Técnico Lisboa
University of Lisbon

Research Seminar in Information Security

(Prof. Paulo MATEUS)

Doctoral Program in Information Security

2023/2024 - 1st Semester

Device-Independent Entanglement Certification with Dishonest Parties

(Gláucia MURTA - November 23, 2023)

Report written by:

- Rúben BARREIRO:
  - *ruben.andre.letra.barreiro@tecnico.ulisboa.pt*

Last updated: February 29, 2024

1 Motivation

One of the tasks of interest in this seminar is to address how to certify some resource states and their quantum properties distributed in a future (experimental) Quantum Communication Network connecting several quantum devices (or quantum nodes) in different places. These quantum properties can be entanglement properties of those resource states distributed on a Quantum Communication Network involving some scenario aspects, such as geographic proximity or political relations. These quantum nodes might be prone to collaborate with each other, so we cannot assume they do their tasks independently. In these scenarios, we would like to certify the entanglement properties even in the presence of some dishonest party. Here, the minimal level of characterization we would want to guarantee for these quantum network systems is that they are Device-Independent (DI). In this characterization scenario, we assume that there might exist some dishonest parties in the quantum network. However, we also want to keep the privacy

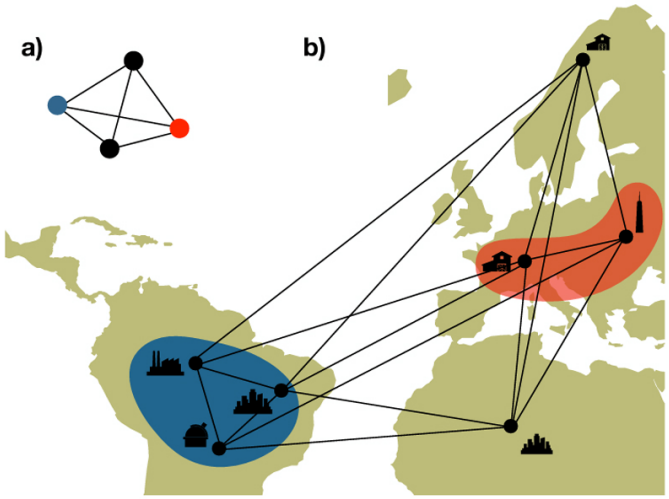

Figure 1: a) Effective Quantum Communication Network for self-testing, where each cluster is treated as a single party. b) Corresponding pictorial representation of a quantum network with cooperating clusters. Shaded blue and red regions indicate nodes that are likely to collude.

of the operations and tasks performed by the quantum nodes or devices in that quantum network. Thus, the main goal of a DI scenario would be for

these quantum nodes and devices to perform these operations and tasks only based on statistics of inputs and outputs rather than the exact details of the laboratories of the experimental setup for this designed quantum network.

This seminar addresses aspects of a research work published by Gláucia Murta from Heinrich-Heine University of Düsseldorf in collaboration with Flavio Baccari from Max-Planck Institute of Quantum Optics, where they introduced a framework for DI entanglement certification with the presence of dishonest parties, obtaining some self-testing properties and a robust certification of particular resource states such as Greenberger–Horne–Zeilinger (GHZ) states [1] in these Quantum Communication Network scenarios [2].

2 Entanglement Certification

The first part of this seminar addressed a simple qualitative overview of the scenario previously introduced, with only an entanglement verification of a simple quantum network. In this simple scenario, instead of having several different clusters of collaborating parties, we have only N parties and a subset D of $(N-K+1)$ dishonest parties that could be collaborating. This simple scenario is a little different from the standard DI scenario. Namely, in the DI scenario, we assume we do not know what the quantum devices or nodes are actually doing. On the other hand, in this scenario variant, some of those quantum devices or nodes could work together and apply some arbitrary joint operations they could communicate. Therefore, in this new scenario, we do not have this overview network separation, and, in fact, we could say one subset of parties is dishonest, although we do not need to know which of them is indeed dishonest. In this quantum communication network,

