UDC 004.056.55

Construction of secure direct communication protocols in the topological quantum computing model

Andrii Fesenko[1], Anastasia Zatsarenko[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

This paper presents an implementation of the six-state quantum key distribution protocol and the LM05 quantum secure direct communication protocol based on anyonic systems. We consider the representation of logical qubits and operations of the protocol through the manipulation of abelian anyons of the Kitaev model and non-abelian Fibonacci anyons. A comparative analysis of the anyonic implementations with the classical photonic approach is carried out in terms of key characteristics such as accuracy, stability, and complexity. The advantages and experimental challenges of anyonic platforms for quantum information exchange are discussed.

Keywords: quantum secure direct communication, topological quantum computing, Kitaev anyons, Fibonacci anyons

Introduction

The development of quantum computing makes some primitives of traditional cryptography vulnerable and requires new approaches to secure communication, while the fundamental problem of decoherence limits the creation of reliable quantum devices. One promising way to overcome decoherence is topological quantum computing — a paradigm proposed by Alexei Kitaev in 1997 [1], which encodes quantum information in global topological properties of the system that are resistant to local perturbations.

In the field of quantum communication, quantum secure direct communication protocols provide an alternative to traditional quantum key distribution methods. One such protocol is the LM05 protocol [2], which enables the deterministic transmission of secret information or the establishment of a key via a two-way quantum channel without using entanglement.

This work aims to develop LM05 protocol implementations based on abelian Kitaev anyons and nonabelian Fibonacci anyons, as well as the six-state quantum key distribution protocol based on nonabelian Fibonacci anyons, and analyze their features.

1. Toolkit for Quantum Secure Direct Communication Based on Anyons

Key components of topological quantum computing are exotic quasiparticle excitations, known as anyons [3].

Definition 1. Anyons are a type of quasiparticle that can only exist in two-dimensional quantum systems. They exhibit exchange statistics that differ from those of bosons and fermions.

Exchange statistics determine how the quantum state of a system changes when two identical particles are interchanged (braided). The braiding operation, which corresponds to the exchange of positions of two anyons a and b, which then fuse into a common channel c, is mathematically described by the operator R_c^{ab}. Depending on the nature of these statistics and the fusion rules, anyons are divided into two main types:

- Abelian anyons are characterized by the fact that when they are exchanged, the system's state acquires only a phase factor $e^{i\theta}$ for some $\theta \in [0, 2\pi)$.

Example 1 (Kitaev Anyons)**.** In this model, the primary elementary excitations above the

vacuum state 1 are anyons such as the electric charge e, magnetic flux m, and their bound state — the fermion ε. The fusion rules are as follows:

$$e \times m = \varepsilon, \quad \varepsilon \times e = m, \quad \varepsilon \times m = e,$$
$$e \times e = m \times m = \varepsilon \times \varepsilon = 1.$$

These rules are deterministic, meaning the fusion always results in a specific anyon.

- Non-Abelian anyons are characterized by the fact that, when exchanged, they cause a unitary transformation of the system's state that acts on a degenerate state space.

Example 2 (Fibonacci Anyons)**.** This model contains two types of particles: the vacuum 1 and the non-Abelian anyon τ. The fusion rules are as follows:

$$\tau \times \tau = 1 + \tau.$$

These rules are nondeterministic: two τ anyons can either annihilate (result 1 — vacuum) or form a new τ anyon.

2. LM05 Quantum Secure Direct Communication Protocol Based on Kitaev Abelian Anyons

The logical qubit for Kitaev anyons is defined through two basic physical states of the system [4]:

- The vacuum state $|0\rangle$, which corresponds to the absence of any nontrivial excitations.
- The state $|\varepsilon\rangle$, which contains exactly one fermionic anyon ε, a bound state of electric charge e and magnetic flux m ($\varepsilon = e \times m$).

