Quantum Security and Improvised BB84 QKD Protocol

S. Dhanalakshmi[1], Jasleen Kaur Sethi[2], Sharmista Paul[3], Yashvardhan Chakraborty[4]

[1]Department of Electronics and Communication, SRMIST, Kattankulathur, India
[2]Department of Electronics and Communication, SRMIST, Kattankulathur, India
[3] Department of Electronics and Communication, SRMIST, Kattankulathur, India
[4]Department of Electronics and Communication, SRMIST, Kattankulathur, India

Abstract The advent of Copenhagen interpretation brought with it the potential for exponential computing that could be applied in 1980's since the first proposed Quantum Computer by Paul Benioff. The domain accelerated soon with the merits that it could provide over classical computing. This paper provides a holistic review of the upbringing of the quantum-peculiar concepts and quantum security, and with that a suggestion for optimally utilizing BB84, a "Quantum Key Distribution" protocol. While the concepts are discussed in brief, BB84 is discussed in enough detail for it to act as a prerequisite for the suggestion. The suggestion is introducing various settings of the number of basis states involved. An optimal solution for appropriate number of basis is made by comparing the received information by Bob in the absence of Eve and that in presence of Eve.

Keywords: *Quantum Computing, Quantum Superposition, Quantum Entanglement, No-Cloning Theorem, Bell State, Quantum Key Distribution, BB84*

1. Introduction

Benioff, in the early 80's, described a quantum computer that governed over the Schrodinger equation description of the Turing Machine [1]. Soon later, Feynman provoked in the physics community the plausibility of Quantum Simulators. These two theoretical models were reversible and did not dissipate energy, something that sounded a revolution in physical hardware enterprise [1]. The evident merits brought the unconventional computing in the global fame for the disciplines such as industry, banking and government records purpose, and cyber security and cryptography with the further realization of non-cloning theorem. Although the push was in the 80's, the whole of quantum computing has its roots over certain primitive and fundamental concepts of the quantum theory that were discovered in the 20's - superposition and entanglement. These are discussed in section 2. With them, the two unconventional constructions of quantum states are discussed that enable quantum computing as a facilitation of encrypted information communication. Section2 acts as a prerequisite for section 3. Encryption of the quantum communication protocols is discussed in section 3, where the payoffs are evaluated over the number of basis considered in the BB84 protocol, devised in 1984 by Charles Bennett and Gilles Brassard as a "Quantum Key Distribution" protocol. Here, an optimal solution for appropriate number of basis is made by comparing the received information by Bob in the absence of Eve and that in presence of Eve. The solution is realized to depend on a common payoff between Alice and Bob, agreed non-publicly prior to setting up BB84. The solutions is subjective making them to host various specific "setting" calls from applications over the globe. The solutions are parameterized quantitatively using probabilistic arguments.

2. Taken from quantum theory

Plank, in 1900, announced his solution for the black-body problem as the "quantized energy" [2]. Endorsed by Einstein in his Nobel-prize winning explanation of the photo-electric effect in 1905, Plank's ansatz was a considerable deal among the community folks then [3]. This birth of quantum theory proceeded with Bohr's "quantized angular momentum," and then Schrodinger's formulation of the equation of motion in the 20's. Until Schrodinger's, although the physicists had been engaged in structuring the theory, the description of particles itself was unclear. Since it was trivial in the context of devising the equation, not only Schrodinger but also Heisenberg, Klien, Gordan and Dirac, who reformed Schrodinger's work in the coming years, could have devise their equations without a known description. Nevertheless, this wasn't the case as Born published his seminal work, a description now known as the "Copenhagen Interpretation", in 1925. Like Plank's, his was an ansatz too. He claimed, the wavefunction used in SE had a physical meaning only when multiplied with its complex conjugate [4]. For the static cases that are solved using the Time-Independent-Schrodinger's-Equation, where the wavefunction appears to be real, the probability reduces down to the wavefunction norm squared.

$$P(x,p)=\psi(x,p)\psi(x,p)* \qquad (1)$$

A typical composite wavefunction takes the form $\psi(x,p) =\int idxdpAi(x,p)\psi i(x,p)$. It "collapses" under classical measurements to the "basis" wavefunction ψ in a manner motivated by (1) - the probability of occurrence of ψ ion the collapsing of ψ is |Ai| 2, the norm square of probability amplitude [4]. The conservation of physical occurrences necessitate ψ to be normalized. This is done by scaling Ai using (2).

∫idxdpAi(x,p) = 1 (2)

The Copenhagen Interpretation and composite form of ψ together depict the completeness of the unconventional kind of superposition of ψ i's. These formulations connect with the information theory by the physical attributes that enforce the information states. A typical thinking involves information as binary, thus the states as |0〉 and |1〉 . A quantum bit, qubit, can be thought of as a superposition between the two binary states. For simplicity and symmetry, Ai=1√2 in (3) and Aii=1√2 in (4).

