# DEVICE-INDEPENDENT TRIPARTITE QUANTUM KEY DISTRIBUTION FROM THREE-PLAYER QUANTUM GAMES

Author: Mahrud Sayrafi
Faculty Mentor: Thomas Vidick

Abstract. Quantum entanglement, one of the most counter-intuitive phenomena in quantum theory, has long been studied in information theoretic contexts. It is known that use of entanglement in multiparty game strategies can lead to arbitrarily large advantage over classical players. These violations of classical bounds, known as Bell's inequalities, are due to the nonlocal nature of the correlations.

Here we introduce a protocol for key distribution among three parties who share nothing other than entangled quantum states. Further, we present partial results in enabling any two players to use partial entanglement to produce a key independent of the third player in order to make the protocol resilient against a corrupted player.

This research contributes to the study of non-locality in the reduced bipartite state of an entangled state that maximally violates a tripartite inequality.

## I. Introduction

I.1. **Goals.** In cryptography, key distribution refers to the process in which two or more parties share or exchange a secret key prior to using any encryption algorithm. In 1991 Artur Ekert proposed a quantum key distribution protocol based on quantum entanglement [1]. While classical key distribution protocols rely on a trusted party to share symmetric keys or the computational difficulty of certain mathematical functions to protect asymmetric keys, in 2005 Berrett et al. proved that Ekert's protocol is secure against an eavesdropper with post-quantum physics and only limited by the impossibility of signaling faster than the speed of light [2]. Even more surprising, in 2007 Acin et al. presented a device-independent security proof, meaning that security holds regardless of the way QKD devices work, provided that quantum physics is correct and the parties do not allow any unwanted signals to escape from their laboratories [3].

The primary objective of this research is to extend the previous results by composing a protocol that enables three parties who only share a number of entangled qubits to produce a secret key known only to them. In the next section we will introduce quantum games as a tool to prove that even if the source of these qubits is untrusted, we can use a classical test to prove that the protocol will function correctly.

An additional question that arises in a three party scenario is whether all parties trust each other. In Sec. III.3 we aim to ensure that the protocol is secure against dishonest parties by providing partial results showing that bipartite correlations can be used to finish the protocol without the corrupted party.

I.2. **Quantum Games and Non-locality.** Here we will motivate the concept of quantum games by introducing the following game:
Suppose Alice, Bob, and Carol are three quantum information researchers each imprisoned in a different isolated lab and they are only allowed to communicate with a Referee. Everyday they receive a message from the Referee containing a single letter, either X or Y, with the condition that only an even number of them will receive Y; i.e., either all receive X (XXX), or one of them receives

*Date*: September 26, 2014.

X and the other two receive Y (XYY, YXY, YYX). By the end of the day the researchers are required to respond to the message with either +1 or -1 and the Referee will extend their research funding if and only if the product of their responses is +1 in the case of XXX or -1 otherwise. As usual in game scenarios, the participants can devise a strategy before the beginning of the game but no communication is permitted once the game begins.

At the first glance it is easy to come up with a strategy for winning in 3/4 of the games, however, it can be proven that no classic strategy can guarantee winning. However, if we modify to game to give slightly more power to the players by allowing them to share entangled particles while still keeping them isolated, we can find a strategy that guarantees winning (see Appendix A). This strategy uses an entangled state known as the GHZ-state for Greenberger, Horne, and Zeilinger, who studied it first in 1989 [14].

This seemingly paradoxical result is due to the non-local nature of the correlations. In the quantum information literature these games are referred to as Bell's inequalities and the quantum strategies are known as violations of those inequalities

I.3. **What is considered secure?** The first step in designing a protocol is to identify the adversarial scenarios that we want to consider and make an explicit security definition.

Here we list the assumptions that we make regarding different parts of our protocol. We generally assume that **any untrusted component may have been altered or even manufactured by Eve, but once the protocol starts she can neither modify the components nor gain any information from them**. In quantum cryptography, Eve sometimes represents the effects of environment on the system (such as inexact qubits or measurements).

- **Untrusted States**: since it is impossible to find out what is the exact state of a qubit, we have to consider a situation where the source of our entangled qubits is untrusted. The fact that creating entangled qubits in a pure state is experimentally difficult makes considering this constraint useful.
- **Untrusted Measurements**: we cannot be certain about the internal measurement made by our devices. However, we know that the devices are sealed and Eve can neither modify the devices nor gain any information from them after the protocol starts.
- **Untrusted Participants**: in multiparty protocols often we want to ensure that the protocol will finish if a portion of participants are dishonest and the **untrusted parties learn nothing more than what they would learn normally** plus what they can compute locally.