These two states $|0\rangle$ and $|\varepsilon\rangle$ form the computational Z-basis, on which the following basic operations act:

- The identity operation $U_0 = I$ requires no action; the state remains unchanged:

$$U_0 |0\rangle = |0\rangle, \quad U_0 |\varepsilon\rangle = |\varepsilon\rangle.$$

- The operation U_1 (phase shift σ_z) acts nontrivially only on the state $|\varepsilon\rangle$, imparting a phase of -1 to it. This is achieved by braiding the anyon ε around itself, using the property $R_1^{\varepsilon\varepsilon} = -1$. The state $|0\rangle$ remains unchanged:

$$U_1 |0\rangle = |0\rangle, \quad U_1 |\varepsilon\rangle = -|\varepsilon\rangle.$$

- The operation U_2 (bit flip σ_x) swaps the states $|0\rangle$ and $|\varepsilon\rangle$. Physically, this is realized by locally creating a fermion ε (if the system is in state $|0\rangle$, according to $1 \times \varepsilon = \varepsilon$) or annihilating it (if the system is in state $|\varepsilon\rangle$, according to $\varepsilon \times \varepsilon = 1$):

$$U_2 |0\rangle = |\varepsilon\rangle, \quad U_2 |\varepsilon\rangle = |0\rangle.$$

The implementation of the LM05 protocol for Kitaev Abelian anyons using this encoding and basic operations is provided in Protocol 1.

Algorithm 1.

1. *Preparation (Bob):*
   Bob creates a sequence of anyonic qubits, randomly choosing for each the preparation basis and a specific state within that basis:
   - *In the Z-basis, one of the states is prepared: $|0\rangle$ (vacuum) or $|\varepsilon\rangle$ (state with one fermion).*
   - *In the X-basis, one of the states determined by the action of the Hadamard operator H on the Z-basis states is prepared:*

$$|u\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |\varepsilon\rangle),$$
$$|v\rangle = H|\varepsilon\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |\varepsilon\rangle).$$

   To realize the H operator in the context of Kitaev anyon model, braiding and fusion operations alone are insufficient; additional non-topological methods are required [5].
2. *First Transmission (Quantum Channel):*
   Bob sends the prepared anyonic systems to Alice via the quantum channel.
3. *Encoding/Control (Alice):*
   Alice randomly chooses one of two modes for each received qubit:
   - *Control Mode: She measures the qubit's state in a randomly chosen basis (Z or X) to check the channel's security.*
   - *Encoding Mode: She encodes one bit of her secret message $m \in \{0, 1\}$ by applying the corresponding unitary operation to the qubit:*
     If $m = 0$: she applies operation U_0 (the state does not change).
     If $m = 1$: she applies the sequence of operations U_1U_2. As a result of this transformation, the states change ac-

cording to the following principle:

$$U_1U_2\left|0\right\rangle = -\left|\varepsilon\right\rangle, \quad U_1U_2\left|\varepsilon\right\rangle = \left|0\right\rangle,$$

$$U_1U_2\left|u\right\rangle = \frac{1}{\sqrt{2}}(U_1U_2\left|0\right\rangle + U_1U_2\left|\varepsilon\right\rangle) = \\ = \frac{1}{\sqrt{2}}(-\left|\varepsilon\right\rangle + \left|0\right\rangle) = \\ = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|\varepsilon\right\rangle) = \left|v\right\rangle,$$

$$U_1U_2\left|v\right\rangle = \frac{1}{\sqrt{2}}(U_1U_2\left|0\right\rangle - U_1U_2\left|\varepsilon\right\rangle) = \\ = \frac{1}{\sqrt{2}}(-\left|\varepsilon\right\rangle - \left|0\right\rangle) = \\ = -\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|\varepsilon\right\rangle) = -\left|u\right\rangle.$$

4. *Second Transmission (Quantum Channel): Alice sends the modified sequence of anyonic systems back to Bob via the quantum channel.*
5. *Decoding Phase (Bob): Bob measures each received qubit in the same basis in which it was prepared. By comparing the measurement results with the expected results for operations U_0 and U_1U_2, Bob unambiguously determines the bit m encoded by Alice.*
6. *Classical Verification (Classical Channel): Alice publicly announces which qubits were control qubits and which were encoding qubits. For the control qubits, they compare the results (where the bases matched) and estimate the Quantum Bit Error Rate (QBER). If the error rate is low, then the sequence of bits that Bob obtained in encoding mode is considered the securely transmitted message.*

Thus, the constructed algorithm shows how the deterministic quantum communication protocol LM05 can be adapted for implementation on the Kitaev Abelian anyon platform using their specific states and operations.

