Survey into Quantum Cryptography

Linares, Bryan
California State University, Long Beach
Bryan.Linares01@student.csulb.edu

ABSTRACT

Quantum Cryptography uses the natural properties of quantum computing to achieve secure communication through encrypting and sending secure data. Here we survey research on the contemporary goals of Quantum Cryptography and survey the state of the theory and practice around protocols and current proposals in hardware and networks to make useful and global quantum cryptography a reality. Weak Quantum Coin Flipping is demonstrated in a practical capacity, achieving some positive results with a good outlook. Device Independent Quantum Key Distribution can be optimized with trusted state generation for the communicated information. This is then shown in a Network configuration to be ready for global usage. Finally, a proposed distributed entanglement source is shown to be a way to take pressure off QKD hardware.

1. INTRODUCTION

Quantum Cryptography(QC) refers to security methods, techniques, and applications that encrypt and transmit secured data using the natural properties provided by quantum mechanics, as harnessed through a quantum computer. Its theoretical capabilities could completely break traditional classical cryptography systems and also create new ones that are much more secure and even unbreakable. Traditional cryptography relies on properties of numbers and mathematical calculations to make encryption difficult to crack practically, as represented through binary bits. Quantum Cryptography uses the unique probabilistic and inherent properties of quantum particles in superposition to use quantum bits to represent exponentially larger values in qubits. Data representation can be done with less physical qubits compared with classical bits for the same operations. QC should not be confused with Post-quantum cryptography, which is any cryptography that is secure against quantum and classical computers, and can be completely classical cryptographic systems.

1.1 The State of Quantum Cryptography

In its current state, the field of Quantum Cryptography (QC) wants to prove practical usage, computationally and hardware-wise. Quantum Cryptography covers a broad range of developing fronts, but the focus here in this research survey will remain on two key problems within, Quantum Key Distribution, and Quantum Coin Flipping, and their implementation. Quantum Coin Flipping (QCF) is a building block of quantum algorithms and an important type of quantum cryptography that involves generating random qubits between two distrusting players who both want to win a coin toss. Proving it experimentally with a defined protocol over a reliable distance remains an open problem. Quantum Key Distribution (QKD) is a secure mechanism for exchanging encryption keys, where only the two parties communicating generate and distribute encryption keys only to each other even in the presence of an eavesdropper. The protocol for its use has been defined more concretely so efforts are more focused on its implementation at a practical scale.

Quantum Cryptography by its nature improves computational speed in general, and quantum particle observation changes its state, which helps with eavesdropping. Most currently and past used, classical cryptography is not quantum safe, so the quantum key distribution cryptography protocol is highly promising, using photons or electrons as the qubits encoded in various possible physical systems. These efforts around Key Distribution and Coin Flipping form the basis of the field today. They were theorized first in 1984. [1]

2. BACKGROUND

There will be an assumption of some understanding of cryptography in general. Classical cryptosystem ideas lie underneath quantum cryptography because their basics goals underlie QC: the secure transmission of private data. The ideas of symmetric keys and ciphers are useful in understanding the contents.

2.1 Quantum Coin Flipping

The concept of quantum coin flipping presents a useful primitive where other algorithms that provide secure protocols can be built with the basic abilities it provides. In coin-flipping two parties, Alice and Bob want to create a single shared random bit using a quantum channel, in a way that both parties can be sure was fair and not biased. They both want to guess the outcome and guess correctly. In this scenario, both Alice and Bob can be thought as adversaries to each other, because they both want to win the coin flip. They also both do not trust the other party, and can assume the other party would try to cheat if able, and there is no third party to rely on.

A simple coin flipping process could begin with Alice preparing a quantum value or "coin" in superposition and sending it to Bob. Both have chosen their desired outcome. Bob receives the value over the quantum channel and is supposed to measure it. Assuming both parties were honest, the probability that both would choose the correct outcome would always be 1/2. The measuring party, however, can possibly alter the received information or their choice to create a certain bias in their favor. Because of this variation a strong and a weak coin flipping is defined. In Strong coin flipping, the two parties agree on a random bit in a way that none can bias the outcome beyond a certain threshold. This is good for communication such as online gaming or shared computation tasks. In Weak coin flipping, there is always one correct party, because each party has a preferred and opposite choice of outcome. A classical network cannot guarantee this kind of secure communication without a third party or other restrictions placed on the communication scheme. [3] Using the properties of quantum mechanics, like the no-cloning theorem, cheat-sensitive coin flipping becomes possible.