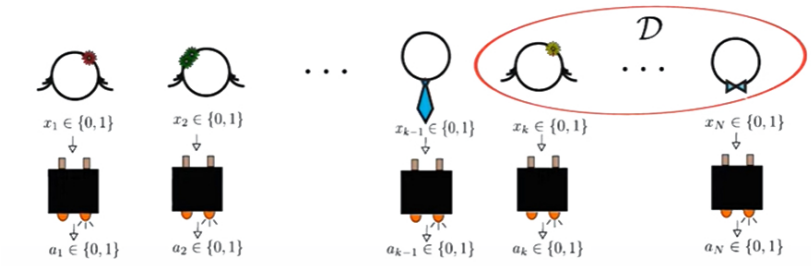

Figure 2: Illustration of Quantum Communication Network scenario with a set $\mathcal{D}$ of dishonest parties.

the honest parties only have local uncharacterized quantum devices or quantum nodes. On the other hand, the dishonest ones are allowed to communicate among themselves, apply classical post-processing operations, and perform joint measurements. In this scenario, we assume the dishonest parties can also control their quantum devices or quantum nodes. However, in the end, we can obtain the statistics, and therefore, we still want to analyze the distributed quantum entanglements through the quantum network.

But the crucial aspect here is that we are actually going to address a DI scenario where we will need a Bell Inequality [3]. The results obtained by the authors demonstrate we can use a particular class of Bell Inequalities to achieve such a strong characterization for this scenario. In this case, the Bell Inequality of interest is called the Svetlichny Inequality [4, 5], an inequality where each one of the parties gets two inputs and two outputs. This inequality is also known as the Full Correlator Inequality since we only have terms that involve the expected value of the observables of all the parties together. Basically, this correlator results in 1 if the parity of the parties' measurement outcomes is 0 and results in -1 if the parity of outcomes is 1. These N-partite Svetlichny Inequalities have the following form below:

$$S_N^{\pm} = \sum_{\vec{x}} (-1)^{\frac{w_{\vec{x}} \times (w_{\vec{x}} \pm 1)}{2}} \left\langle A_{x_1}^{(1)} A_{x_2}^{(2)} \dots A_{x_N}^{(N)} \right\rangle$$

Where:

$\vec{x} = (x_1, x_2, \dots x_N)$ is the bitstring of inputs for all N parties,

$w_{\vec{x}}$ is the Hamming weight of $\vec{x}$,

$$\left\langle A_{x_1}^{(1)} A_{x_2}^{(2)} \dots A_{x_N}^{(N)} \right\rangle = p\left(\oplus_{j=1}^{N} a_j = 0 | x_1 x_2 \dots x_N\right) - p\left(\oplus_{j=1}^{N} a_j = 1 | x_1 x_2 \dots x_N\right),$$

$$\text{and } S_N^{\pm} \overset{\mathcal{C}}{\leq} 2^{(N-1)} \overset{\mathcal{Q}}{\leq} 2^{(N-1)} \times \sqrt{2},$$

for a classical bound $\mathcal{C}$ and a (estimated) quantum bound $\mathcal{Q}$.

Therefore, this is a family of N-partite Svetlichny Inequalities for any number N of parties. Such as any other Bell Inequality, these Svetlichny Inequalities have a classical bound that Quantum Mechanics can violate, as well as they have a (estimated) quantum bound. However, this classical bound is a little more interesting in the sense that when we have more than $N = 2$ parties, we start having a structure for the outcomes of our parties involved, so

we do not have only a separable notion for them (e.g., local or non-local), but also a different structure notion, namely a party grouping concept.
This classical bound $S_N^{\pm} \overset{\mathcal{C}}{\leq} 2^{(N-1)}$ sets a limit for all the probability distributions in a way we cannot decompose them in the following form:

$$p(a_1 a_2 \dots a_N | x_1 x_2 \dots x_N) =$$
$$= \sum_{\mathcal{P} \subsetneq [N]} \int p(\lambda) \times \underbrace{p\left(a_{\mathcal{P}} | (x_{\mathcal{P}} \times \lambda)\right)}_{\text{arbitrary } [1]} \times p\left(a_{\mathcal{P}^{\mathcal{C}}} | (x_{\mathcal{P}^{\mathcal{C}}} \times \lambda)\right) \; d\lambda$$

