Tripartite Quantum Key Distribution From Three-Player Nonlocal Games

Mahrud Sayrafi — Mentor: Thomas Vidick
mahrud@berkeley.edu — vidick@cms.caltech.edu
Department of Mathematics, University of California, Berkeley — Institute for Quantum Information and Matter, Caltech

Motivation and Background

Quantum Cryptography is the only approach to privacy ever proposed that has fulfilled the dream of two parties without a pre-shared key to communicate with provably perfect secrecy under the nose of an eavesdropper equipped with unlimited computational power whose technology is only limited by the fundamental laws of nature.

Although the no-cloning and no-signaling theorems of quantum mechanics rule out the trivial applications of entanglement, what makes entangled states particularly interesting for cryptographers and theoretical physicist alike are **"games" in which having a quantum advantage gives us an edge over classical players.**

- [Clauser et al. '69] provide a test to local hidden-variable theories using CHSH game.
- [Ekert '91] constructed a QKD protocol using entanglemed Bell states.
- [Berrett et al. '05] proved security against an eavesdropper with post-quantum physics and only limited by no-signaling theorem.
- [Acin et al. '07] prove device-independent security, meaning that it holds true regardless of the way QKD devices work, provided that quantum physics is correct and parties are isolated.

The primary objective of this research is to compose a protocol that enables three parties who only share a number of entangled qubits to produce a secret key known only to them, even if one party decides to lie in the process. We aim to use quantum games to prove that even if the source of these qubits is untrusted, as long as they can be used in a game such as the one above, the protocol will function correctly.

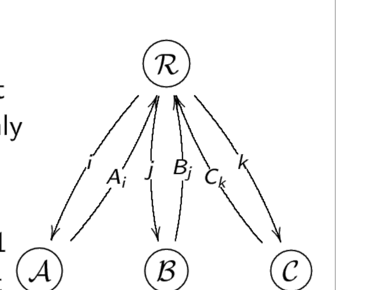
Nonlocal Games and Bell Inequalities

Best classical strategy for this game wins in 75% of all games , however , it can be proven that no classic strategy can guarantee winning.

A quantum strategy gives slightly more power to each of the players by allowing them to share entangled particles while still keeping them isolated, we can find a strategy using an entangled GHZ-state, that guarantees winning in every game. This seemingly paradoxical result is due to the non-local nature of the correlations.

The GHZ Game

1. Three isolated players $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$
2. Referee $\mathcal{R}$ sends each player an input in $\{X, Y\}$ with the condition that only an even number receive Y. i.e., $\{XXX, XYY, YXY, YYX\}$
3. Players respond with either $+1$ or -1
4. Players win if and only if the product of their outputs is:
   - $+1$ if the input was XXX.
   - -1 otherwise.



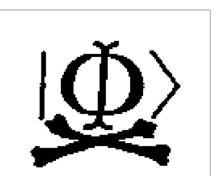
A nonlocal game consists of three parts; for instance in GHZ game we have:

1) A **Bell inequality**: $$\langle\beta\rangle = \langle A_x B_x C_x\rangle - \langle A_y B_x C_x\rangle - \langle A_x B_y C_x\rangle - \langle A_x B_x C_y\rangle \le 3$$

2) An **entangled state**:
Here we use the maximally entangled GHZ state: $$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

3) A **measurement strategy**:
- If received X, measure in the basis: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- If received Y, measure in the basis: $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

What is considered secure?



The first step in designing a security protocol is to identify the adversarial scenarios that we want to consider and make an explicit security definition.

In general we assume that:
Any untrusted component may have been altered or even manufactured by Eve.
After protocol starts she cannot modify the components or gain any information.
Eve can represent the effects of environment on the system (such as inexact qubits or measurements).

- **Untrusted States**:
  The source of entangled qubits is untrusted.
  => Creating entangled qubits in a pure state is difficult in experimental.
- **Untrusted Measurements**:
  The devices are sealed once the protocol starts.
  => We are unaware of the measurements bases.
  => Eve cannot modify the devices or steal any information.
- **Untrusted Participants**:
  Want to ensure that:
  (a) The protocol will finish if some participants are dishonest.
  (b) The untrusted parties learn nothing more than what they would learn normally or what they can compute locally.

We consider the situation where:
(a) only one participant (out of three) may lie in public announcements (e.g., when announcing the measurement that they performed or the outcome of it)
(b)They do not reveal any information to Eve.