  Here we consider the situation where only one of participants may lie in public announcements (e.g., when announcing the measurement that they performed or the outcome of it), but they do not reveal any information to Eve.

## II. Results

Although a device-independent tripartite protocol satisfying all of our requirements could not be found, in Appendix B we describe a key distribution protocol for three parties based on the GHZ state.

In addition, we will show that it is possible to have a state and measurement settings that violate a tripartite inequality such that the reduced density operator of that state also violates a bipartite inequality. That is equivalent to having non-locality in a tripartite and bipartite game using the same state. We propose the name **concurrent non-locality** to be used for this phenomenon.

The main state that we found to exhibit this quality is:

$$|W^-\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle - |100\rangle) \tag{1}$$

Note that the only distinction from the W-state is the minus sign of one of the terms.

This state can violate the inequality defined in Eq. 2. Using numerical methods the maximum violation of that inequality using this state is 7.2593 which can be achieved using measurement angles $\theta_0 = 0.2677\pi$ and $\theta_1 = \pi - \theta_0$. It is worth mentioning that this violation and measurement angles are the same for the normal W-state. Further, the reduced density operator of this state, shown in Eq. 3, can violate the $I_{3322}$ inequality [7]. We numerically found the maximum amount of this violation to be 0.0554 while the highest known violation of the $I_{3322}$ is 0.25 achieved using the maximally entangled state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

In the rest of the paper we will describe the methods and definitions used in this research.

## III. Building Blocks

In [4], Dür et al. showed that there are two nonequivalent classes of three-qubit entangled states that cannot be obtained from each other using invertible local transformations. In the introduction we presented the motivation for this project using a game based on the GHZ-state which represents one of the two equivalence classes. That state satisfied some, but not all, of our goals. In particular, the GHZ-states are maximally entangled but as we will justify in Sec. III.3, they are fragile with respect to losses. This can be inferred from the fact that the reduced density operator of any two parties is separable. As a result GHZ-states could not be used for two-party key distribution if one of the particles was lost due to environmental errors. Since all other entangled states of that class share that property, we shifted our focus onto the W-state which represents the second class that is less entangled but highly robust against losses.

In this work we will primarily discuss our results using the $|W^-\rangle$-state along with the methods that we used to look for best strategies. This state, which can be represented in the bra-ket notation as:

$$|W^-\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle - |100\rangle)$$

is interesting for us because if we trace out the second or third qubit, the reduced state will still exhibit non-locality. We will show the robustness of $|W^-\rangle$-state and fragileness of GHZ-state in Section (III.3).

III.1. **Bell Inequality.** In Sec. I.2 we claimed that a three party game can be used in building a protocol. Quantum games are in fact informal thought processes based on Bell's inequalities. The first step in using this state is looking for a Bell-type inequality that can be maximally violated by the $|W^-\rangle$-state. For now we will focus on inequalities that represent strategies with two measurements and binary outputs and are symmetric with respect to the parties; i.e., the measurement settings for all parties are the same. One such inequality found by Brunner et al. in Ref. [8] can be written as:

$$\begin{aligned} \langle\beta\rangle = &\langle A_0B_0C_0\rangle + \langle A_1B_0C_0\rangle + \langle A_0B_1C_0\rangle + \langle A_0B_0C_1\rangle \\ &-(\langle A_1B_1C_1\rangle + \langle A_0B_1C_1\rangle + \langle A_1B_0C_1\rangle + \langle A_1B_1C_0\rangle) \\ &+\langle A_0B_1I_C\rangle + \langle A_1B_0I_C\rangle + \langle A_0I_BC_1\rangle + \langle A_1I_BC_0\rangle + \langle I_AB_0C_1\rangle + \langle I_AB_1C_0\rangle \leq 6 \end{aligned} \tag{2}$$

where we used the shorthand:

$$\langle A_0B_0C_0\rangle = \langle\psi|A_0 \otimes B_0 \otimes C_0|\psi\rangle,$$

in which $\langle A_iB_jC_k\rangle \in [-1, 1]$ for $i, j, k \in \{0, 1\}$ denotes outcome of parties $A$, $B$, and $C$ measuring their qubits in $i$-th, $j$-th, and $k$-th measurement setting respectively, and $I_A$, $I_B$, and $I_C$ denote measuring using the identity operator. This inequality is created by adding some two-party correlation terms to the Svetlichny's inequality [6]. It can be proven that this inequality cannot be violated by the GHZ-state [8].