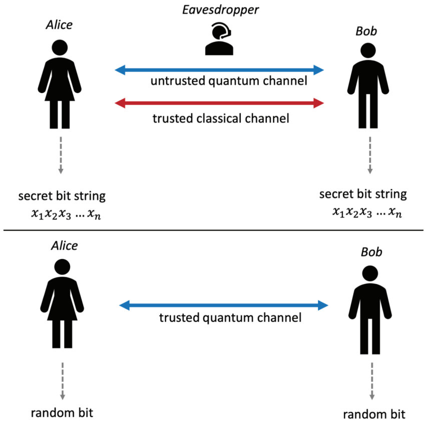

Figure 1: Comparing generalized Quantum Key Distribution(top) with Quantum Coin Flipping (bottom)

2.2 Quantum Key Distribution

Quantum Key Distribution is an analogue to a secure key distribution communication in classical cryptography. In key distribution, Alice and Bob attempt to share a random secret string of bits in the presence of an untrusted eavesdropper, Eve. The goal is for both to send secure symmetric keys between each other, Alice and Bob. The QKD system has a transmitter and a receiver which has a quantum channel and a classical channel. This "transceiver" uses the quantum channel to transmit quantum signals with the information in quantum states for the keys. The classical channel is used for synchronization and other processing like error correction, verification, and other privacy focused operations so Alice and Bob can securely agree on a secret key. If Eve the eavesdropper measures some of the quantum states over the quantum channel, those states will be altered and not received by Bob, they are guaranteed to have collapsed to a classical state after being observed by Eve.

Once the keys have been shared they can be used by Alice and Bob to encrypt or decrypt the message, and send or receive the text respectively. This is the same as it would be in the classical scheme. This is in theory a totally secure method of key distribution that relies only on the natural properties of quantum mechanics.

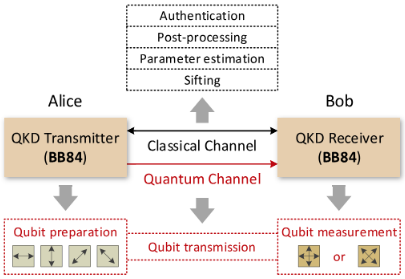

Figure 2: BB84, a protocol implementing QKD

3. PROBLEM STATEMENTS

Various papers with methodologies and approaches to various problems within the field were surveyed. Experimental weak coin flipping, advances in QKD with device independence, a controlled entanglement source for QKD, and possible network schemes for a worldwide communication of QKD were surveyed.

3.1 Experimental cheat-sensitive quantum weak coin flipping [4]

Weak coin flipping is a significant primitive cryptographic operation that allows two mistrustful parties to agree on an outcome bit while favoring opposite outcomes. Conceptual and practical issues have prevented the demonstration of this primitive, but in this paper the issues of finding a setup and quantum resources to provide cheat sensitivity is presented. [4] They implement a refined, loss-tolerant version of a proposed theoretical protocol and exploits heralded single photons generated by an optimized light beam with optical switches for verification. The demonstration required finding a way of generating single photons which are effectively entangled with the vacuum on a beam splitter of adjustable reflectivity. The protocol proposed and implemented is as follows:

- Preparation: Alice sends one photon on a splitter in reflectivity mode x, keeps the mode, and sends another to Bob.
- Decision: Bob sends the state he received on splitter y, and measures the mode on detector Db, and broadcasts outcome b=0 for no detection, or b=1 for photon detected.
- Verification: If b=0 Alice sends her mode to Bob, and it is mixed with his own mode on a splitter z, and both outputs are measured on Dv1 and Dv2.
  - If v2=1 Alice is sanctioned for cheating.
  - (v1,v2)=(1,0) Alice wins
  - (v2,v2)=(0,0) abort
- If b=1 Bob discards his state. Alice measures her state with DA, then depending on output a:
  - a=0: Bob wins.
  - a=1 Bob sanctioned for cheating.

3.2 Advances in device-independent quantum key distribution [5]

A major difficulty for QKD devices is that they behave up to the standards presented in the theory. Real implementations lack "security" and deviation from the intended operation can create security loopholes and invalidate the system. A breakthrough solution for these issues is Device-Independent QKD. This improves the measurement unit but requires a very high quality of specification of the hardware. The concept is proposed as follows: a central untrusted source distributes entangled photon pairs to Alice and Bob, each has a measurement unit—and the violation of a Bell inequality signals the security of the quantum channel. By performing enough local measurements on their incoming photons, the parties can certify the presence of the correct measurement outcomes completely based on the statistics of their inputs and outputs alone. When their results violate a Bell Inequality, their outcomes are guaranteed not to arise from an attack from Eve.

