Modifying BB84 For Topological Quantum Systems

Pratyansha Rana
Computer Science Engineering AI/ML
Lakshmi naraian college of technology and Science
Bhopal ,India
pratyanshrana1@gmail.com

Dr. niketa persai
Department of Engineering Physics
Lakshmi naraian college of technology and Science
Bhopal ,India
persainiketa@gmail.com

***Abstract*—The 21st century has seen a rapid development in the field of quantum computing which is based on the principles of quantum physics , such as quantum superposition , quantum entanglement , no-cloning theorem etc. As we witness advancement in quantum computers the classical cryptography is getting increasingly vulnerable , as the classical encryption is based on complex mathematical problems which quantum computers can solve in a matter of seconds and hence breaking the encryption will become significantly easy. To counter this challenge Researchers introduced a secure system of cryptography which was achieved with the help of Quantum Key Distribution or QKD. It has multiple existing protocols for example, BB84 , E91 etc. These protocols were designed to work on the conventional qubit systems but the recent development of topological qubits has raised a need of a more efficient Quantum Key Distribution protocol .**

In this research paper we propose a modified BB84 protocol Which is optimized for Topological qubit system. And we have analyzed the efficiency, security, and performance of the proposed protocol.

Keywords—Quantum , Quantum Computing , Quantum Key Distribution(QKD),Superposition,entanglement,No-cloning , QKD protocol , Qubit , Topological Qubit ,BB84 protocol , E91 protocol.

I. Introduction

A. Quantum Computing Overview

The realm of quantum computers is being explored by scientists for a long time now , quantum computing is an emerging field of computing which leverages quantum physics' principles for computing efficiently and this ability of quantum computers to leverage these rules has given quantum computers an edge over the classical computers. The very basic difference between the classical computers and quantum computers is the fundamental way of storing data , in classical computing the data was stored in the form of bits which holds value either 0 or 1 , it is basically a transistor on or off , but in quantum computers the data is stored in a qubit (Quantum bits) , unlike classical bits which can store only 0 or 1 a qubit can exist in superposition of both 0 and 1.

The recent advancemens in the field of quantum computing has changed the whole scenario , recently Google had introduced it's willow chip with 105 Physical qubits similarly IBM's Condor chip , unveiled in december 2024 had 1121 qubits , making a quantum processor with larger number of qubit is a challenging , the reason for this issue is the fragile quantum states of the qubits which is very sensitive to the environmental noise and any other disturbance ,even with a very small disturbance the quantum state of the qubit collapses, and as a result of that when we increase the number of qubits in the chip the error rates in the chip increases exponentially, so devloping a chip with larger number of qubit requires very advanced engineering and complex problems such as maintaining a temperature near absolute zero for maintaining least environmental noise possible to make the qubits stable.

But the whole landscape got flipped when the Majorana 1 was introduced by Microsoft , the world's first quantum processing unit, powered by a topological core.

B. Introduction to Quantum Key Distribution.

In the era of advancing Technologies and communication methods the importance of secure communication has increased drastically as the user is getting more and more involved in online communication , the protection of users' data is the need of hour , to achieve the security of the communication we use encryption of messages which falls under cryptography , The classical cryptography is based on complex mathematical problems which are difficult for classical computers to solve but as we see advancements in the field of quantum computing , breaking these classical encryption is not a difficult task , and exposing every single data to an unknown risk. Classical cryptographic systems such as RSA and AES , rely on computational hardnedd assumptions , making them vulnerable to Quantum attacks.

Quantum Key Distribution offers a revolutionary approach to encryption systems by leveraging the Quantum physics laws to provide a much secure way to exchange keys. The BB84 protocol proposed by Bennet and Brassard in 1984 , is the most widely studied QKD protocol , relying on the quantum superposition and measurement disturbances hence ensuring security.

C. Need of separate QKD protocol for Topological Qubits

The traditional QKD protocols were designed to work over photonic qubits , which could be easily transmitted through optical fibres.

Topological qubits are based on Majorana zero modes , and have unique error dynamics and are more resistant to decoherence . The standard BB84 protocol assumes single photonic measurement whereas Topological qubit may require different measurement techniques.In BB84 the measurement is done in rectilinear and diagonal bases using photons detectors. Topological qubits do not rely on direct quantum state measurements like photonic qubits do. Instead they use non-Abelian braiding operations to manipulate and measure quantum states. A modified BB84 protocol must have a specifically designed reading mechanism for topological Qubits.