III.2. **The Strategy.** A strategy for a quantum game consists of the quantum state along with the measurement settings that can violate the inequality. For this game Brunner et al. gave the optimal measurements to be of the form:

$$A_i = \cos\theta_i Z + \sin\theta_i X$$

where $X$ and $Z$ are Pauli matrices. The optimal violation of the inequality above using the $|W^-\rangle$-state is $\langle\beta\rangle \approx 7.2593$ given by identical measurements with angles $\theta_0 = 0.2677\pi$ and $\theta_1 = \pi - \theta_0$ for all parties. However, the maximal violation has been numerically found to be achieved by a slightly modified state $|\psi\rangle = 0.9971|W\rangle - 0.07597|111\rangle$ with measurement angles of $\theta_0 = 0.2615\pi$ and $\theta_1 = \pi - \theta_0$.

The next step in the 3-party setting is to find measurements such that all parties have the same outcome with the highest probability possible. The purpose of this step is to provide a shared bit from which we can distill a key. Unfortunately, however, we could not find such a measurement on xz-plane of the Block sphere for the $|W^-\rangle$ state. Once a satisfying measurement is found, the next step is to apply key distillation processes such as information reconciliation to find a secure string that can be used as a key. An example of such a protocol is described in Section (6.3) of Ref. ([13]).

III.3. **Bipartite Correlations.** The next step before devising a protocol is finding bipartite correlations of $|W^-\rangle$-state that can be used to create a key if information about a single qubit is lost. The effects of such an event can be represented by tracing out a qubit from the density operator. The resulting reduced density operator is:

$$\rho_{AB} = Tr_C(|W^-\rangle\langle W^-|) = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{3}$$

We can use the Positive Partial Transpose (PPT) criterion to check that this reduced density operator is entangled. To do so, we have to show that the partial transpose of this operator has negative eigenvalues. The partial transpose of $\rho_{AB}$ is:

$$\rho_{AB}^{T_B} = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

which in fact has eigenvalues $\{\frac{1}{2} + \frac{\sqrt{5}}{2}, 1, 1, \frac{1}{2} - \frac{\sqrt{5}}{2} \approx -0.62\}$, thus $\rho_{AB}$ is entangled.

As a side note, we can see that tracing out one qubit from a GHZ-state will result in the following reduced density operator:

$$\begin{aligned} Tr_C(|GHZ\rangle\langle GHZ|) =& \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ =& \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \\ =& \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \end{aligned}$$

which is only classically correlated since the state is completely separable.

By this point we have shown that the reduced density operator of the $|W^-\rangle$-state is entangled. However, entanglement is only a necessary condition for non-locality. In order for this state to be useful in our protocol we need an inequality that can be violated by it. Note that this state will not maximally violate any inequality. To prove that, first we have to look at the eigendecomposition of $\rho_{AB}$:

$$\begin{aligned}\rho_{AB} &= \sum \lambda_i |v_i\rangle\langle v_i| \\ &= \frac{2}{3}|\Psi^-\rangle\langle\Psi^-| + \frac{1}{3}|00\rangle\langle 00|\end{aligned} \tag{4}$$

where $\lambda_i$ and $v_i$ are the eigenvalues and eigenvectors of $\rho_{AB}$, and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. This is equivalent to having the Bell state $|\Psi^-\rangle$ with probability $\frac{2}{3}$ and the classical state $|00\rangle$ with probability $\frac{1}{3}$. Assume we have an inequality $\langle B\rangle \leq X$ that can be maximally violated by $\rho_{AB}$:

$$\begin{aligned}\langle B\rangle &= \sum Tr(\rho_{AB}B) \\ &= \sum \lambda_i Tr(|v_i\rangle\langle v_i|B) \\ &= \frac{2}{3}Tr(|\Psi^-\rangle\langle\Psi^-|B) + \frac{1}{3}Tr(|00\rangle\langle 00|B) \leq X + \varepsilon_0\end{aligned}$$