From this mathematical form, we can divide the subset of parties into two main groups, where we may have arbitrary collaborations within these groups, but we still have some separate actions. Then, we can take some convex combination of this type of correlation, where we have arbitrary correlations within these groups of parties. And, since these correlations are within this local classical bound, we are able to witness a strong genuine multipartite non-locality. Thus, we violate the Svetlichny Inequality only when we cannot decompose this probability distribution in this mathematical form. Nowadays, the first proposal for the definition of genuine multipartite non-locality, where Svetlichny allowed this joint probability distribution of the group to be arbitrary, is not used anymore because when we abstract from the considered scenario, we usually want to look at non-locality property as an operational framework, what leads to some inconsistencies if we define locality regarding that operational outlook [6]. To overcome this, people often add some assumptions to these joint probability distributions, often assuming they have to be non-signaling or one-way signaling [6, 7], but they cannot be arbitrary. However, for our scenario, it turns out that this definition is the one that is interesting because we want to address these collaborating parties that could be realizing an arbitrary action. Another important observation is that this inequality also detects Genuine Multipartite Entanglement (GME) since we would never be able to violate it if the quantum entangled state we want to verify is bi-separable in the standard Bell Inequality scenario.
A violation of this GME would imply the following mathematical expression:

$$\rho \neq \sum_{\mathcal{P} \subsetneq [N]} \sum_i q_{\mathcal{P}}^i \times \rho_{\mathcal{P}}^i \otimes \rho_{\mathcal{P}^{\mathcal{C}}}^i$$

[1] Detects strong genuine multipartite non-locality.

For the Svetlichny Inequality with dishonest parties, the honest action would be the following observable, which describes a subtraction between two arbitrary Positive Operator-Valued Measure (POVM) elements, one for each measurement outcome, where, in principle, honest actions should apply local actions, but they will have these two global POVM elements instead:

$$\textbf{Honest Action: } A_{x_i}^{(i)} = \prod\nolimits_{0|x_i} - \prod\nolimits_{1|x_i},\ i \in \mathcal{H}$$

$$\textbf{Dishonest Action: } A_{x_K}^{(K)} \times A_{x_{(K+1)}}^{(K+1)} \times \ldots A_{x_N}^{(N)} \rightarrow M_{x_K x_{(K+1)} \ldots x_N}^{(N)}$$

Now we can look at the Svetlichny Inequality for $N = 3$ (similar to the tripartite Mermin's Inequality [8] that contains half of the terms of this tripartite Svetlichny Inequality) through the mathematical expression below:

$$N = 3,\ \mathcal{H} = \{\text{Alice}\},\ \mathcal{D} = \{\text{Bob, Charlie}\}$$

$$\begin{aligned} S_3 = &\langle A_0 B_0 C_0\rangle - \langle A_0 B_1 C_0\rangle - \langle A_1 B_0 C_0\rangle - \langle A_1 B_1 C_0\rangle \\ &- \langle A_0 B_0 C_1\rangle - \langle A_0 B_1 C_1\rangle - \langle A_1 B_0 C_1\rangle + \langle A_1 B_1 C_1\rangle \Leftrightarrow \\ S_3 = &\langle A_0 M_{00}\rangle - \langle A_0 M_{10}\rangle - \langle A_1 M_{00}\rangle - \langle A_1 M_{10}\rangle \\ &- \langle A_0 M_{01}\rangle - \langle A_0 M_{11}\rangle - \langle A_1 M_{01}\rangle + \langle A_1 M_{11}\rangle \end{aligned}$$

Thus, this Svetlichny Inequality contains all the possible terms we might have, and we can recall that Quantum Mechanics does not saturate the algebraic bound in this inequality. For example, for a tripartite scenario, we can have Alice as an honest party, while Bob and Charlie are dishonest parties. Therefore, Bob and Charlie can apply a joint operator, and we can rebuild what is the actual inequality with the mathematical expression below:

$$\begin{aligned} S_3 = &\langle A_0 M_{00}\rangle - \langle A_0 M_{10}\rangle - \langle A_1 M_{00}\rangle - \langle A_1 M_{10}\rangle \\ &- \langle A_0 M_{01}\rangle - \langle A_0 M_{11}\rangle - \langle A_1 M_{01}\rangle + \langle A_1 M_{11}\rangle \\ = &\beta_0 + \beta_1 \end{aligned}$$

$$\Downarrow$$

$$S_3 \leq 2 \times \max\{\beta_0, \beta_1\} = 2 \times \beta, \beta \geq \frac{S_3}{2}$$

By doing this mathematical reformulation, if we are familiar with the non-locality concept, we can recognize two Clauser-Horne-Shimony-Holt