3.3 Evolution of Quantum Key Distribution Networks [2]

QKD networks are two or more QKD nodes connected by optical fiber or free space links. Each pair of QKD nodes negotiates secret keys and with correct implementation can guarantee protection and secrecy going forward. There are upstream and downstream difficulties in keeping information secure from eavesdroppers, meaning going from local to long distance scale and vice-versa. The are multiple possible implementations each with pros and cons, say with optical switches between the nodes, or relays, or quantum repeating of signals. In the repeater case, a physical device needs to be able to decontaminate and forward quantum signals without measuring or cloning them. [2] Such a device does not exist at this time.

3.4 Controlled entanglement source for quantum cryptography [6]

Classical cryptosystems depend on computational complexity to prevent eavesdropping, QKD relies on natural physical principles which guarantee information theoretic security. Device Independent QKD eliminates the need for trust on the communicating party's machines but this trades off with a huge demand in accuracy in the physical devices used. A highly-reliable entanglement source would take some of this demand pressure off for use in DI-QKD. A collective attack could break a DI QKD system, and very efficient detection is needed to not add bias to the system. Here is proposed foreseeing quantum entanglement as a useful resource in networks like gas or electricity, where dealers will distribute entangled states to establish secret keys.

4. APPROACHES AND SOLUTIONS

4.1 Experimental cheat-sensitive quantum weak coin flipping [4]

The approach's solution demonstration relies on the generation of heralded photons that are converted down to pairs of photons at lower energies.3 The outcome becomes the detection or absence of a photon at the detector. There is a refinement in that the presence of losses relate more to cheat sensitivity than bias. By dropping the condition that both have an equal probability of winning when cheating, there is now a verification step that does not punish an honest party, and retains security.

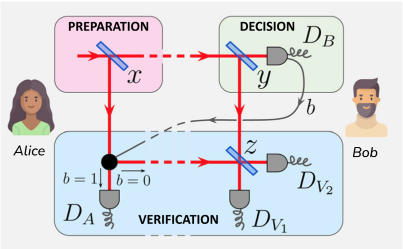

Figure 3: The Weak Coin Flipping experiment

The results are that there are strictly 5 outcomes, "Alice wins or is sanctioned, Bob wins or is sanctioned, or the protocol aborts." [4] Under the experimental setup, the optical fiber components are kept at a telecom wavelength, to show practical usage. Accounting for errors in the hardware, like fluctuations in the reflectivity of the detectors, the probabilities may also change even if both parties are being honest. So this has to be accounted for with fairness and correctness values when measuring. When one or both parties are being dishonest, the verification step must be accounted for. In one example Bob's optimal cheating strategy is shown by forcing the switch to send the photon to DA, the probablity of sanctioning Bob decreases as communication losses increase, which limits Alice's cheat sensitivity, and possibly gives an advantage to Bob when Alice's section has losses. Bob can only win or be sanctioned in that case he cheats. There are methods in the choice of materials and hardware and the instruments chosen as well.

4.2 Advances in device-independent quantum key distribution [5]

The central source has to distribute particles with proper quantum states, and the hardware has to be able to test Bell states randomly at a high enough speed with high efficiency. In a completely photonic implementation, photon pulses are periodically generated by a source, and Alice and Bob both have photon receivers that have to be attuned to fidelity that reaches 84% 4 There are error detection signal dropoffs when distance is added in the communication hardware. So despite the progress, photon based implementations still need a lot of improvement.4

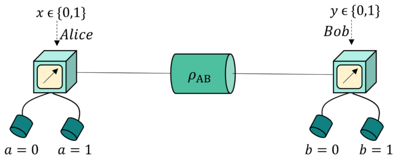

Figure 4: Device Independent QKD

4.3 Evolution of Quantum Key Distribution Networks [2]

A proposed QKD Node is demonstrated with a design that can be a backbone or access node for the network. A physical

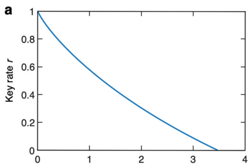

Figure 5: DI-QKD distance dropoff

QKD node will need a few components: first the transceiver to generate the local secret keys that will be forwarded to the next component. Then the key manager, which would be a distributed server for managing generated secret keys connected to that node up to their employment by their application. Following that an Optical Switch to facilitate the connection of a quantum channel from a transmitter to any receiver or the reverse at a limited distance. This device would be able to multiplex across the different frequency bands of the quantum channel. So lastly the multiplexer component would decide the final output. Outside of this a secure infrastructure is needed to provide more safeguards for the network overall.