Then each component $|v_i\rangle\langle v_i|$ must violate the inequality equally on their own, because otherwise there exists $j$ such that for all $i$ we have:

$$Tr(|v_i\rangle\langle v_i|B) < Tr(|v_j\rangle\langle v_j|B)$$

Thus:

$$\langle B\rangle = \sum \lambda_i Tr(|v_i\rangle\langle v_i|B) \leq \sum \lambda_i Tr(|v_j\rangle\langle v_j|B) \leq X + \varepsilon_0 + \varepsilon_1$$

However, that would contradict our initial assumption, so all components violate the inequality equally. But in the case of $\rho_{AB}$ one of the components is $|00\rangle\langle 00|$ which is not an entangled density operator, thus our assumption is wrong and $\rho_{AB}$ cannot produce a maximal violation.

III.4. **Security from No-signaling Conditions.** The fact that a reduced correlation can never achieve maximal violation does not mean that it cannot lead to a key. Intuitively the reason behind this statement is that even with smaller amounts of violation we can have a protocol that only has a lower rate of producing key bits. In our security proof we will use the fact that the devices are under no-signaling constraints to show that if Eve, an adversary, has a way of guessing the key bit with a probability higher than a bound, then the no-signaling condition is broken, thus Eve's guessing ability is limited by that bound.

The No-Signaling Assumption states that the choice of observable for one system cannot modify the marginal distribution for the rest of the systems; that is, the probability of each outcome for any measurement on Bob's qubit must be independent of Alice's choice of measurement because otherwise Alice would be able to convey messages to Bob faster than the speed of light. This method has been described in details in [10] and [11].

Denote $P_e$ as the probability that Eve can guess Alice's outcome without violating the no-signaling condition. For the inequality 2 we generated the following table using linear programming techniques to show what is the upper bound on $P_e$ if we can violate the inequality with probability $P_w$:

| $P_w$ | 0.75 | 0.76 | 0.77 | 0.78 | 0.79 | 0.80 | 0.81 | 0.82 | 0.83 | 0.84 | 0.85 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $P_e$ | 1.00 | 0.98 | 0.96 | 0.94 | 0.92 | 0.90 | 0.88 | 0.86 | 0.84 | 0.82 | 0.80 |

For instance in the first column there is no violation of classical inequality $P_w \leq 0.75$, so Eve has at least one strategy for guessing Alice's output deterministically ($P_e = 1$). As the non-locality increases, Eve's guessing ability reduces. However, even with the maximum violation, Eve can have a non-trivial way of guessing they key bit with a relatively high probability (note that such a method is not necessarily limited by quantum mechanics, but it is limited by the no-signaling assumption). In other words, the key string produced by the protocol until this step is only partially secret.

The last step required in the protocol is privacy amplification. The purpose of this step, as described in Section (5) of Ref. ([13]), is to distill a secret key from only partially secret data to get a completely secure key.

## IV. Methods

In this section we describe the optimization methods that we used to approximate the best strategy (state and measurements) for a Bell inequality. We categorize the inequalities based on three parameters $(n, m, \Delta)$ where the number of parties is $n$, number of measurement settings for each party is $m$, and number of possible outcomes for each measurement is $\Delta$. As mentioned before, for now we focus only on the cases where the measurements have two possible outcomes; i.e., $\Delta = 2$.

Using the fact that the Pauli matrices $X$, $Y$, and $Z$ together with the $2 \times 2$ identity matrix $I$ form an orthogonal basis for the real Hilbert space of $2 \times 2$ complex Hermitian matrices, we can parametrize our measurement operators in the form:

$$M_j = c_I I + c_X X + c_Y Y + c_Z Z \tag{5}$$

where $M_j$ is the $j$-th measurement setting and $c_j$ are real coefficients with $c_i^2 + c_x^2 + c_y^2 + c_z^2 = 1$. This decomposition is also known as the Hilbert-Schmidt decomposition. Additionally, in Ref. [8] Brunner et al. claim that the optimal measurement settings for our inequality can always be taken to be real and we can simplify the parametrization to:

$$M_j = \cos\theta_j Z + \sin\theta_j X \tag{6}$$

where $\theta_j$ is an angle from 0 to $\pi$.

IV.1. **Strategy for Tripartite Inequality (3,2,2).** Given an inequality for three parties we need to find the state $|\psi\rangle$ and measurement settings that maximally violate it. Our task is to maximize $\langle\psi|\beta|\psi\rangle$ where $\beta$ is the Bell inequality in Eq. (2) if we substitute the measurement operators with operators in the form of Eq. (6).

