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

Summer 2014 SURF Proposal in Quantum Information and Cryptography
Student: Mahrud Sayrafi Mentor: Dr. Thomas Vidick

I. Introduction 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. However, it is important to remember that there is more to quantum cryptography than quantum key distribution (QKD) and these ideas can potentially revolutionize every aspect of modern computing [1].

An important quantum phenomena that has been often used in cryptography contexts is entanglement. It turns out that in some cases it is impossible to infer the state of one qubit in a multi-qubit system using Dirac's notation; for instance, it is not possible to write $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, known as Einstein-Podolsky-Rosen (EPR) state, as a product of two individual qubits. Such multi-qubit systems are referred to as entangled systems or quantum correlations and are explained by the Entanglement principle of quantum mechanics.

Although the no-cloning and no-signaling theorems of quantum mechanics rule out the trivial applications of entanglement, what makes them particularly interesting for cryptographers are "games" in which having such a correlation gives us an edge over classical players. In 1969 Clauser, Horne, Shimony and Holt (CHSH) published [6] in which they proposed the well known CHSH game as a way to test local hidden-variable theories[1]. In this game Alice and Bob who share an entangled qubit pair in the EPR state (the entangled state above) can win with the probability of $\cos^2(\pi/8) \approx 85.4\%$, but the best classic strategy can win at most 75% of the time. It is crucial to note that according to Bell's theorem, this advantage is due to the non-local nature of these games and a local system, such as a shared random bit, cannot achieve the same probability [2].

In 1991 Ekert used quantum entanglement to construct a QKD protocol [12]. In 2005 Berrett et al. proved that this protocol is secure against an eavesdropper with post-quantum physics and only limited by the impossibility if signaling faster than the speed of light [4]. Even more surprising, in 2007 Acin et al. presented a device-independent security proof, meaning that it holds true 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.

II. Objectives

The primary goal of this research is to compose a fully device-independent tripartite quantum key distribution protocol. Such a protocol will enable three parties – Alice, Bob, and Carol – who don't have a pre-shared key but share an entanglement to produce a secret key known only to them.

Date: February 21, 2014.

[1]According to theory of relativity events in one point of space-time cannot affect spatially apart points at the same time, hence the name "locality"; i.e., if Alice observes her qubit, this qubit cannot affect Bob's qubit sooner than the time it takes for light to travel the distance between them. In non-local games, however, Alice and Bob measure their qubits at the same moment, hence the non-local nature of quantum entanglement.

Further, we will prove device-independent security for our protocol, meaning that regardless of what steps the quantum device is taking, as long as it is accepted by the protocol, the produced key is secure. Currently there are various device-independent bipartite QKD protocols in the literature, such as [13], and at least one tripartite QKD without device-independent security in [14]. We will analyze these protocols, among others, during the program.

A device-independent tripartite QKD protocol can be used in various three party cryptography protocols such as Secure Multiparty Computation (SMPC)[2]. Although it is possible to perform a bipartite QKD protocol multiple times to share pairwise keys between parties and then share a key with all three, such a protocol is not useful in certain cryptography settings such as multiparty computation with dishonest players or even semi-honest groups[3].

Additionally we hope to find an efficient measure for usefulness of non-local games, especially XOR games, for cryptography purposes. Such a method will take into account various parameters, in particular we are interested to know whether it is possible to ensure that the given qubits are in fact in the state required by the protocol. This property is stronger than device-independence and is referred to as the rigidity of a quantum game [10]. Another factor is the number of qubits in the system. While it is possible to correlate any number of qubits in a state, the monogamy of entanglement puts strong constraints on the spatial separation of the system [9].

III. Approach

Ideally, in the next few months and before the beginning of the SURF program I will gain a high understanding of Bell's theorem and proofs of device independent security. I will achieve that by an extensive review of the literature involving bipartite quantum key distribution systems such as [11] and [12].

The major milestones in the duration of the program are:

- Finding useful tripartite quantum states and games: The first portion of the project consists of building an understanding of two- and three-qubit correlation and more importantly the quantum games that show a high bias[4] on those states. Two famous entangled states involving more than two qubits are the Greenberger-Horne-Zeilinger (GHZ) state studied in [7] and the W-state studied in [8], both of which involve three qubits. These states enable us to perform three-player quantum games such as the GHZ game.
- Devising a tripartite QKD protocol: For the majority of the program we will look for a tripartite QKD protocol and try to prove its device-independent security.
- Finding a proof of rigidity: Finding a strategy to ensure rigidity of the games used in our protocol is a secondary objective of this project. Given a qubit, we need to make sure that it is really in the state required by the protocol.

After that and as a continuation of this research we will review various non-local XOR games in order to look for possible methods of measuring usefulness of one such game for cryptography purposes, based on the principles of rigidity and monogamy.

The final weeks will be spent on finalizing proofs under advisement of Professor Vidick and compiling the findings into a paper.

---

[2]Secure multiparty computation – also known as non-local computation in quantum information literature – refers to algorithms that intend to answer the question of how can we compute a function in a group while keeping each party's input secret from other parties. The main requirements of such a protocol are privacy and correctness.

[3]In the context of SMPC, a semi-honest groups are groups in which all members follow the protocol but they might try to gain additional knowledge, and dishonest refers to when some members may intentionally lie in order to break the protocol or gain additional knowledge

[4]Bias is defined as two times the difference between the winning probability of quantum players and classical players

References

[1] Gilles Brassard; "Brief History of Quantum Cryptography" Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, Awaji Island, Japan, pp. 19-23, October 2005 arXiv:quant-ph/0604072

[2] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner; "Bell nonlocality" arXiv:1303.2849 [quant-ph]

[3] Richard Cleve, Peter Hoyer, Ben Toner, and John Watrous; "Consequences and Limits of Nonlocal Strategies" arXiv:quant-ph/0404076

[4] 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

[5] 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

[6] 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

[7] 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]

[8] W. Dr, 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

[9] 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]

[10] Ben W. Reichardt, Falk Unger, and Umesh Vazirani; "A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games" arXiv:1209.0448 [quant-ph]

[11] C. H. Bennett and G. Brassard; "Quantum Cryptography: Public key distribution and coin tossing" in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)

[12] 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

[13] Umesh Vazirani and Thomas Vidick; "Fully device independent quantum key distribution" arXiv:1210.1810 [quant-ph]

[14] Gyoung Luck Khym, Woo Young Chung, Ji In Kim, Hyung Jin Yang, Hwa Yeon Lee, and Chang Ho Hong; "Quantum Key Distribution among Three Parties Using GHZ States" Journal of the Korean Physical Society, Vol. 44, No. 6, June 2004, pp. 1349-1354