Kartik Padave

A022

70362019039

Experiment 10

Aim

Study of Quantum Coin Flipping, a Quantum Cryptography Cipher.

Abstract

Manuel Blum introduced coin flipping as part of a classical system in 1983 based on computational algorithms and assumptions. Blum's version of coin flipping answers the following cryptographic problem:

Alice and Bob are recently divorced, living in two separate cities, and want to decide who gets to keep the car. To decide, Alice wants to flip a coin over the telephone. However, Bob is concerned that if he were to tell Alice heads, she would flip the coin and automatically tell him that he lost.

Thus, the problem with Alice and Bob is that they do not trust each other; the only resource they have is the telephone communication channel, and there is not a third party available to read the coin. Therefore, Alice and Bob must be either truthful and agree on a value or be convinced that the other is cheating.

In 1984, quantum cryptography emerged from a paper written by Charles H. Bennett and Giles Brassard. In this paper, the two introduced the idea of using quantum mechanics to enhance previous cryptographic protocols such as coin flipping.[3] Since then, many researchers have applied quantum mechanics to cryptography as they have proven theoretically to be more secure than classical cryptography, however, demonstrating these protocols in practical systems is difficult to accomplish.

Introduction

In cryptography, Coin Flipping is defined to be the problem where two mutually distrustful and remote players want to agree on a random bit without relying on any third party. Strong Coin Flipping (SCF) is defined to be a coin flipping problem where each player is oblivious to the preference of the other. Weak Coin Flipping (WCF) is defined to be a coin flipping problem where each player knows the preference of the other. It follows that the players have opposite preferences. If this were not the case, then the problem will be pointless as the players can simply choose the outcome they desire. Consider any coin flipping protocol. Let Alice and Bob be the two players who wish to implement the protocol. Consider the scenario where Alice cheats using her best strategy against Bob who honestly follows the protocol. Let the probability that Bob obtains the outcome Alice preferred be given by P_a*. Consider the reversed situation, i.e. Bob cheats using his best strategy against Alice who honestly follows the protocol. Let the corresponding probability that Alice obtains the outcome Bob preferred to be given by P_b*.

The bias of the protocol is defined to be e = max[P_a*, P_b*] – (1/2).

The half is subtracted because a player will get the desired value half the time purely by chance.

Theory

Quantum coin flipping and other types of quantum cryptography communicate information through the transmission of qubits. The accepting player does not know the information in the qubit until he performs a measurement. Information about each qubit is stored on and carried by a single photon. Once the receiving player measures the photon, it is altered, and will not produce the same output if measured again. Since a photon can only be read the same way once, any other party attempting to intercept the message is easily detectable.

Quantum coin flipping is when random qubits are generated between two players that do not trust each other because both want to win the coin toss, which could lead them to cheat in a variety of ways. The essence of coin flipping occurs when the two players issue a sequence of instructions over a communication channel that then eventually results in an output.

A basic quantum coin flipping protocol involves two people: Alice and Bob.

1. Alice sends Bob a set number of K photon pulses in the quantum states $\emptyset_{\propto c}$. Each of these photon pulses is independently prepared following a random choice by Alice of basis αi and bit ci where i = 1, 2, 3...K.

2. Bob then measures the pulses from Alice by identifying a random basis βi. Bob records these photons and then reports back the first successfully measured photon j to Alice along with a random bit b.
3. Alice reveals the basis and bit that she used at the basis Bob gave her. If the two bases and bits match, then both parties are truthful and can exchange information. If the bit reported by Bob is different than that of Alice's, one is not being truthful.

A more general explanation of the above protocol is as follows:

1. Alice first chooses a random basis (such as diagonally) and a sequence of random qubits. Alice then encodes her chosen qubits as a sequence of photons following the chosen basis. She then sends these qubits as a train of polarized photons to Bob through the communication channel.
2. Bob chooses a sequence of reading bases randomly for each individual photon. He then reads the photons and records the results in two tables. One table is of the rectilinear (horizontal or vertical) received photons and one of the diagonally received photons. Bob may have holes in his tables due to losses in his detectors or in the transmission channels. Based on this table, Bob makes a guess as to which basis Alice used and announces his guess to Alice. If he guessed correctly, he wins and if not, he loses.
3. Alice reports whether he won or not by announcing what basis she used to Bob. Alice then confirms the information by sending Bob her entire original qubit sequence that she used in step 1.
4. Bob compares Alice's sequence with his tables to confirm that no cheating occurred on Alice's part. The tables should correspond to Alice's basis and there should be no correlation with the other table.

There are a few assumptions that must be made for this protocol to work properly. The first is that Alice can create each state independent of Bob, and with an equal probability. Second, for the first bit that Bob successfully measures, his basis and bit are both random and completely independent of Alice. The last assumption is that when Bob measures a state, he has a uniform probability to measure each state, and no state is easier to be detected than others. This last assumption is especially important because if Alice were aware of Bob's inability to measure certain states, she could use that to her advantage.