Error correction and fault tolerance abilities of a topological qubit is significantly high as compared to a conventional qubit , and also the conventional QKD protocols rely on error correction methods suitable for photonic noise models . The new protocol should have an optimized error correction method specifically designed for the noise models of topological systems.

II. Background and related work

A. Basic quantum mechanic principles

Quantum computing rely on quantum mechanics laws such as superposition, entanglement, no cloning theorem. Similarly the Quantum Key Distribution also depends upon these laws of quantum physics.

- Superposition – This law states that a quantum system can exsist in multiple states simultaniously.

  Mathematically a quabit state is represented as :

  $$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$$

  where α and β are probability amplitudes such that

  $$|\alpha|^2 + |\beta|^2 = 1.$$

  when these qubits are measured the quantum state collapses into either $|0\rangle$ or $|1\rangle$ with certain probability.

- Entanglement – entanglement is a quantum phenomenan which is responsible for linking two or more than two quantum particles such that the state of one qubit immediately influences the state of other(s) regardless of the distance between them.

  Mathematically these entangled qubit are represented as :

  $$|\psi\rangle= 1/\sqrt{2}\ (|00\rangle+|11\rangle\ )$$

  if one qubit is measured $|0\rangle$ the automatically collapses to $|0\rangle$, similarly for $|1\rangle$, even if they are light years apart.

- No-cloning – NO cloning theorem states that it is impssible to create an identical copy of an arbitrary unknown quantum state.

  This prevents eavesdroppers from copying the quantum information without detection.

B. Existing QKD protocol

The development of QKD protocol had started in late 20th century and from that time onwards we have witnessed many Quantum Key Distribution protocols but the most widely used QKD protocol is the BB84 protocol.

It is a prepare and measure protocol, which allows two parties to generate a shared key.

Lets assume the two parties to be Alice and Bob, Alice sends a random quantum state to Bob, Bob measures that quantum state in random basis. They communicate over a public channel to compare measurement basis. A secure key is extracted after error correction and privacy amplification.

Flow of the protocol

- Alice prepares and sends qubit :

  Alice randomly chooses a bit (0 or 1).

  She randomly chooses a measurement basis, either X-basis or Z-basis .

  X-basis - $|+\rangle$ or $|-\rangle$

  Z-basis - $|0\rangle$ or $|1\rangle$

  Now she sends qubits one by one over a quantum channel (photons). Alice sends qubits through polarised photons through optical fibres.

  Alice uses a photon polarizer to prepare each photon in specific quantum state.

- Bob's measurement

  Bob uses a beam splitter and a polarization filter to measure the incoming photons, he randomly chooses either Z-basis or X-basis for each recived qubit.

  If he chooses the same basis as alice he gets the correct bit, if he chooses the wrong basis the measurement is random (50% chance of getting the right bit).

- Comparision

  Alice and Bob publically announce their chosen basis, but not their measurement results.

  They compare their chosed basis and discards the bits where they chose different basis. And store the bits in ehich they used the same basis for measurement.

- The final shared-key is generated with the stored bits.

C. Topological Qubit system

One of the biggest challanges in quantum computing is the quantum decoherence, the tendency of qubits to loose their quantum state due to environmental noise. Traditional qubits (like superconducting qubits or trapped ions) require error correction mechanism, which puts unnecessary load over the computational resources. Whereas topological qubits provide intrinsic error protection due to the way quantum information is stored in them.

Topological qubits are based on anyons, a special type of quasiparticle which exists in 2D topological materials. Anayons exists in certain topological states of matter, these particles have unique property : When one anion moves around another, the quantum state of the system changes in a predictable way. This movement of anion around another

anion is called Braiding. The quantum information is stored in these braided paths and not the anions themselves.

Since braiding operations do not depend upon the particles, local errors such as environmental noise do not affect the quantum information.

There are two types of anions :

- Abelian anions – these anions follow commmutative statistics which means swapping two anions only adds a phase factor to the quantum state but the final quantum state remains the same. Hence making it not much useful for quantum computing applications.
- Non-Abelian – Non-Abelian ions have a complex braiding rule, exchanging them does not just ass a phase factor but also changes the quantum state in a way that also depends upon the braiding history. Which makes them ideal for quantum computing applications. One of the leading candidate for topological qubit is Majorana zero mode which is a non-abelian anions.