If we let $\mathcal{M}$ be a measurement operator, we know that it has an eigendecomposition of the form:

$$\mathcal{M} = \sum_i \lambda_i |v_i\rangle\langle v_i| \tag{7}$$

where $\lambda_i$ are the eigenvalues and $v_i$ are the respective eigenvectors (i.e., $\mathcal{M}v_i = \lambda_i v_i$). We have:

$$\begin{aligned} \langle\psi|\mathcal{M}|\psi\rangle &= \sum_i \lambda_i \langle\psi|v_i\rangle\langle v_i|\psi\rangle \\ &= \sum_i \lambda_i |\langle v_i|\psi\rangle|^2 \end{aligned} \tag{8}$$

Thus, our optimization problem is:

$$\begin{aligned} \text{given} \quad & \mathcal{M} = \sum \lambda_i |v_i\rangle\langle v_i| \\ \text{maximize} \quad & |\langle v_i|\psi\rangle|^2 \\ \text{subject to} \quad & |\langle\psi|\psi\rangle|^2 = 1 \end{aligned} \tag{9}$$

Hence, since the dot product of two vectors is maximum when the angle between them is zero, the optimal strategy would be to set our state equal to the eigenvector with the largest eigenvalue. That is:

$$|\psi\rangle = |v_{\underset{i}{argmax}\{\lambda_i\}}\rangle \tag{10}$$

Note that we need to check this for all possible measurement settings. As mentioned before, each measurement can be described in the form of Eq. (6), so we need to run a loop for the angle of each of the six measurements. As a result the computational complexity of this program would be in the order of $\mathcal{O}(n^6)$ where $n$ is the number of angles we check for each measurement. However, we can optimize our algorithm by only considering the difference between the angles of measurements. Intuitively this is justified by considering that we can choose an arbitrary basis for our system. Using that fact we can fix $A_0$, $B_0$, and $C_0$ and run the loop only on the second measurement of each party. This will reduce the complexity to $\mathcal{O}(n^3)$.

IV.2. **Strategy for Bipartite Inequality (2,m,2).** Once we have a state $|\psi\rangle$ that satisfies the previous condition, we need to find an inequality and strategy that uses the reduced density operator $\rho_{AB} = Tr_C(|\psi\rangle\langle\psi|)$.

For simplicity we started by looking at inequalities with $m = 2$. However, in Ref. [9] Brunner et al. show that the CHSH inequality [12] is the only tight Bell inequality for the (2,2,2) case, which means that if there is a strategy that violates a different inequality, then it will also violate the CHSH inequality. Using the same shorthand used in Eq. (2), we can write the CHSH inequality as:

$$\langle CHSH\rangle = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2 \tag{11}$$

Similar to the previous section we need to use run loops on the measurement angles, however, we can first group the measurements in the following manner:

$$\langle CHSH\rangle = \langle B_0(A_0 + A_1)\rangle + \langle B_1(A_0 - A_1)\rangle \leq 2 \tag{12}$$

Now if we run two loops for $A_0$ and $A_1$, our problem would reduce to maximizing:

$$\begin{aligned}\langle CHSH\rangle &= Tr_{AB}(B_0 \otimes (A_0 + A_1)\cdot\rho_{AB}) + Tr_{AB}(B_1 \otimes (A_0 - A_1)\cdot\rho_{AB}) = \\ &= \sum_{i=\{0,1\}} Tr_{AB}(B_i \otimes X_i \cdot \rho_{AB})\end{aligned} \tag{13}$$

where $X_0 = A_0 + A_1$ and $X_1 = A_0 - A_1$ are known. Next, we can use partial trace to trace out qubit $A$:

$$\begin{aligned}\sum_{i=\{0,1\}} Tr_{AB}(B_i \otimes X_i \cdot \rho_{AB}) &= \sum_{i=\{0,1\}} Tr_B(B_i \cdot Tr_A(X_i \otimes I_B \cdot \rho_{AB})) \\ &= \sum_{i=\{0,1\}} Tr_B(B_i \cdot Z_i)\end{aligned} \tag{14}$$

where $Z_i = Tr_A(X_i \otimes I_B\rho_{AB})$ are known. At this point, we can use Hilbert-Schmidt decomposition to rewrite the $2\times 2$ matrices $B_i$ and $Z_i$ as:

$$\begin{aligned}B_i &= b_I I + b_X X + b_Y Y + b_Z Z \\ Z_i &= z_I I + z_X X + z_Y Y + z_Z Z\end{aligned} \tag{15}$$

where $b_j$ and $z_j$ are real coefficients with $\sum_j b_j^2 = \sum_j z_j^2 = 1$. Using this decomposition, we can rewrite the traces as:

$$\sum_{i=\{0,1\}} Tr_B(B_i \cdot Z_i) = \sum_{i=\{0,1\}} \bar{b}\cdot\bar{z} \tag{16}$$