(CHSH) Inequalities in the expression resulting from it. The structure of these symmetric Svetlichny Inequalities says that if we have a tripartite inequality and violate it with these dishonest parties, we know they are in a Bell scenario with two practical parties. On one side, we have Alice as an honest party from set $\mathcal{H}$, and on the other, we have Bob and Charlie together in a group from set $\mathcal{D}$, and they would be violating the CHSH Inequality. What we show is that this property happens for any number K of honest parties and any total number N of parties. So, whenever we have Svetlichny Inequality and K effective parties, we would have a violation of a corresponding K-partite inequality in the standard Bell scenario, where these K parties are not communicating. Thus, we have the following statement:

$$|\mathcal{H}| = (K-1),\ |\mathcal{D}| = (N-K+1)$$

Violation of S_N in the Svetlichny Inequality Scenario

$$\Downarrow$$

Violation of S_K in the standard Bell Inequality Scenario

With:

$$S_K \geq \frac{S_N}{2^{(N-K)}},$$

where S_N denotes violation of S_N^+ or S_N^-.

From this property, we can get this qualitative certification where we do not know which parties in our Quantum Communication Network are dishonest, but we are certifying that we have a genuine K-partite quantum entanglement between the sets of honest parties and dishonest parties. As a result, we obtain a **certification of genuine K-partite entanglement among the honest parties and the unknown set of dishonest parties**.

3 Self-Testing with Dishonest Parties

In particular, what is interesting here is that we can also perform a stronger characterization of our simplest scenario, such that we do not have just the qualitative entanglement witnessing but also a self-testing result in that scenario. For completeness and to define this self-testing, we should consider that we have a probability distribution of outcomes given the inputs,

and with that, we can infer that we have a specific quantum state. Namely, all the self-testing results cannot guarantee the absolute occurrence of this quantum state. However, we can infer its occurrence from the correlations of the probability distribution of outcomes up to some undetectable symmetry (local isometries), and we can be sure that we have our quantum state $|\phi\rangle$. Then, the formal self-testing statement will be of the following form:

$$p(a_1, a_2, \ldots, a_N|x_1, x_2, \ldots, x_N) \longrightarrow |\phi\rangle^2$$

From which it is stated the following:

$$\Lambda_1 \otimes \Lambda_2 \otimes \cdots \otimes \Lambda_N(|\psi\rangle) = |\phi\rangle \otimes |\zeta\rangle,$$

where:

$|\psi\rangle$: Quantum state producing the observed correlations,

$|\zeta\rangle$: Uncorrelated degrees of freedom, and

Λ_i: Local isometries.

We have a quantum state $|\psi\rangle$ that produces the correlations we observed, and these correlations ensure that there is a set of local isometries Λ_i, with $1 \leq i \leq N$, that we could apply to the quantum state that brings me to the target quantum state $|\phi\rangle$ and some extra uncorrelated degrees of freedom $|\zeta\rangle$. Now, we can extend this definition of self-testing to the DI quantum network scenario. Here, the idea is that we cannot prevent the set of dishonest parties from applying a global operation. So, we would define the self-testing up to local isometries and global isometry of the set of dishonest parties. Moreover, the authors proved that if we have the maximum violation of this Svetlichny Inequality, we could self-test that we have the K-partite GHZ state between the set of honest parties and the global set of dishonest parties. Therefore, **a maximum violation of an N-partite Svetlichny Inequality self-tests a K-partite GHZ state shared by the honest parties and the set of dishonest parties $\mathcal{D}$**, as we mathematically demonstrate below:

$$\Lambda_1 \otimes \Lambda_2 \otimes \cdots \otimes \Lambda_{(K-1)} \otimes \Lambda_{\mathcal{D}}(|\psi\rangle) = \left|\phi^K_{GHZ}\right\rangle \otimes |\zeta\rangle$$

[2]Up to undetectable symmetries (local isometries).