  Pairs of Majorana modes encode a single qubit in a non local way, making them robust against local errors.

D. Need of modification in BB84

The BB84 QKD protocol depends upon the prepration and measurements of the qubit, but if we are working with a topological qubit then the whole mechanism changes. As the BB84 protocol was supposed to be working on photonic systems, in which the photons were polarized to store quantum information and was easily transmitted through optical fibre. But in the topological qubit the way quantum information is stored is completely different from thr conventional qubit, the quantum information is stored in the braiding paths and not in any particles. Sending these topological qubit is another challange, photon based qubits can be transfered through optical fibre, but there is no clear method of transmission of topological qubit over long distances. Measuring the topological qubit is also very different from the measurement of photonic qubits.

So the sections which require modifications are :

- Prepration of the qubit
- Sending mechanism
- Measurement of the qubit

III. PROPOSED MODIFICATIONS

To modify BB84 protocol, we need to replace standard basis selection (X or Z) with braiding operations. Let's define mathematical framework for this new setup :

Topological qubits are made of anyons, which uses non-abelian braiding statistics. A logical qubit is encoded using pair of anions. Logical state $|0\rangle_L$ and $|1\rangle_L$ are determined by fusion outcomes :

$$\psi_1 \times \psi_2 = I(\text{Logical}|0\rangle_L)$$

$$\psi_1 \times \psi_2 = \psi(\text{Logical}|1\rangle_L)$$

where I represents the vacuum state (fusion to no particles).

And ψ is a non-trivial fusion outcome.

The basis of measurement in standard BB84 protocol are:

- Z-basis = $|0\rangle, |1\rangle$
- X-basis = $|+\rangle, |-\rangle$

For topological qubit we redefine these basis with braiding operations.

The fundamental braiding operation is

$$B = e^{i\theta\sigma x}$$

B is unitary operator for braiding,

θ is a topological phase

Now we define,

- Z-basis = Logical states without Braiding

$$|0\rangle_L, |1\rangle_L$$

- X-basis = Logical states obtained by $\pi/4$ braiding operation :

$$|+\rangle_L = B_{\pi/4}|0\rangle_L,$$

$$|-\rangle_L = B_{\pi/4}|1\rangle_L$$

Thus instead of randomly choosing Z or X , Alice and Bob can perform controlled braiding operation to decide the basis.

Final BB84 protocol with braiding based basis selection.

1 Alice prepares qubits :

  She uses anyon pairs to encode Z-basis states ($|0\rangle_L, |1\rangle_L$).

  Applies braiding $B_{\pi/4,}$ with 50% probability to create X-basis states.

2 Now Alice transfers the topological qubit throught protected topological medium for small distances. Whereas for long distances she creates a polarized photon which has the quantum information of the topological qubit and sends it through optical fibre, and on the other end Bob receives the polarized photon and prepares a new topological qubit similar to the quantum information encoded in the photon.

3 Bob decodes basis via braiding, instead of choosing basis randomly he uses counter braiding operations for checking fusion outcome.

4 Alice and bob compare their basis choices over a classical channel, they sidcard mismatched basis results. They apply error correction and privacy amplification to remove eavesdropper influence.

Iς. SIMULATIONS AND RESULTS

To validate the efficiency of our proposed topological BB84 protocol, w've created a simulation of this Quantum Key Distribution protocol , we used python simulating the basis selection using braiding operations and error detection

through fusion measurement and hence calculated the error rate based on the fusion outcmes.