Thus, we can rephrase the optimization problem:

$$\begin{aligned}\text{given} \quad & \mathcal{M} = \sum \lambda_i |v_i\rangle\langle v_i| \\ \text{maximize} \quad & |\langle v_i|\psi\rangle|^2 \\ \text{subject to} \quad & |\langle\psi|\psi\rangle|^2 = 1\end{aligned} \tag{17}$$

is again reduced to maximizing a bounded dot product which means the optimal value is achieved when:

$$\bar{b} = \bar{z}$$

so:

$$\begin{aligned} B_0 &= Tr_A((A_0 + A_1) \otimes I_B \rho_{AB}) \\ B_1 &= Tr_A((A_0 - A_1) \otimes I_B \rho_{AB}) \end{aligned} \tag{18}$$

However, we found out that the reduced density operator that we found in Sec. (1.3) does not violate the CHSH inequality. Thus, we needed to look into (2,3,2) inequalities.

IV.3. **The $I_{3322}$ Inequality.** The $I_{3322}$ inequality, studied in [7], is an inequality consisting of three possible 2-outcome measurements on two particles and can be written as:

$$\begin{aligned} \langle I_{3322} \rangle = &\langle A_0 B_0 \rangle + \langle A_1 B_0 \rangle + \langle A_2 B_0 \rangle - 2\langle I_A B_0 \rangle \\ &+\langle A_0 B_1 \rangle + \langle A_1 B_1 \rangle - \langle A_2 B_1 \rangle - \langle I_A B_1 \rangle \\ &+\langle A_0 B_2 \rangle - \langle A_1 B_2 \rangle \\ &-\langle A_0 I_B \rangle \leq 0 \end{aligned} \tag{19}$$

where $\langle A_i B_j \rangle \in [-1, 1]$ for $i, j \in \{0, 1, 2\}$ denotes outcome of parties $A$ and $B$ measuring their qubits in $i$-th and $j$-th measurement setting respectively, and $I_A$ and $I_B$ denote measuring using the identity operator. Using the numerical approximation similar to the methods above we can show that maximum value of this inequality using a pair of qubits (two dimensional system) is 0.25 achieved using the state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. The measurements for the maximum violation all lie on the zx-plane in the Bloch sphere: $A_0 = 0$, $A_1 = \frac{\pi}{3}$, $A_2 = \frac{2\pi}{3}$, $B_0 = \frac{4\pi}{3}$, $B_1 = \pi$, and $B_2 = \frac{2\pi}{3}$.

We are interested in this inequality because it can be violated by states that do not violate the CHSH inequality. In particular, using the methods described above we found measurement settings that violate this inequality using our reduced density operator in Eq.3. The highest value of violation was found to be 0.0554 using measurements in the form of Eq. 6.

IV.4. **Discussion and Future Directions.** The main focus in the continuation of this project will be on working out a complete protocol using the aforementioned $|W^-\rangle$ state. Specifically, a search for a better measurement for getting a key bit using a more general form of measurement will be useful.

Further, an investigation regarding a generalization of concurrent non-locality seems to be an interesting direction for future research. Is there a non-local state such that any reduction would lead to another, perhaps weaker, non-local state? In particular, the prospect of a multipartite quantum key distribution protocol that allows any subset to generate a separate key is a very fascinating question for the author.

IV.5. **Acknowledgments.** This work was made possible by a Summer Undergraduate Research Fellowship from California Institute of Technology in Pasadena, California. I would like to thank Professor Thomas Vidick, my mentor, who generously spent time to help me through the simplest obstacles in our weekly meetings and changed my perspective on academia; Fernando Granha, Matthew Coudron, and Rotem Arnon Friedman for the incredibly useful conversations that we had; Spiros Michalakis and John Preskill for their invaluable comments during weekly group meetings; and many others who helped me through different stages of this project.