Concurrent Nonlocality

Old concept:
- **Non-local state**:
  - An entangled state that can **violate a Bell inequality**.
  - I.e., we need a nonlocal game.

New concept:
- **Concurrently Nonlocal state**:
  - An entangled state that can **violate two <u>inequivalent</u> Bell inequalities.**
  - E.g., a tripartite inequality and a bipartite inequality.

1. The inequality:
$$\begin{aligned}\langle\beta\rangle &= \langle A_0B_0C_0\rangle + \langle A_1B_0C_0\rangle + \langle A_0B_1C_0\rangle + \langle A_0B_0C_1\rangle \\ &\quad -(\langle A_1B_1C_1\rangle + \langle A_0B_1C_1\rangle + \langle A_1B_0C_1\rangle + \langle A_1B_1C_0\rangle) \\ &\quad +\langle A_0B_1I_C\rangle + \langle A_1B_0I_C\rangle + \langle A_0I_BC_1\rangle + \langle A_1I_BC_0\rangle + \langle I_AB_0C_1\rangle + \langle I_AB_1C_0\rangle \le 6\end{aligned}$$
Here, $\langle A_iB_jC_k\rangle \in [-1,1]$ 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.
This inequality is created by adding some two-party correlation terms to the Svetlichny's inequality.
It can be proven that this inequality cannot be violated by the GHZ-state

2. The state:
$$|W^-\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle - |100\rangle)$$
Note that this state is different from $|W\rangle$ state only by a minus sign.

3. Measurement strategies:
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.
For this state, optimal measurement is given by angles:
$$\theta_0 = 0.2677\pi \quad \text{and} \quad \theta_1 = \pi - \theta_0$$
And maximal violation is:
$$\langle\beta\rangle \approx 7.2593$$

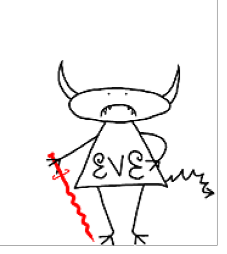
Next, the reduced density matrix of this state is:
$$\rho_{AB} = Tr_C(|W^-\rangle\langle W^-|) = \frac{1}{3}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Now to show that $|W^-\rangle$ is concurrently nonlocal, we show that reduced density matrix is :
a) Entangled:
We can show using the PPT criterion that this density matrix is entangled.
b) Nonlocal:
i. We need bipartite inequality:
$$\begin{aligned}\langle I_{3322}\rangle &= \langle A_0B_0\rangle + \langle A_1B_0\rangle + \langle A_2B_0\rangle - 2\langle I_AB_0\rangle \\ &\quad +\langle A_0B_1\rangle + \langle A_1B_1\rangle - \langle A_2B_1\rangle - \langle I_AB_1\rangle \\ &\quad +\langle A_0B_2\rangle - \langle A_1B_2\rangle \\ &\quad -\langle A_0I_B\rangle \le 0\end{aligned}$$
Here, $\langle A_iB_j\rangle \in [-1,1]$ 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. Note that here each party has **three** different measurement choices.

This inequality can be violated by states that do not violate the CHSH inequality.

By numerical approximation we know that maximum value of this inequality using a pair of qubits (two dimensional system) is:
$$\langle I_{3322}\rangle \le 0.25$$
achieved using the state: $$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
Also note that the spectral decomposition of our reduced density matrix gives:
$$\rho_{AB} = \sum \lambda_i |v_i\rangle\langle v_i| = \frac{2}{3}|\Psi^-\rangle\langle\Psi^-| + \frac{1}{3}|00\rangle\langle 00|$$
which is similar to having the maximally entangled state with probability 66% and a classical bit otherwise.
ii. We need a measurement strategy:
By similar numerical approximations the maximum values of this inequality using our reduced state is:
$$\langle I_{3322}\rangle \le 0.0554$$
Which is a violation, thus the reduced density matrix is nonlocal.

Thus the state $|W^-\rangle$ is concurrently nonlocal in three- and two-party correlations.



Quantum Key Distribution using Nonlocal Games

Although the security definitions seem impossible to satisfy, using nonlocal games can help significantly in achieving them.