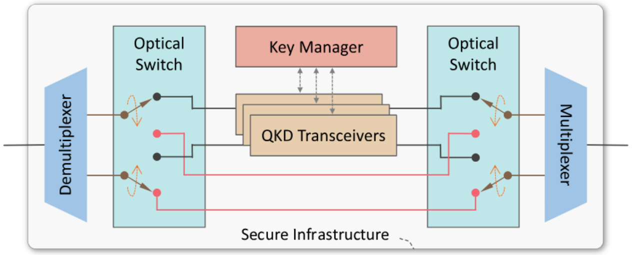

Figure 6: QKD Network Node

4.4 Controlled entanglement source for quantum cryptography [6]

The proposed scheme involves adding quantum secret sharing (QSS) to a protocol to enhance an entanglement source to have access control to binary pseudo randomness introduced to the generated keys. [6] This mixed state can add protection to DI-QKD with a time-bin encoding system.

In the scheme, a random value of 0 or pi is assigned to entangled qubits,this modulation then has to be communicated to the legitimate users. The scheme means that the raw key given by the qubit dealer has modulation information, which is the same size as the key held by each user. So the controller must participate in sharing a string longer than the raw key. Since the source needs to generate random bits throughout that need to be decrypted, their suggested practical solution is to use a block cipher algorithm like AES in stream encryption mode, already used in some cases to prepare and measure QKD implementations. [6]

5. CONCLUSION

Our survey noted important progress points on problems in the contemporary state of Quantum Cryptography. For the Weak Quantum Coin Flipping experiment, the implementation of the proposed protocol showed a promising demonstration using tunable beam splitters, and fast optical switches with a customized protocol to create a more balanced implementation of the theory. QKD is in a much more practically advanced state, with work surveyed here, being put into networks, and using an ultimate form of the scheme in Device Independence, and optimizing the implementation by controlling its entanglement source.

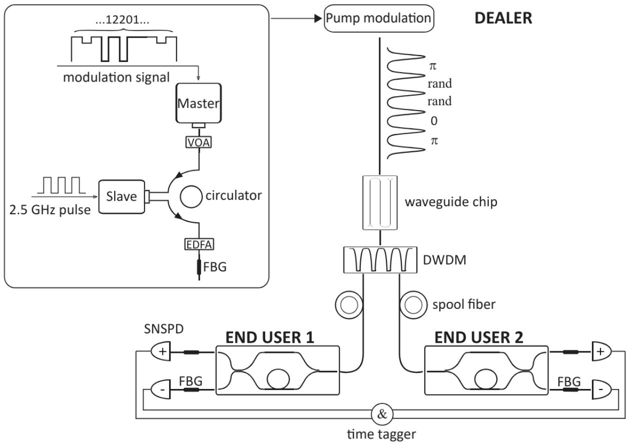

Figure 7: Controlled Entanglement Based QKD

5.1 Benefits

Improved Quantum Cryptography has huge and widely important consequences for the future and past of all cryptography and encryption. Weak Quantum Coin Flipping is in a state of improvement but not completely reliable hardware. QKD networks are in a valid state of progress, and their future implementation relies on physical hardware that does not exist in a practical form yet.

5.2 Risks

These software, hardware, and theoretical solutions may prove to only be temporary as new theory is studied and discovered. Demonstrating Weak Quantum Coin Flipping in its current state presents challenges in the hardware and tunability for widespread use. Accounting for noise and distance, photon based implementation of Device Independent QKD needs more improvement. The demands of the protocol also puts a high amount of efficiency demand in the hardware that implements it. Changes, additions, and new theory added to the the protocol are also possible avenues of solutions.

6. FUTURE OUTLOOK

The improvement of practical Quantum Cryptography is arguably the most pressing and impacting consequence of the development of capable quantum computers at scale. The future of Quantum Computing will continue to evolved depending on how quickly discoveries are made and the hardware and theory is improved. There are many open problems. All our past and future data protected by cryptographic systems are all at risk with its improvement.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, Dec. 2014. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2014.05.025

[2] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[3] C. A. Miller, "The mathematics of quantum coin-flipping," no. 69, 2022-12-01 05:12:00 2022. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934443

[4] S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti, "Experimental cheat-sensitive quantum weak coin flipping," *Nature Communications*, vol. 14, no. 1, Apr. 2023. [Online]. Available: http://dx.doi.org/10.1038/s41467-023-37566-x

[5] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, "Advances in device-independent quantum key distribution," *npj Quantum Information*, vol. 9, no. 1, Feb. 2023. [Online]. Available: http://dx.doi.org/10.1038/s41534-023-00684-x

[6] Q. Zeng, H. Wang, H. Yuan, Y. Fan, L. Zhou, Y. Gao, H. Ma, and Z. Yuan, "Controlled entanglement source for quantum cryptography," *Physical Review Applied*, vol. 19, no. 5, May 2023. [Online]. Available: http://dx.doi.org/10.1103/PhysRevApplied.19.054048