## Appendix A. GHZ Inequality

A.1. **The Game.** Suppose Alice, Bob, and Carol are three quantum information researchers each imprisoned in a different isolated lab and they are allowed to communicate only with a Referee. Everyday the Referee sends each one of them an email containing a single letter, either X or Y, with the condition that only an even number of them will receive Y; i.e., either all receive X (XXX), or one of them receives X and the other two receive Y (XYY, YXY, YYX). By the end of the day the researchers are required to respond to the email with either +1 or -1 and the Referee will extend their research funding if and only if the product of their replies is +1 in the case of XXX or -1 otherwise. As it is usual in these games, the participants can devise a strategy before the beginning of the game but once it begins no communication is permitted.

A.2. **The Problem.** In the first glance it is easy to come up with a strategy that guarantees winning in 3/4 of the games, but is there a strategy that guarantees winning all the time?

Let $A_X$ denote Alice's response if she received an X and $A_Y$ denote her response if she received a Y and so on for $B_X$, $B_Y$, etc. Then, we can formulate the requirements for winning the game:

$$\begin{aligned} A_X B_X C_X &= +1 \\ A_X B_Y C_Y &= -1 \\ A_Y B_X C_Y &= -1 \\ A_Y B_Y C_X &= -1 \end{aligned}$$

But here we have a contradiction because the product of the left sides is a perfect square and the outputs are all real: $A_X^2 A_Y^2 B_X^2 B_Y^2 C_X^2 C_Y^2 = -1$

There could be other classic strategies with probabilistic outputs. The proof of impossibility of those are very similar to this case and can be found in Ref. [15].

A.3. **The Solution.** Now that the researchers are confident that classical strategies are not helpful in saving their funding, the trio decide to put their quantum information research to use. They begin by creating three entangled particles in the following state:

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

This entangled state is known as the GHZ-state for Greenberger, Horne, and Zeilinger, who studied it first in 1989 [14]. After taking one part of the state each, they go to their labs and measure their qubits according to the letter in the Referee's email: if the email contains X, the receiver measures their share in the basis of the eigenstates of the Pauli X operator:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{and} \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and outputs +1 if the outcome of the measurement is $|+\rangle$ or -1 for $|-\rangle$. Similarly if the email contains Y, the receiver measures their share in the basis of the eigenstates of the Pauli Y operator:

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \qquad \text{and} \qquad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

and outputs +1 if the outcome of the measurement is $|+i\rangle$ or -1 for $|-i\rangle$.

Using this system, the probability of an odd number of researchers observing $|-\rangle$ if the Referee sent X to everyone (i.e., they all measured in $|+\rangle$ and $|-\rangle$ basis) will be zero [1], so in the case of XXX, always an even number of measurements result in -1 and the final product will be +1.

[1] For instance: $|(\langle -| \otimes \langle +| \otimes \langle +|)|\gamma\rangle| = 0$

For the other three cases the probability of an even number of researchers observing $|-\rangle$ or $|-i\rangle$ will be zero [2], so always an odd number of measurements result in -1 and the final product will be -1.

Thus, using this quantum strategy, the researchers can guarantee perpetual funding.

## Appendix B. A GHZ-based Tripartite QKD Protocol

Here we describe a protocol based on the GHZ game in the honest majority:

### Tripartite QKD Using GHZ-State

Assumptions: Three honest parties $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ have prepared $N$ entangled GHZ states and each have access to one of the qubits in their own spatially isolated laboratories. Further, we assume that parties have access to an authenticated channel.

(1) Each party begins making random measurements using Pauli operators $X$, $Y$, and $Z$ with probabilities $P_x$, $P_y$, and $P_z$; for instance, if $P_x = P_y = P_z = \frac{1}{3}$ then each party randomly chooses $\frac{N}{3}$ qubits and performs a measurements in the $Z$ basis $(\{|0\rangle, |1\rangle\})$ and similarly for $X$ and $Y$ basis. Denote $A_i^Z$ as the outcome of a measurement in $Z$ basis on the $i$-th qubit of party $\mathcal{A}$.

(2) Each party publishes an ordered list of the basis of each performed measurement.