Imagine three black boxes ...
- Inputs: $\{X, Y, Z\}^3$
- Outputs: $\{+1, -1\}^3$
- Each party has one of the boxes
- They play the game!
  - If they lose suspiciously often, something is wrong.
  - If they always win, they start to measure in the Z basis ($|0\rangle, |1\rangle$) which is guaranteed to return the same output for all of them.
- We have a Quantum Key Distribution protocol!

The powers of adversary are limited to what he can do when manufacturing this black box and all other communications are assumed to be authentic (i.e., Eve cannot modify the contents of public announcements).

Although a device-independent tripartite protocol satisfying all of our requirements could not be found, here we describe a protocol based on the GHZ game in the honest majority:

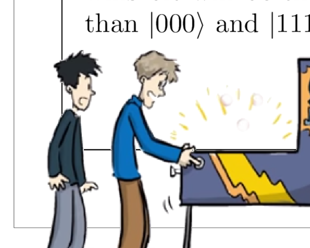
Tripartite QKD Using GHZ-State

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

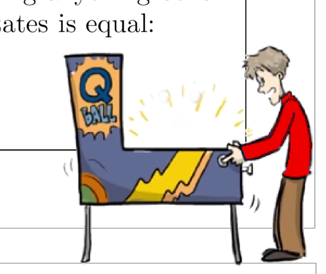
Protocol:
(1) Each party begins making random measurements using Pauli operators X, Y, and Z with probabilities P_x, P_y, and P_z.
Denote A_i^Z as the outcome of a measurement in Z basis on the i-th qubit of party $\mathcal{A}$.
(2) Each party publishes an ordered list of the basis of each performed measurement.
(3) For each GHZ state, the parties publish the measurement outcomes over the authenticated channel if:
- The measurement on all qubits has been in X basis.
- One qubit has been measured in the X basis and the other two have been measured in the Y basis.

(4) The parties calculate the product of the outcomes for each GHZ state in the published list. That is they calculate $O_i^{XXX} = A_i^X B_i^X C_i^X$ if all measurements have been performed in X basis.
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.

Key extraction:
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:



$$|\langle 000|GHZ\rangle|^2 = |\langle 111|GHZ\rangle|^2 = \frac{1}{2}$$

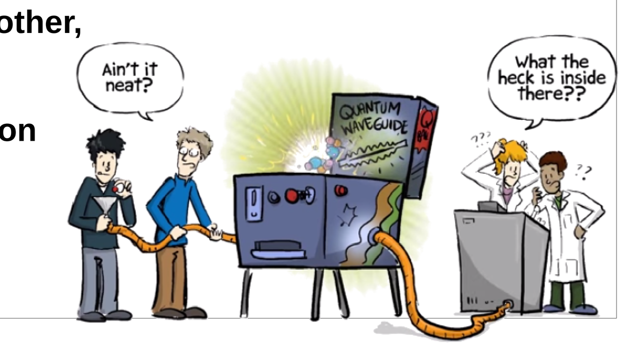


Conclusion:

We showed existence of a tripartite quantum state that, given the right set of measurement strategies, can maximally violate a tripartite Bell inequality and the reduced bipartite correlations violate a bipartite Bell inequality.

Future work:

- Finding an optimal key extraction strategy for the $|W^-\rangle$ state.
- Proving the device-independence limits for the protocol.
- Generalizing concurrent nonlocality and more examples; in particular:
  - **Is there a non-local state such that any nontrivial reduction would lead to another,**
  - **perhaps weaker, non-local state?**
- **Is a multipartite quantum key distribution protocol that allows any subset to generate a separate key possible?**



Notable References:
N. Brunner, et al.; "Bell nonlocality" **arXiv:quant-ph/1303.2849**
R. Renner; "Security of Quantum Key Distribution" **arXiv:quant-ph/0512258**
Ll. Masanes, R. Renner, et al.; "Full security of quantum key distribution from no-signaling constraints" **arXiv:quant-ph/0606049**
D. Collins, N. Gisin; "A Relevant Two Qubit Bell Inequality Inequivalent to the CHSH Inequality" **arXiv:quant-ph/0306129**

Acknowledgements:
This research was funded by a Summer Undergraduate Research Fellowship (SURF) from California Institute of Technology and carried out at Institute for Quantum Information and Matter (IQIM) in Pasadena, California. We also thank Professor Whaley and other members of Berkeley Quantum Information and Computation Center (BQIC) for their guidances.

All comics are from "Piled Higher and Deeper" by Jorge Cham at www.phdcomics.com.