Conclusion

Previous protocols called for a single photon source or an entangled source to be secure. However, these sources are why it is difficult for quantum coin flipping to be implemented. Instead, the researchers at LTCI used the effects of quantum superposition rather than a single photon source, which they claim makes implementation easier with the standard photon sources available. The researchers used the Clavis2 platform developed by IdQuantique for their protocol but needed to modify the Clavis2 system in order for it to work for the coin flipping protocol. The experimental setup they used with the Clavis2 system, involves a two-way approach. Light pulsed at 1550 nanometres is sent from Bob to Alice. Alice then uses a phase modulator to encrypt the information. After encryption, she then uses a Faraday mirror to reflect and attenuate the pulses at her chosen level and sends them back to Bob. Using two high quality single photon detectors, Bob chooses a measurement basis in his phase modulator to detect the pulses from Alice. They replaced the detectors on Bob's side because of the low detection efficiencies of the previous detectors. When they replaced the detectors, they were able to show a quantum advantage on a channel for over 15 kilometres (9.3 mi). A couple of other challenges the group faced was reprogramming the system because photon source attenuation was high and performing system analyses to identify losses and errors in system components. With these corrections, the scientists could implement a coin flipping protocol by introducing a small honest abort probability, the probability that two honest participants cannot obtain a coin flip at the end of the protocol, but at a short communication distance.

References

1. *Blum, Manuel (1983-01-01). "Coin flipping by telephone a protocol for solving impossible problems". ACM SIGACT News.* ***15*** *(1): 23–27. doi:10.1145/1008908.1008911. ISSN 0163-5700.*
2. *^ Oded., Goldreich (2003). Foundations of cryptography. Cambridge, UK: Cambridge University Press. ISBN 9780521791724. OCLC 45093786.*
3. ^ Jump up to:*a b c d e f g h i j* Stuart Mason Dambort, "Heads or tails: Experimental quantum coin flipping cryptography performs better than classical protocols", *Phys.org*, March 26, 2014

4. ^ *Cleve, R. (1986-11-01). "Limits on the security of coin flips when half the processors are faulty". Proceedings of the eighteenth annual ACM symposium on Theory of computing - STOC '86. ACM. pp. 364–369. doi:10.1145/12130.12168. ISBN 0897911938.*
5. ^ A. Kitaev, Quantum Coin Flipping, Quantum Information Processing Workshop, Mathematical Sciences Research Institute, University of California, Berkeley, 2003.
6. ^ *Ambainis, A.; Buhrman, H.; Dodis, Y.; Rohrig, H. (2004). "Multiparty quantum coin flipping". Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004. IEEE: 250–259. arXiv:quant-ph/0304112. doi:10.1109/ccc.2004.1313848. ISBN 0769521207.*
7. ^ C. Mochon, Quantum Weak Coin Flipping with Arbitrarily Small Bias, preprint, arXiv:0711.4114, 2007.
8. ^ *Aharonov, Dorit; Chailloux, André; Ganz, Maor; Kerenidis, Iordanis; Magnin, Loïck (January 2016). "A Simpler Proof of the Existence of Quantum Weak Coin Flipping with Arbitrarily Small Bias". SIAM Journal on Computing.* ***45*** *(3): 633–679. arXiv:1402.7166. doi:10.1137/14096387x. ISSN 0097-5397.*
9. ^ *Mochon, Carlos (2005). "Large family of quantum weak coin-flipping protocols". Physical Review A.* ***72*** *(2): 022341. arXiv:quant-ph/0502068. Bibcode:2005PhRvA..72b2341M. doi:10.1103/PhysRevA.72.022341.*
10. ^ Jump up to: *a b c d e f* Vivek R and Dr. J. Roopchand, "Emerging Trends in Quantum Cryptography – A Survey", *International Journal of Computer Technology and Applications*, August 2012
11. ^ Jump up to: *a b c d* Anna Pappa et al., "Experimental Plug and Play Quantum Coin Flipping", *Nature Communications*, April 24, 2014
12. ^ Jump up to: *a b c* C. Döscher and M. Keyl, "An Introduction to Quantum Coin-Tossing", *Cornell University Library*, February 1, 2008
13. ^ *Blum, Manuel (1983-01-01). "Coin flipping by telephone a protocol for solving impossible problems". ACM SIGACT News.* ***15*** *(1): 23–27. doi:10.1145/1008908.1008911. ISSN 0163-5700.*
14. ^ D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, Quantum bit escrow, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, ACM, New York, 2000, pp. 705–714.
15. ^ *Spekkens, R. W. (2002). "Quantum Protocol for Cheat-Sensitive Weak Coin Flipping". Physical Review Letters.* ***89*** *(22): 227901. arXiv:quant-ph/0202118. Bibcode:2002PhRvL..89v7901S. doi:10.1103/PhysRevLett.89.227901. PMID 12485105.*

16. ^ Jump up to: *a b c d e f g h i j* Charles H. Bennett and Giles Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science*, December 4, 2014
17. ^ *Mochon, Carlos (2005). "Large family of quantum weak coin-flipping protocols". Physical Review A.* ***72*** *(2): 022341. arXiv:quant-ph/0502068. Bibcode:2005PhRvA..72b2341M. doi:10.1103/PhysRevA.72.022341.*
18. ^ *50th Annual IEEE Symposium on Foundations of Computer Science, 2009 FOCS '09 ; 25-27 Oct. 2009, Atlanta, Georgia, USA ; proceedings. IEEE Computer Society Technical Committee on Mathematical Foundations of Computing, Annual IEEE Symposium on Foundations of Computer Science 50 2009.10.25-27 Atlanta, Ga., FOCS 50 2009.10.25-27 Atlanta, Ga. Piscataway, NJ. ISBN 9781424451166. OCLC 838170374.*