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

First Progress Report
Mahrud Sayrafi

I. Introduction

We begin motivating this research by studying a simple game.

I.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.

I.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:

$$A_X B_X C_X = +1$$
$$A_X B_Y C_Y = -1$$
$$A_Y B_X C_Y = -1$$
$$A_Y B_Y C_X = -1$$

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. [2].

I.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 [1]. 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:

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

Date: July 6, 2014.

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.

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.

I.4. **The Aftermath.** The study of these quantum games and strategies has lead to interesting results in cryptography and other information theoretic fields. In this case, it is important to note that the labs were still isolated and no information was transferred. This seemingly paradoxical result is in fact due to the non-local nature of the correlations. In the quantum information literature these games are sometimes referred to as violations of Bell's inequalities because these quantum correlations cannot be explained by a local hidden variables theory.

The primary objective of this research is to compose a protocol that enables three parties – Alice, Bob, and Carol – who only share a number of entangled qubits to produce a secret key known only to them, assuming that they all remain honest. Further, we will 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. For instance, if we had an unknown tripartite quantum state, we can use the game introduced above as a classical test [3] in which if the game is lost, we will know that the qubits were not in the GHZ-state (but if we won the game we still need to prove that no other state can accomplish this before reaching any conclusions).

In the Sec. II.3 we will introduce a protocol that can be proved secure using the game above. In addition, we want to ensure that the protocol is secure against dishonest parties; that is, some members may intentionally lie in order to break the protocol or gain additional knowledge, and we want to have a plan for detecting such parties and, if possible, finishing the protocol without them. Such a protocol will also be useful in the practical sense because it will be resilient against the case where some particles are lost.

II. Results To Date

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

II.1. **The Ingredients.** 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.

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

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

[3] The test is classical because the only operation performed by us is measurement of qubits

A particular case is when Eve (an eavesdropper) has a secret entanglement with our qubits.

- **Untrusted Measurements**: we cannot be certain about which measurement was 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 a minority (less than half) 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. In the future we might also consider a dishonest majority.

II.2. **The Intuition.** : Although the restrictions listed above sound impossible to satisfy, using quantum games can help us significantly in achieving them. Imagine Alice, Bob, and Carol each have a sealed and isolated black box with a single button. Each box contains one particle of some 3-partite state that is entangled with the particles in the other two boxes and a program for performing a set of measurements and returning a classical bit each time the button is pressed. The idea in this research is that if the trio can use their boxes to participate in a quantum game and achieve satisfactory results, then they can use the same boxes to distribute a key among them. This intuition is helpful in thinking about our security definitions because 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).

II.3. **First Protocol.** The three quantum information researchers have acquired a sufficient amount of quantum entangled qubits and wish to distribute a key among themselves. The protocol consists of: (i) for each of the 3-partite qubit systems, Alice, Bob, and Carol each choose a random measurement basis between eigenstates of Pauli X, Y, or Z operators [4] and perform the measurement. (ii) they publish a table containing only their choice of measurement for each system. (iii) since the chance of choosing each basis is equal, in about 4/27 of the systems the participants measured in XXX or XYY or a permutation of the latter. Only, in those cases, they all publish the result of their outcomes. (this is equivalent to playing the game described in Sec. I.1) (iv) if the qubit systems were all in the GHZ-state, the product of the outcomes of each system must match the requirements of winning the game (this is equivalent to using the strategy described in Sec. I.3). If not, then abort the protocol. (v) now, each time all participants had used the Z basis, they use the outcome bit as one bit of the secret key. This bit is the same between all members because when measuring a GHZ-state in the Z basis, all outcomes have to be the same [5].

Weaknesses:

- This protocol can be disrupted if a qubit is disposed due to physical or environmental errors or observed early (see Ref. [4]).
- If the systems are correct but one party lies in announcements the protocol is disrupted. For instance if Alice flipped the outcome bit every time she measured using eigenstates of Pauli X operator, the game would fail half the times and the protocol would be aborted.
- This protocol is inefficient because only 1/27th of systems result in a key bit. However, we can change the probability of each measurement choice; for instance parties can measure 99% of the systems in the Z basis.

[4] the basis for X and Y where mentioned in Sec. I.3. The basis for Z is simply $|0\rangle$ and $|1\rangle$

[5] For instance: $|(\langle 0| \otimes \langle 0| \otimes \langle 0|)|\gamma\rangle| = 1/2$

III. Planning Ahead

More recently we have started looking at another 3-partite state referred to as the W-state [3]:

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

The main benefit of this state is that it is more resilient against disposal of a particle; in the GHZ-state if one particle is measured, the state of the remaining particles is only classically correlated and not entangled [4]. However, this state seems to be in some sense weaker than GHZ in quantum games.

In the following month my plan is to investigate whether or not there are useful strategies using the W-state in a quantum game [5] and whether it can be used in designing a protocol. This task involves reviewing the literature on non-local inequalities with three particles. Another method for this task would be simulating different strategies based on this state for different three party quantum games to see if there is a game in which this state violates Bell's inequalities maximally.

To recapitulate, my plan for the following month consists of:

- Algorithmic search for high-biased quantum games using the W-state
- Devising a tripartite key distribution protocol based on that game
- Formal proofs for the protocol and compiling the findings in a paper.

References

[1] 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]`

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

[3] W. Dur, 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`

[4] W. Dur "Entanglement molecules" `arXiv:quant-ph/0006105`

[5] Nicolas Brunner, James Sharam, Tamas Vertesi; "Testing the Structure of Multipartite Entanglement with Bell Inequalities" `arXiv:1110.5512 [quant-ph]`

[6] Alexander Streltsov, Gerardo Adesso, Marco Piani, and Dagmar Bruss; "Are general quantum correlations monogamous?" Physical Review Letter, Vol. 109, No. 5, American Physical Society, August 2012, pp. 050503 [5 pages] `arXiv:1112.3967 [quant-ph]`