(3) For each GHZ state, if the measurement on all qubits has been in $X$ basis, or if one qubit has been measured in the $X$ basis and the other two have been measured in the $Y$ basis, the parties publish the measurement outcomes over the authenticated channel; for instance, if all measurements on the $i$-th state have been in $X$ basis, $\mathcal{A}$ publishes $A_i^X$, $\mathcal{B}$ publishes $B_i^X$, and $\mathcal{C}$ publishes $C_i^X$.

(4) The parties calculate the product of the outcomes for each GHZ state in the published list. That is, for the previous example, they calculate $O_i^{XXX} = A_i^X B_i^X C_i^X$. Next, they calculate the average of all $O_i^{XXX}$, $O_i^{XYY}$, $O_i^{YXY}$, and $O_i^{YYX}$ and find their sum: $S = \sum_{i=0}^{N} O_i^{XXX} + O_i^{XYY} + O_i^{YXY} + O_i^{YYX}$.
The value of $\varepsilon = 1 - S$ describes the trustworthiness of the measurement devices.

(5) Finally, for each GHZ state that was measured using the $Z$ basis by all parties, the parties use the outcome as a key bit. This bit will be the same for all parties because the probability of measuring anything other than $|000\rangle$ and $|111\rangle$ is zero while the probability of measuring those two states is equal:
$|\langle 000|GHZ\rangle|^2 = |\langle 111|GHZ\rangle|^2 = \frac{1}{2}$

Note that we have not provided a proof for the security of this protocol and it is not robust against loss of a qubit.

## Appendix C. Source codes

All computer programs used in this research have been written using Sage and Matlab and the scripts can be found at the following address:
`http://www.its.caltech.edu/~msayrafi/surf-2014/codes`

[2] For instance: $|(\langle -i| \otimes \langle +i| \otimes \langle -|)|\gamma\rangle| = 0$

## References

[1] Artur K. Ekert; "Quantum cryptography based on Bell's theorem" Physical Review Letters, Vol. 67, No. 6, American Physical Society, August 1991, pp. 661-663 `doi:10.1103/PhysRevLett.67.661`

[2] Jonathan Barrett, Lucien Hardy, and Adrian Kent; "Quantum cryptography based on Bell's theorem" Physical Review Letters, Vol. 67, American Physical Society, June 27 2005 `arXiv:quant-ph/0405101`

[3] Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani; "Device-independent security of quantum cryptography against collective attacks" Physical Review Letters, Vol. 98, 230501, American Physical Society, June 25 2007 `arXiv:quant-ph/0702152`

[4] W. Dür, G. Vidal, and J. I. Cirac; "Three qubits can be entangled in two inequivalent ways" Physics Review, A 62, 062314 (2000) `arXiv:quant-ph/0005115`

[5] W. Dür; "Entanglement molecules" `arXiv:quant-ph/0006105`

[6] G. Svetlichny; "Distinguishing three-body from two-body nonseparability by a Bell-type inequality" `Phys. Rev. D 35. 3066 (1987)`

[7] D. Collins, N. Gisin; "A Relevant Two Qubit Bell Inequality Inequivalent to the CHSH Inequality" `arXiv:quant-ph/0306129`

[8] N. Brunner, J. Sharam, T. Vertesi; "Testing the Structure of Multipartite Entanglement with Bell Inequalities" `arXiv:1110.5512 [quant-ph]`

[9] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner; "Bell nonlocality" `arXiv:1303.2849 [quant-ph]`

[10] Umesh V. Vazirani, Thomas Vidick; "Certifiable Quantum Dice - Or, testable exponential randomness expansion" `arXiv:1111.6054 [quant-ph]`

[11] Ll. Masanes, R. Renner, M. Christandl, A. Winter, J. Barrett; "Full security of quantum key distribution from no-signaling constraints" `arXiv:quant-ph/0606049`

[12] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt; "Proposed Experiment to Test Local Hidden-Variable Theories" Physical Review Letters, Vol. 23, No. 15, American Physical Society, October 1969, pp. 880-884 `doi:10.1103/PhysRevLett.23.880`

[13] Renato Renner; "Security of Quantum Key Distribution" `arXiv:quant-ph/0512258`

[14] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger; "Going Beyond Bell's Theorem" in: 'Bell's Theorem, Quantum Theory, and Conceptions of the Universe', M. Kafatos (Ed.), Kluwer, Dordrecht, 69-72 (1989) `arXiv:0712.0921 [quant-ph]`

[15] Dave Bacon; CSE 599d lecture notes, Quantum Entanglement and Bell's Theorem.