3. Implementation of the Six-State Quantum Key Distribution Protocol Using Fibonacci Anyons

A qubit on Fibonacci anyons τ is encoded in the states of three such anyons with a total topological charge τ. The basis states are defined by the fusion channel a of the first pair of anyons in diagrammatic notation $((\bullet,\bullet)_a,\bullet)_1$, where $\bullet$ denotes a τ-anyon [6]:

- $a = 0$: the first pair of anyons fuses into the vacuum channel;
- $a = 1$: the first pair of anyons fuses into the τ channel.

Changing the qubit state is achieved by braiding adjacent anyons. The basic exchange operations σ_1 (between the first and second) and σ_2 (between the second and third) are represented in the corresponding state space by unitary matrices:

$$\sigma_1 = \begin{pmatrix} e^{\frac{-4\pi i}{5}} & 0 \\ 0 & e^{\frac{3\pi i}{5}} \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} \varphi^{-1}e^{\frac{4\pi i}{5}} & \varphi^{-\frac{1}{2}}e^{\frac{-3\pi i}{5}} \\ \varphi^{-\frac{1}{2}}e^{\frac{-3\pi i}{5}} & -\varphi^{-1} \end{pmatrix},$$

where $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio constant. Combinations of these elementary braids and their inverses allow for the realization of arbitrary quantum operations.

The six-state quantum key distribution protocol [7], an extension of the BB84 protocol that incorporates an additional measurement basis, is theoretically more resistant to certain attacks. To operate in three bases on the non-Abelian Fibonacci anyon platform, it is essential to leverage their unique properties, namely the ability to perform the necessary quantum operations through braiding.

Thus, the protocol uses three mutually unbiased bases: the computational (Z), diagonal (X), and circular (Y) bases. States in these bases are defined as follows:

- The Z-basis consists of states $\left|0\right\rangle_\tau$ and $\left|1\right\rangle_\tau$, where $\left|0\right\rangle_\tau = ((\bullet,\bullet)_0,\bullet)_1, \left|1\right\rangle_\tau = ((\bullet,\bullet)_1,\bullet)_1$.
- The X-basis states are obtained by applying an approximated Hadamard operator H to the Z-basis states.
- The Y-basis states are obtained by sequentially applying approximated $S^\dagger$ and H operators to the Z-basis states.

Preparing states in these bases requires applying the corresponding unitary transformations, which, in turn, are approximated by sequences of Fibonacci anyon braids. One of the key operations necessary for constructing the protocol is the Hadamard gate H, which is mathematically defined as follows:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Figure 1 shows one sequence of elementary braids that approximates the H gate with high precision. This sequence consists of 34 elementary braiding operations and is written as follows:

$$B_H = \sigma_2^{-4}\sigma_1^{-4}\sigma_2^2\sigma_1^4\sigma_2^2\sigma_1^{-2}\sigma_2^{-4}\sigma_1^{-2}\sigma_2^{-2}\sigma_1^{-2}\sigma_2^{-2}\sigma_1^2\sigma_2^{-2}$$

Figure 1: Braiding approximating the Hadamard gate

The matrix approximates the target H matrix with an error of approximately 0.003. This small error value shows that the Hadamard gate can be accurately implemented using Fibonacci anyon braiding. This example shows how the fundamental operations σ_1 and σ_2 can be combined to perform complex quantum gates, which is the basis for constructing quantum algorithms on this platform.

Another important single-qubit gate is the phase gate $S^\dagger$, which corresponds to a phase rotation by $-\frac{\pi}{2}$ and is defined by the following matrix:

$$S^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

This gate is commonly used in quantum algorithms, especially for implementing measurements in the Y-basis.

One sequence of elementary braids $B_{S^\dagger}$, that approximates the $S^\dagger$ gate, is defined as follows:

$$B_{S^\dagger} = \sigma_2^2\sigma_1^{-4}\sigma_2^{-2}\sigma_1^2\sigma_2^2\sigma_1^4\sigma_2^{-4}\sigma_1^{-4}\sigma_2^2\sigma_1^{-2}\sigma_2^4\sigma_1^2\sigma_2^2$$

Figure 2 graphically depicts this sequence of 36 elementary operations.

