|++\rangle\langle++| + |--\rangle\langle--|)$. As a consequence Eve’s measurements on the first transmitted qubit (from Bob to Alice) can be detected by the computation of test statistic even
if no operation is performed on the second transmitted qubit (from Alice to Bob). On the other hand Eve can intercept qubit $b$ once again (after Alice’s processing) and perform some operation to hide her attack during the previous quantum transmission. However any local operation performed by Eve cannot entangle the qubit $b$ (to be re-transmitted to Bob) with the qubit $c$ of Bob so the computation of test statistic reveals an interception over the quantum channel.

Another general eavesdropping strategy is entangling the intercepted qubits with a probe quantum system in Eve’s hands. Assume Eve intercepts the first transmitted qubit and acts with an entangler, i.e. a quantum operation on the bipartite system made by the intercepted qubit and an ancillary system (the probe) producing an entangled state. So the goal of Eve is entangling a probe with Alice and Bob’s systems in order to gain the values of datum $x$ (i.e. 3/4 of the secret key at the end of the round) performing measurements only on her system leaving correctly correlated Alice and Bob’s qubits. This goal is unattainable because of entanglement monogamy that can be expressed by CKW inequality [7]: If two quantum systems $A$ and $B$ are maximally entangled then $A$ or $B$ cannot be entangled with a third system $C$. So when Alice receives the first qubit after the action of Eve’s entangler, it cannot be maximally entangled with Bob’s qubit as provided by the protocol then CHSH inequality cannot be maximally violated. On the other hand if Eve wants to gain the value of $x$ she must perfectly entangle the intercepted qubit with the probe destroying the quantum correlation with the Bob’s qubit at all.

6 Security against eavesdropping: Quantitative estimates

After a qualitative discussion on intercept/re-send attacks let us quantify the security of the protocol within a general device-independent scenario. Hence we assume that any element of the QKD scheme is completely untrusted, i.e. Eve may have fabricated the measuring devices of Alice and Bob in addition to controlling the entanglement source. So Alice and Bob can estimate Eve’s information only by qubit error rate $Q$ and violation $S$ of CHSH inequality.

The qubit error rate is given by the weighted sum of the probabilities of mismatching outcomes:

$$Q = \frac{1}{8} p(a_2 \neq b_1) + \frac{1}{8} p(a_3 \neq b_2) + \frac{3}{4} p(x \neq x_b),$$

where $a_i$ are the measurement outcomes of $A_i$ obtained by Alice, $b_j$ are the outcomes of $B_j$ measured on qubit $b$ and $x_b$ is the outcome of $B_2$ measured on qubit $c$ by Bob. Then normalized mutual information between Alice and Bob is:

$$I_{AB} = 1 - H(Q),$$

where $H$ is the binary entropy function.

In order to evaluate the secret key rate of the protocol, we can consider the purified version of the protocol applying lemma 1 in [3]. When Alice receives the qubit from Bob, she acts with an encoding (given by the processing with the gate $\Sigma$ for a fixed value of the parameter $x$) before re-sending the qubit. In the purified setting, the encoding operation (described by the action a completely positive trace-preserving map) is equivalent as a POVM-measurement (with binary outcome) performed on the received state with the half of an entangled state so that, after the measurement, the other half corresponds to the encoded state to be sent to Bob. Hence, within the purified version of the protocol, we can assume that a pure state $|\Psi\rangle_{ABE} \in H_A \otimes H_B \otimes H_E$ is shared among Alice, Bob and Eve and dimensions of $H_A$ and $H_B$ are unknown to Alice and Bob but fixed by Eve according to the device-independent assumption. Alice performs a measurement process $M_A$ (representing the encoding) and another one $M(A_j)$ (corresponding to the measurement of $A_j$) on two subspaces of $H_A$, on the other side Bob performs his measurement $M(B_j) \otimes M(B_2)$. All the measurement processes are defined by Eve who controls the devices. The measurement $M_A$ produces two possible outcomes that are assumed to be correlated to the outcomes of $M(B_2)$ then the purified protocol is equivalent to E91 protocol where the involved
measurement processes are $E_j^A := M_A \otimes M(A_j)$ and $E_j^B := M(B_j) \otimes M(B_2)$, for $j = 1, 2, 3$.