ψ=1√2 |0〉 +1√2 |1〉 (3)

ψ′=1√2|00〉 +1√2|11〉 (4)

(4) Represents a composite information built by taking ψ's besides each other in multiplication. The no-cloning principle is evident here. It says, the state of the n-qubit system cannot be factorized into the state of individual parent qubits. (4), called the Bell State, is a special kind. If both Alice and Bob share (4), and if Alice measures the state as|00〉 , since the available state to Bob will collapse to ψ = |00〉 , it would now be certain and not partially probabilistic for Bob to measure|00〉 [5]. Thus, such a state is also called the "entangled state" and the phenomenon of sharing an entangled state that leads to spontaneous discharge of probabilities, not allowed in classical scenarios, is called the "entanglement". The spontaneity involved added on to Einstein's denial for the quantum theory, a denial that he published as the EPR paradox in 1935 [5].Furthermore, two properties that enable information security in quantum computing are mentioned as follows. An arbitrary photon, for illustration, in any state of polarization is realized to be identical with the other photons prepared in the same polarization, irrespective of the relative phase, φ. This is unlike what the classical mechanics suggests for the waves.

Furthermore, the building up of composite states implies in the process the information loss about the parent states, unlike the traceability of the parent waves using the Fourier coefficients.

3. BB84 and Improvisation

Exploiting the properties of quantum theory, discussed in section 2, enhances the cryptography perspective of the communication. A best known example of quantum cryptography is quantum key distribution (QKD) which offers an information-theoretically secure solution to the key exchange problem. BB84, Bennett-Brassard1984, is the most primitive example of QKD protocols that ensure the information correctness as well as the security. The first action in any quantum communication protocol is "distributing the states" [6]. Following are the steps for the same for BB84 protocol under the tradition of Alice and Bob. Note that BB84 uses two channels, classical and quantum.

1. Alice chooses a bit string xA=x1,...,xN.
2. Alice chooses a random basis string θA=θ1,...,θN and so does Bob,˜θB.θ=0 refers to the orthogonal basis pair [|0〉 ,|1〉] and θ = 1 refers to [|+〉 ,|−〉], the Hadamard basis.3. For 1≤j≤N, Alice sends to Bob bit xj encoded in the basis θj :|xj〉 θj.4. Bob measures the qubit in basis˜θj to obtain the outcome ˜xj.

The protocol proceeds with Bob announcing the receipt of the states over a classical channel. Alice and Bob exchange the strings θA and˜θB. The key step is - they discard all the rounds where˜θj6 = θj. Now, they exchange the shortest string that they supposed to have all the bits common. Statistically, the length of this string can be supposed as N2. To test the error rate, δ, Alice randomly choose half of the remaining rounds. She tells Bob which rounds are tested. Alice and Bob exchange bits xj and ˜xj for those rounds. For a noise free environment, δ= 0 [6].δ6= 0 signifies either the quantum noise due to "quantum decoherance", presence of Eve, or both. Ideally, both Alice and Bob can choose to abort the protocols in such a case. Nonetheless, given that the current technology that withholds the qubits is considerably susceptible to decoherence, discarding the protocol for every non-zero error rate would waste not only the power to run quantum computers but also the time, one significant aspect that constitutes as a default objective in quantum communication [7].To resolve this, a novel standard is provided that suggests accepting certainδ6= 0 settings, σ. We formulate these settings by introducing, one by one, more θ pairs. If [|0〉 ,|1〉] is considered to be [0,π2] geometrically, and so [|+〉 ,|−〉] to be [π4,3π4], other θ's could be [π8,5π8] and so on, or the standards [π3,4π3] and so on. For σ= 2, Bob reconstructs the right information half of the times, as mentioned. If information bits are sent through the quantum channel as qubits, even for a wrong randomly chosen basis by Bob, half of these qubits can be statistically supposed to collapse giving out the right bit. Thus, the probability of inferring the correct information is 75%. If Eve is listening to the quantum channel, the case whenδ6= 0, out of the 25% gain in probability due to the reason mentioned right above, she will tend to regenerate false information towards Bob making probability of inferring the correct information as 62.5% Bob. Using the same logic, probability of inferring the correct information for Bob is calculated for few σ's. This calculation is evident from the following quantitative expression, (5).

1/σ + ∑ 1/2σ (from σ=1) (5)

Certain attributes are plotted in the table 1. While Δ is the percentage difference between the values of column (2) and (3) for a fixed σ, τ is Δ divided by the values of column (2). τ indicates the reliability of σ system over the argument that more the difference between the values of column (2) and (3), more distinguishable is the presence of Eve with a considerate noise due to quantum decoherence. Setting σ=5 seems a visually appealing setting just because the numerals are integers and thus, it could work on computers providing broad resolution. Thus, we stop there. With increment in τ, the payoff is dropping probability of inferring information. Nonetheless, with each next σ, the drop becomes minute, motivating the user to explore further settings.