- We have considered braiding oberator B(θ) as rotation matrix.
- Fusion measurement :

Probability of vaccum (correct measurement) = 90%

Probability of non-trival (error) = 10%

Simulation Methodology

1. Alice and Bob randomly choose a basis (X or Z)
2. Alice applice braiding of X-basis qubits
3. Bob applies inverse braiding operation for X-basis qubits.
4. Bob performs fusion measurement and stores the result.
5. Calculation of error rate :

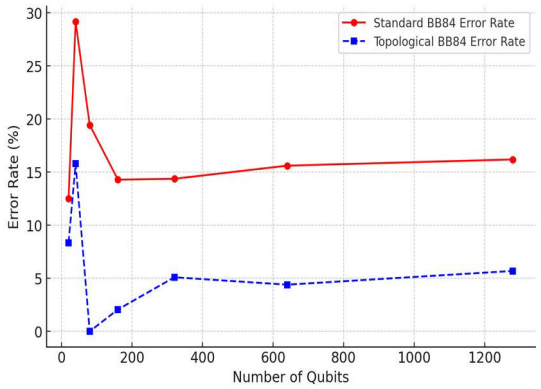
   Error rate = no. of errors / Total matching basis pairs

Results and Analysis:

After running the simulation at the strength of 100 qubits for several times following are the observations:

- Matching basis pairs : 48 – 52
- Errors detected : 4 – 10
- Final secret key length : 45 – 55
- Error rate : 7% - 10%

The error rate in this protocol remains very low because of the fusion measurement system, which aligns with the theoretical predictions.



A. This graph explains the behaviour of error rates according to the number of qubits in the topological BB84 and Standard BB84.

COMPARISION OF BB84 & TOPOLOGICAL BB84

Criteria	BB84	Topological BB84
Error rate (%)	10-12%	7-10%
Error source	Measurement errors due to environmental noise	Fusion measurement errors
Security	Vulnerable to certain attacks	High security due to topological protection
Scalability	Requires high quality quantum memory.	More scalability due to error resistance.
Implementation complexity	Easier with existing quantum hardware.	Requires topological qubits which are harder to build.

ς. Future aspect

This researcher places the first step towards the integration on Quantum Key Distribution and Topological qubits, by modifying the standard BB84 protocol. In this modification we have tried to take advantage of error resilience of topological qubit, there are still areas that need further exploration to make is practical for the real world applicaton.

One such key area would be reducing errors in fusion measurements. While topological qubits are resistant to decoherence, measurement errors still exists. Future work could focus on inmroving these fusion processes or developing a better error correcting technique that work specifically for this topological protocols.

Another arey for further exploration is testing this protocol on actual quantum hardware. Right now the topological qubits are based on Majorana fermions which is still being developed in labs. The next step would be to collaborate with experimental researchers working on topological quantum processors to see how well this modified BB84 protocol performs in real world.

For using topological BB84 protocol we need to be able to send qubits to longer distances which is not practical yet so the area of development can be either making the transfer of topological qubit over long distances possible or exploring new ways for the transfer of the quantum information of the topological qubit.

Finally, expanding this research to other QKD protocols (such as B92, E91, and MDI-QKD) could provide a more comprehensive understanding of topological qubits in quantum cryptography. Additionally, building better simulation tools for topological QKD would help researchers refine and optimize these protocols before real-world deployment.

References

[1] *Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179. Retrieved from https://arxiv.org/abs/2312.05609*

[2] Scarani, V., Acín, A., Ribordy, G., & Gisin, N. (2004). *Quantum cryptography protocols beyond BB84.* Physical Review Letters, 92(5), 057901.

[3] Renner, R., Gisin, N., & Kraus, B. (2005). *An information-theoretic security proof for QKD protocols.* Physical Review A, 72(1), 012332. Retrieved from https://arxiv.org/abs/quant-ph/0502064

[4] Shor, P. W., & Preskill, J. (2000). *Simple proof of security of the BB84 quantum key distribution protocol.* Physical Review Letters, 85(2), 441–444. Retrieved from https://arxiv.org/abs/quant-ph/0003004

[5] Nayak, C., Simon, S. H., Stern, A., Freedman, M., & Das Sarma, S. (2008). *Non-Abelian anyons and topological quantum computation.* Reviews of Modern Physics, 80(3), 1083–1159. Retrieved from https://arxiv.org/abs/2410.13547

[6] Microsoft Quantum Team. (2025). *Topological qubits: A new approach to quantum computing.* Microsoft Quantum Blog. Retrieved from https://quantum.microsoft.com/en-us/insights/education/concepts/topological-qubits

[7] M. O'Neill, "Experts weigh in on Microsoft's topological qubit claim," *Phys. World*, 2025. Available: https://physicsworld.com/a/experts-weigh-in-on-microsofts-topological-qubit-claim/