In order to estimate the accessible information to Eve we consider the Holevo quantity $\chi_{EB}$ between Eve and Bob. Since our purified protocol turns out to be a modification of E91 protocol within the device-independent scenario, then $\chi_{EB}$ is completely characterized by the violation $S$ of CHSH inequality and applying the main result of [1] we have:

$$\chi_{EB} \leq H \left( \frac{1 + \sqrt{(S/2)^2 - 1}}{2} \right). \tag{30}$$

The secret key rate $r$ is lower-bounded by Devetak-Winter rate $r_{DW}$ [8]:

$$r \geq r_{DW} = I_{AB} - \chi_{EB}, \tag{31}$$

where $I_{AB}$ is given by (29) and $\chi_{BE}$ is constrained by (30). Under assumption of device-independence, we can provide the following secret key rate for the presented protocol:

$$r \geq 1 - H(Q) - H \left( \frac{1 + \sqrt{(S/2)^2 - 1}}{2} \right). \tag{32}$$

According to the first analysis of the protocol in section 4, the ratio between the length of the secret key and the total number of the transmitted qubit is:

$$R = \frac{2}{3} r, \tag{33}$$

which attains the maximum for $Q = 0$ and $S = 2\sqrt{2}$.

Summarizing: The two-way protocol can be purified applying lemma 1 in [3], so that the scheme can be described within a device-independent scenario where Alice and Bob share a pure state with Eve. They perform local measurements on their states like in E91 protocol, under collective attacks (i.e. Eve moves the same attack to each system of Alice and Bob) the Holevo quantity between Bob and Eve can be evaluated in terms of violation of CHSH inequality.

7 Conclusions and open issues

In this paper we have described a two-way QKD protocol based on the preparation and processing of tripartite GHZ-type entangled states. A quantum circuit has been defined to entangle three qubits in order to implement a quantum transmission where the receiver measures two distinct outcomes: The value of a fixed bit and another value to compute the test statistic to quantifying violation of CHSH inequality like within the ordinary E91 protocol. The maximum violation shows that no eavesdropping attack occurred like in the standard picture. In the ideal case of no eavesdropping and no noise at all the length of the sifted key is $n \simeq \frac{2}{3} N$, where $N$ is the total number of transmitted qubits, instead of $n \simeq \frac{N}{3}$. Moreover we have focused on the security of the QKD scheme with a qualitative and a semi-quantitative analysis. Eve cannot perform any operation to gain the values of the datum $x$ or disturb the key distribution without introducing local realism in the system. The monogamy of entanglement prevents any perfectly hidden eavesdropping attack which is moved entangling intercepted qubits with an auxiliary system. In order to evaluate the trade-off between secret key rate and noise we have considered the purification of the protocol which allow us to analyze the security within a device-independent scenario where Alice, Bob and Eve share a pure state and the only figures of merit to estimate the secret key rate are the qubit error rate and the violation of CHSH inequality. Although we presented a lower bound for the secret key rate in a device-independent scenario, further work is needed to reach a complete and satisfactory security proof of the protocol. In this regard an interesting direction of investigation could be the estimation of the effects of noise, modeled by depolarizing channels and decoherence channels, on the security.
References

[1] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani Device-independent security of quantum cryptography against collective attacks Phys. Rev. Lett. 98, 230501 (2007)

[2] A. Aspect, J. Dalibard, G. Roger Experimental test of Bell’s inequalities using time-varying analyzers Phys. Rev. Lett. 49, 1804-1807 (1982)

[3] N. J. Beaudry, M. Lucamarini, S. Mancini, R. Renner Security of two-way quantum key distribution Phys. Rev. A 88, 062302 (2013)

[4] J. S. Bell On Einstein Podolski Rosen paradox Physics 1, 195-200 (1964)