In order to give a little idea of the corresponding proof, let's consider the previously mentioned observation that there are some CHSH Inequalities in the Svetlichny Inequality. Namely, the Svetlichny Inequality has several terms that increase with the number N of parties. But, we can always decompose this inequality into some inequalities called S_2, for example. We use this terminology because the first and the second parties have different inputs, but all the other parties have the same fixed input. Thus, the first and second parties provide a CHSH Inequality, while the remaining parties always provide the same input for the mathematical expressions below:

$$S_N^+ = \sum_{\substack{\vec{x}_{(N-2)} \\ \omega_{\vec{x}} \text{ odd}}} (-1)^{\frac{\omega_{\vec{x}_{(N-2)}} \cdot \left(\omega_{\vec{x}_{(N-2)}}+1\right)}{2}} \times S_2^- \times \left(\vec{x}_{(N-2)}\right) +$$

$$+ \sum_{\substack{\vec{x}_{(N-2)} \\ \omega_{\vec{x}} \text{ even}}} (-1)^{\frac{\omega_{\vec{x}_{(N-2)}} \cdot \left(\omega_{\vec{x}_{(N-2)}}+1\right)}{2}} \times S_2^+ \times \left(\vec{x}_{(N-2)}\right)$$

Where:

$$S_2^+ \left(\vec{x}_{(N-2)}\right) = \left\langle A_0^{(1)} A_0^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle - \left\langle A_0^{(1)} A_1^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle -$$
$$- \left\langle A_1^{(1)} A_0^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle - \left\langle A_1^{(1)} A_1^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle$$

$$S_2^- \left(\vec{x}_{(N-2)}\right) = \left\langle A_0^{(1)} A_0^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle + \left\langle A_0^{(1)} A_1^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle +$$
$$+ \left\langle A_1^{(1)} A_0^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle - \left\langle A_1^{(1)} A_1^{(2)} A_{x_3}^{(3)} \dots M_{\vec{x}_{\mathcal{D}}}^{(K)} \right\rangle$$

Another part of the proof idea is that these S_2 Inequalities are very similar to CHSH Inequalities, except we have the operators of all the other parties. Then, we can construct a Sum Of Squares (SOS) decomposition of each term, which is usually a standard technique used to prove self-testing experimental

results. This SOS decomposition for each term is demonstrated below:

$$2\times\sqrt{2}\times\mathbb{1}-\hat{S}^{+}_{2,\vec{x}_{(N-2)}}=\frac{1}{\sqrt{2}}\left[\left(\mathbb{1}-\frac{\hat{A}^{(1)}_0-\hat{A}^{(1)}_1}{\sqrt{2}}\hat{A}^{(2)}_0\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}\right)^2+\right.$$
$$\left.+\left(\mathbb{1}+\frac{\hat{A}^{(1)}_0+\hat{A}^{(1)}_1}{\sqrt{2}}\hat{A}^{(2)}_1\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}\right)^2\right]$$

$$2\times\sqrt{2}\times\mathbb{1}-\hat{S}^{-}_{2,\vec{x}_{(N-2)}}=\frac{1}{\sqrt{2}}\left[\left(\mathbb{1}-\frac{\hat{A}^{(1)}_0+\hat{A}^{(1)}_1}{\sqrt{2}}\hat{A}^{(2)}_0\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}\right)^2+\right.$$
$$\left.+\left(\mathbb{1}-\frac{\hat{A}^{(1)}_0-\hat{A}^{(1)}_1}{\sqrt{2}}\hat{A}^{(2)}_1\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}\right)^2\right]$$

Then, we can finally obtain the stabilizer conditions, as well as the respective commutation relations of the operator for a K-partite GHZ state:

$$(-1)^{\frac{\omega_{\vec{x}_{(N-2)}}\cdot\left(\omega_{\vec{x}_{(N-2)}}+1\right)}{2}}\times\frac{A^{(1)}_0+A^{(1)}_1}{\sqrt{2}}\times A^{(2)}_0\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}|\psi\rangle=|\psi\rangle,$$
$$\text{with } \omega_{\vec{x}_{(N-2)}} \text{ odd},$$

$$(-1)^{\frac{\omega_{\vec{x}_{(N-2)}}\cdot\left(\omega_{\vec{x}_{(N-2)}}+1\right)}{2}}\times\frac{A^{(1)}_0-A^{(1)}_1}{\sqrt{2}}\times A^{(2)}_1\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}|\psi\rangle=|\psi\rangle,$$
$$\text{with } \omega_{\vec{x}_{(N-2)}} \text{ odd},$$