No. of basis	Probability of Inferring Correct Information to Bob	Probability of Inferring Correct Information to Bob in presence of Eve.	Δ	τ
2	75%	62.50%	12.50	0.16
3	66.65%	49.99%	16.66	0.24
4	62.5%	43.75%	18.75	0.3
5	60%	40%	20	0.33

Table 1. Probabilistic Attributes For Bob

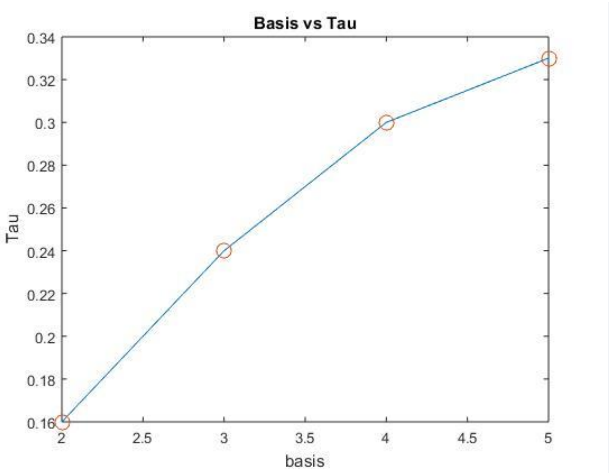

Figure 1. Theoretical attributes of τ vs. Number of Basis involved

3. Results and Discussion

The BB84 protocol is programmed and simulated using the quantum computing software launched by IBM, named Qiskit. Initially the number of basis states introduced in the BB84 protocol simulation is constraint to two as already stated in the actual protocol and the practical values of the probability of obtaining the correct information to Bob when no Eve is introduced in the back-end circuit of the protocol under consideration is noted down after successfully performing the simulations. Furthermore, the codes of the program is accordingly improvised to add more number of basis states in the quantum circuit. This is substantially done by adding more gates to the circuit at appropriate positions accordingly contributing to increment of number of basis states available. Similarly, more number of basis are added to the simulation circuit for the required increment. All the practical values of probabilities of inferring correct information for Bob, in both absence and presence of Eve, Δ,the percentage difference between the values of probabilities of obtaining the right information in presence from absence of Eve and τ, stating the percentage value obtained throughout the simulations is noted down in the table 2.

No. of basis	Probability of Inferring Correct Information to Bob	Probability of Inferring Correct Information to Bob in presence of Eve.	Δ	τ
2	68.75%	62.50%	6.18	0.09
3	62.50%	56.25%	6.2	0.1
4	56.2%	50%	6.2	0.11

Table 2. Practical Attributes For Bob

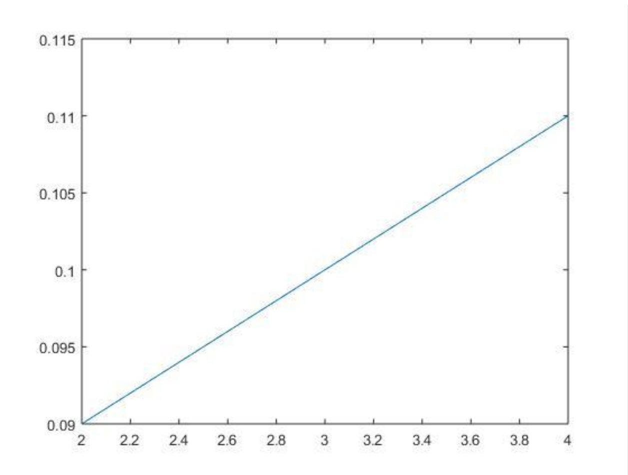

Figure 2. Practical attributes of τ vs. Number of Basis involved

From the final simulation results and the practical values obtained after increasing the number of basis states in the quantum circuit of Alice and Bob verified the theoretical calculations done in the prior section, which also stated that the increment in the same will contribute in the easy detection of eavesdropping by Eve in the quantum protocol application of BB84.

Conclusion

A brief review of quantum superposition and quantum entanglement is provided. The properties of quantum theory that enable quantum computing are discussed. An emphasis is put on quantum security. Condition for Quantum Key Distribution protocol BB84 is shown to be highly non-pragmatic with the current technology on the quantum computers. A suggestion to optimize the protocol on the payoff of losing probability of accessing correct information is made. The suggestion is supported by converging function, (5), that is evident from Table1 and Figure 1. Optimal solution between payoff and maximum plausible τ for the two numerals to be integers is propounded.

References

[1] P. Benioff, *“Quantum mechanical models of turing machines that dissipate no energy”,* Physical Review Letters 48 (1982) 1581.

[2] M. Plank, “*On the theory of the energy distribution law of the normal spectrum*”, Verhandl. Dtsch. phys. Ges. 2 (1900) 237..

[3] Einstein, “*Concerning an heuristic point of view toward the emission and transformation of light*”, Annalen der Physik 17(1905) 132.

[4] A. Pais, “*Max born’s statistical interpretation of quantum mechanics*”, Science 218 (1982) 1193–1198.

[5] L. Hadjiivanov, I. Todorov, “*Quantum entanglement*”, arXiv preprint arXiv: 1506.04262.

[6] . W. Shor, J. Preskill, “*Simple proof of security of the bb84 quantum key distribution protocol*”, Phys. Rev. Lett. 85 (2000)441.

[7] M. A. Saki, Abdullah Ash, S. Ghosh, “*Study of decoherence in quantum computers: A circuit-design perspective*”, arXiv preprintarXiv: 1904.04323.