[5] C. H. Bennett and G. Brassard in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York, 1984) pp. 175-179

[6] I. Chuang, M. Nielsen, Quantum Computation and Quantum Information Cambridge University Press (2000)

[7] V. Coffman, J. Kundu, W. K. Wootters Distributed entanglement Phys. Rev. A 61 052306 (2000)

[8] I. Devetak, A. Winter Distillation of secret key and entanglement from quantum states Proc. R. Soc. Lond. A 461, 207 (2005)

[9] W. Dür, G. Vidal, J. I. Cirac Three qubits can be entangled in two inequivalent ways Phys.Rev. A62 (2000) 062314

[10] I. M. Gelfand, N. M. Kapranov, A.V. Zelevinski Hyperdeterminants Adv. in Mathematics 96, 226-263 (1992)

[11] C. Kollmitzer, M. Pivk Applied Quantum Cryptography Lecture Notes in Physics 797 (2010)

[12] A. Einstein, B. Podolski, N. Rosen Can Quantum-Mechanical description of physical reality be considered complete? Phys. Rev. 47, 777 (1935)

[13] A.K. Ekert, Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67, 661 (1991)

[14] H. Ollivier, W. H. Zurek Quantum Discord: A measure of quantumness of correlations. Phys. Rev. Lett. 88, 017901 (2001)

[15] A. Peres, D.R. Terno Quantum information and relativity theory Rev. Modern Physics 76.1:93 (2004)

[16] R.F. Werner Quantum states with Einstein-Podolski-Rosen correlations admitting a hidden-variable model. Phys. Rev. A 40, 4277-4281 (1989)

[17] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt Proposed experiment to test local hidden-variable theories Phys. Rev. Lett. 23, no. 15, 880-884 (1969)

[18] W.K. Wootters, W.H. Zurek A Single Quantum Cannot be Cloned. Nature 299, 802-803 (1982)
Appendix

As a technical observation let us remark that the entangled states \((\Sigma \otimes \mathbb{I}_2)|\epsilon_0\rangle\) and \((\Sigma \otimes \mathbb{I}_2)|\epsilon_1\rangle\), defined in (24), belong to the same entanglement class, in fact they are related by means of the invertible local operation \(\mathbb{I}_2 \otimes \sigma_x \otimes \mathbb{I}_2\).

**Proposition 7**  The pure state (24) belongs to the entanglement class of the state GHZ.

**Proof.** If we consider a pure state \(|\Psi\rangle = \sum_{ijk=0}^{1} a_{ijk} |ijk\rangle\) of three qubits, the Cayley’s hyperdeterminant of its coefficients hypermatrix is defined as:

\[
\begin{align*}
\text{Det}(|\Psi\rangle) &:= a_{000}^2 a_{111} + a_{001}^2 a_{110} + a_{100}^2 a_{011} - 2[a_{000} a_{001} a_{110} a_{111} + a_{010} a_{101} a_{011} a_{111} + \\
&+ a_{000} a_{011} a_{100} a_{111} + a_{001} a_{010} a_{101} a_{110} + a_{001} a_{011} a_{101} a_{100} + a_{010} a_{011} a_{101} a_{100}] + \\
&+ 4[a_{000} a_{011} a_{101} a_{100} + a_{001} a_{010} a_{100} a_{111}].
\end{align*}
\]

We have \(\text{Det}[(\Sigma \otimes \mathbb{I}_2)|\epsilon_x\rangle_{abc}] = 1\) for \(x = 0, 1\). The Cayley’s hyperdeterminant is invariant under the action of \(SL(2, \mathbb{C})^{\otimes 3}\) [10], then the property \(\text{Det} \neq 0\) is invariant under the action of \(GL(2, \mathbb{C})^{\otimes 3}\). Since \(\text{Det}(|W\rangle) = 0\) and \(\text{Det}(|GHZ\rangle) = 1/4\) we can conclude that (24) is a GHZ-type state. \(\square\)