$$(-1)^{\frac{\omega_{\vec{x}_{(N-2)}}\cdot\left(\omega_{\vec{x}_{(N-2)}}+1\right)}{2}}\times\frac{A^{(1)}_0-A^{(1)}_1}{\sqrt{2}}\times A^{(2)}_0\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}|\psi\rangle=|\psi\rangle,$$
$$\text{with } \omega_{\vec{x}_{(N-2)}} \text{ even, and}$$

$$(-1)^{\frac{\omega_{\vec{x}_{(N-2)}}\cdot\left(\omega_{\vec{x}_{(N-2)}}+1\right)}{2}}\times\frac{A^{(1)}_0+A^{(1)}_1}{\sqrt{2}}\times A^{(2)}_1\ldots A^{(K-1)}_{x_{(K-1)}}M^{(K)}_{\vec{x}_{\mathcal{D}}}|\psi\rangle=|\psi\rangle,$$
$$\text{with } \omega_{\vec{x}_{(N-2)}} \text{ even}.$$

In particular, the authors showed an experimental result we do not know so far. Namely, we cannot only use the Mermin's Inequality to self-test the GHZ state, but we can also use the Svetlichny Inequality for that purpose.

Thus, in self-testing, we want to infer if we have the maximum violation and the exact GHZ state. In order to build realistic quantum cryptographic protocols that we can implement shortly, the authors tried to make some robust statements about the quantum state obtained when we do not have a maximum violation of the entanglement. In that direction, for the second part of the proof, the authors tried to deduce which privacy guarantees we can have as a mathematical function of this maximum violation. For that, the authors introduced the concept of fidelity with the target quantum state, generalizing what happens for the standard Bell scenario. In this case, let's assume we have an arbitrary quantum state ρ, and we want to see what fidelity we can obtain for the expected N-partite GHZ state, up to the local quantum channels Λ_i and global quantum channel Λ_D, with the dishonest parties. We can make this statement because, ideally, we would expect the Quantum Communication Network to distribute this N-partite GHZ state. However, it can be distributing another arbitrary quantum state, and we are giving the freedom to the set of dishonest parties to act in that network. So, we can define this described self-testing scenario mathematically as follows:

$$\mathcal{F}_{DI}^{\mathcal{D}(S_N)} = \inf_{\rho \in \mathcal{S}\left(S_N^{\mathcal{D}}\right)} \max_{\Lambda_{\mathcal{D}}, \{\Lambda_i\}_{i \in \mathcal{H}}} \mathcal{F}\left(\otimes_{i \in \mathcal{H}} \Lambda_i \otimes \Lambda_{\mathcal{D}}(\rho), \phi_{GHZ}^N\right)$$

Where:

$\mathcal{S}(S_N^{\mathcal{D}})$**:** Quantum States that achieve value S_N with dishonest parties $\mathcal{D}$;

Λ_i**:** Local Quantum Communication Channels, with $1 \leq i \leq N$;

Λ_i**:** Global Quantum Communication Channel with dishonest parties $\mathcal{D}$.

In the standard Bell scenario, and regarding this self-testing quantity, we do not have the freedom of operations for the set of dishonest parties. However, Jędrzej Kaniewski introduced this self-testing quantity before, and he also introduced a method to bound the fidelity in the standard Bell scenario, called Self-Testing from the OPerator Inequalities (STOPI) [9, 10]. This method transforms the fidelity we pretend to bound into an operator inequality and then calculates some coefficients for this fidelity bound. Some further research work on this concept was done by Jędrzej Kaniewski, Tim Coopmans, and Christian Schaffner, namely in explaining better this method and using it for different Bell Inequalities. For what remains of the idea proof, the authors also showed that in the case we want to bound the fidelity of our quantum state in the presence of dishonest parties, if we have a fixed number

$N-K+1$ of dishonest parties (and $K-1$ honest parties), such that effectively we have a K-partite Bell scenario, we can bound this fidelity quantity using the same coefficients of the standard K-partite Bell scenario. Namely, we only have to apply this method developed for the specific case of the Svetlichny Inequality, and then, we can also generate bounds for the fidelity. We can mathematically define this bound obtained from the STOPI method as:

$$F_{DI}^{|\mathcal{D}|=(N-K+1)} \geq f_K \times \frac{S_N}{2^{(N-K)}} - \mu_K$$

Where:

f_K and μ_K are obtained from the STOPI method.

Self-Testing from the OPerator Inequalities (STOPI):

$$\mathcal{F}\left(\otimes_{i=1}^{k}\ \Lambda_i(\rho), \phi_{GHZ}^{K}\right) = Tr\left(\otimes_{i=1}^{k}\ \Lambda_i^{\dagger}\left(\phi_{GHZ}^{K}\right) \times \rho\right) =$$
$$= Tr(K \times \rho) \rightarrow K - f_K \times S_K + \mu_K \times \mathbb{1} \geq 0$$

Thus, we can guarantee that any fidelity value above 50% certainly implies the occurrence of quantum entanglement, but we can also deduce more about the fidelity quantity even when we do not have the maximum violation.

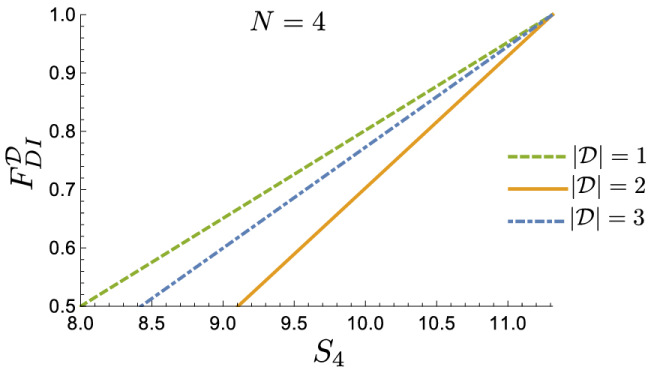

Figure 3: Numerical lower bounds on the fidelity as a function of the violation of a 4-partite Svetlichny Inequality. The curves represent scenarios with different numbers of dishonest parties.

4 Outlook

Now, we can think a little more about open questions of the experimental results obtained by the author, connecting to Quantum Cryptography. There are many quantum cryptographic protocols where the parties might be interested in collaborating and trying to obtain some information before the end of the protocol. Namely, two examples of this situation are the Secret Sharing (SS) and Anonymous Communication protocols. In the SS protocol, a party (e.g., Alice) wants to share a secret (e.g., a quantum or a classical state) with other parties (e.g., Bobs) such that they can recover the secret only if every party collaborates. However, some malicious parties could try to spoil this protocol and get the information before its end. In the Anonymous Communication protocol, a sender (e.g., Alice or an abstract S) who would like to send a message (e.g., a set of quantum or classical states) to a receiver (e.g., Bob or an abstract R) in such a way that everyone in the quantum network has to collaborate for that, but in the end, no one is aware of the identity of each other. Thus, in the end, no one is aware of who is sending the message, and maybe neither the receiver is aware of who sent the message. Therefore, in both of these quantum cryptographic protocols, everyone needs to perform some specific actions, and these protocols are usually based on very particular quantum or classical states to guarantee their security.

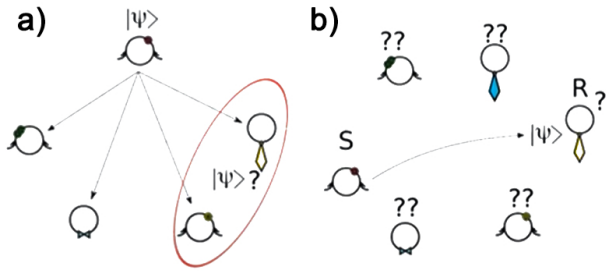

Figure 4: a) Secret Sharing (SS) protocol.
b) Anonymous Communication protocol.

As a next step, the authors pointed out it is desirable to use these experimental results obtained for state certification to prove the security of the quantum cryptographic protocols previously mentioned. However, just the certification is not enough to prove it. For example, in the case of the Anonymous Communication protocol, Matthias Christandl and Stephanie Wehner introduced another protocol that uses the GHZ state, and we can

perform the task of Anonymous Communication once we have that GHZ state, assuming that it is a trusted source that distributes it [11]. Then, in the Anonymous Communication protocol based on this auxiliary protocol, we would like to know that it is the source that distributes the GHZ state but can exist some dishonest parties that might not be following the verification protocol correctly. These certification protocols for the GHZ state in the standard DI scenario, where we know which measurements the parties are performing, have been introduced before [12]. This type of guarantee stating the distance of the quantum state up to a general quantum communication channel on the dishonest parties should be Λ_D for consistent entropy. However, since the distance from the quantum state obtained to the actual GHZ state up to local general operations on the dishonest parties is very small, it is enough to guarantee the security of this task of Anonymous Communication. Hence, we can use this state certification result to have these security guarantees even when we do not have characterized devices. Thus, for a Device-Dependent (DD) certification of a GHZ state, we can compute the ϵ-security bound in the presence of dishonest parties as follows:

$$\min_{\mathcal{M}_{\mathcal{D}}} D\left(Id_{\mathcal{H}} \otimes \mathcal{M}_{\mathcal{D}}(\rho), \phi_{GHZ}^{N}\right) \leq \epsilon$$

Still addressing the connection between state certification and the task of Anonymous Communication, we have another protocol variant based on the W state [13] rather than the GHZ state [14]. So far, there is no state certification for the W state, and maybe the DI scenario approach would be a way to define a non-stabilizer state certification, which we can use to lift the security of this protocol, such that we do not have to trust the source.

Finally, the type of guarantees [11] we usually obtain from self-testing is insufficient [15] because the distance between the quantum state we got and the desired GHZ state is equivalent to the ϵ-security obtained on the protocol proposed by the author. For example, for Quantum Key Distribution (QKD) protocols, we can tolerate noise values usually between 10% and 20% and have ϵ-security with an ϵ value as small as we would like just by performing more rounds of the protocols. A big open question is how to use this type of self-testing result more effectively in Quantum Cryptography or even how we apply it to prove the security of these quantum cryptographic protocols, such that we have ϵ-security but also tolerate a reasonable amount of noise.

References

[1] Daniel Greenberger, Michael Horne, and Anton Zeilinger. Going Beyond Bell's Theorem, 2007.

[2] Gláucia Murta and Flavio Baccari. Self-Testing with Dishonest Parties and Device-Independent Entanglement Certification in Quantum Communication Networks. *Phys. Rev. Lett.*, 131:140201, 2023.

[3] John Bell. On the Einstein Podolsky Rosen Paradox. *Physics Physique Fizika*, 1:195–200, 1964.

[4] George Svetlichny. Distinguishing Three-Body from Two-Body Nonseparability by a Bell-Type Inequality. *Phys. Rev. D*, 35:3066–3069, 1987.

[5] Michael Seevinck and George Svetlichny. Bell-Type Inequalities for Partial Separability in N-Particle Systems and Quantum Mechanical Violations. *Phys. Rev. Lett.*, 89:060401, 2002.

[6] Rodrigo Gallego, Lars Würflinger, Antonio Acín, and Miguel Navascués. Operational Framework for Nonlocality. *Phys. Rev. Lett.*, 109:070401, 2012.

[7] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio. Definitions of Multipartite Nonlocality. *Phys. Rev. A*, 88:014102, 2013.

[8] David Mermin. Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States. *Phys. Rev. Lett.*, 65:1838–1840, 1990.

[9] Jędrzej Kaniewski. Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities. *Phys. Rev. Lett.*, 117:070402, 2016.

[10] Tim Coopmans, Jędrzej Kaniewski, and Christian Schaffner. Robust Self-Testing of Two-Qubit States. *Phys. Rev. A*, 99:052123, 2019.

[11] Matthias Christandl and Stephanie Wehner. *Quantum Anonymous Transmissions*, page 217–235. Springer Berlin Heidelberg, 2005.

[12] Anupama Unnikrishnan, Ian MacFarlane, Richard Yi, Eleni Diamanti, Damian Markham, and Iordanis Kerenidis. Anonymity for Practical Quantum Networks. *Phys. Rev. Lett.*, 122:240501, 2019.

[13] Wolfgang Dür, Guifré Vidal, and Ignacio Cirac. Three Qubits can be Entangled in Two Inequivalent Ways. *Physical Review A*, 62(6), 2000.

[14] Victoria Lipinska, Gláucia Murta, and Stephanie Wehner. Anonymous Transmission in a Noisy Quantum Network Using the W State. *Phys. Rev. A*, 98:052320, 2018.

[15] Federico Grasselli, Gláucia Murta, Jarn de Jong, Frederik Hahn, Dagmar Bruß, Hermann Kampermann, and Anna Pappa. Secure Anonymous Conferencing in Quantum Networks. *PRX Quantum*, 3:040306, 2022.