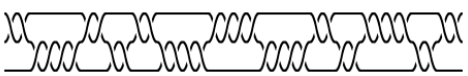

Figure 2: Braiding approximating the phase gate $S^\dagger$.

Applying this braiding sequence $B_{S^\dagger}$ to a three-anyon Fibonacci qubit yields a unitary transformation that approximates the target $S^\dagger$ matrix with an error of approximately 0.0045. Like the Hadamard gate, this example shows that it is possible to perform necessary quantum operations by physically manipulating Fibonacci anyons.

It is important to note that B_H and $B_S^\dagger$ are sequences of elementary braids (σ_1, σ_2) that only approximate ideal unitary operations. The accuracy of this approximation depends on the length and complexity of the braiding sequence.

Thus, the described methods for approximating the key H and $S^\dagger$ gates using Fibonacci anyon braiding form a necessary toolkit for constructing the six-state protocol, the step-by-step procedure of which is given in Protocol 2.

Algorithm 2.

1. Preparation Phase (Alice):

Alice creates a sequence of three-anyon qubits. For each qubit, she first randomly chooses one of three bases (Z, X, Y) and one bit of classical information (0 or 1). She then prepares the corresponding anyonic state:

- *Z-basis: If bit 0 is chosen, she prepares state $|0\rangle_\tau$; if bit 1 is chosen, state $|1\rangle_\tau$:*

$$|0\rangle_\tau = ((\bullet,\bullet)_0,\bullet)_1, \qquad |1\rangle_\tau = ((\bullet,\bullet)_1,\bullet)_1.$$

- *X-basis: If bit 0 is chosen, she prepares state $|+\rangle_\tau$, which corresponds to the result of the Hadamard operation H acting on state $|0\rangle_\tau$; if bit 1 is chosen, state $|-\rangle_\tau$, which corresponds to the result of the Hadamard operation H acting on state $|1\rangle_\tau$:*

$$|+\rangle_\tau = H|0\rangle_\tau, \qquad |-\rangle_\tau = H|1\rangle_\tau.$$

  Operation H is approximately realized by the braid sequence B_H, given by Equation 3.

- *Y-basis: If bit 0 is chosen, she prepares state $|+i\rangle_\tau$, which corresponds to the result of sequentially applying operations $S^\dagger$ and H to state $|0\rangle_\tau$; if bit 1 is chosen, state $|-i\rangle_\tau$, which corresponds to the result of sequentially applying operations $S^\dagger$ and H to state $|1\rangle_\tau$:*

$$|+i\rangle_\tau = HS^\dagger|0\rangle_\tau, \qquad |-i\rangle_\tau = HS^\dagger|1\rangle_\tau.$$

  Operation $HS^\dagger$ is approximately realized by the braid sequence $B_H B_S^\dagger$, where B_H and $B_S^\dagger$ are given by Equations 3 and 3 respectively.

Alice records the sequence of prepared states and their corresponding bases.

2. Transmission Phase (Quantum Channel):

Alice sends the prepared anyonic systems to Bob via the quantum channel. Each system carries the state of one qubit.

3. Measurement Phase (Bob):

For each received system, Bob, independently of Alice, randomly chooses one of the three measurement bases (Z, X or Y) and performs the corresponding measurement:

- *Z-basis:*
  - *If state $|0\rangle_\tau$ (vacuum) is measured, bit 0 is recorded.*
  - *If state $|1\rangle_\tau$ (anyon τ) is measured, bit 1 is recorded.*
- *X-basis:*
  - *If state $|+\rangle_\tau$ is measured, bit 0 is recorded.*
  - *If state $|-\rangle_\tau$ is measured, bit 1 is recorded.*
- *Y-basis:*
  - *If state $|+i\rangle_\tau$ is measured, bit 0 is recorded.*
  - *If state $|-i\rangle_\tau$ is measured, bit 1 is recorded.*

Bob stores the results of his measurements and the corresponding bases.

4. Classical Reconciliation Phase (Classical Channel):

After the quantum transmission, Alice and Bob use an open authenticated classical channel to reconcile the key. They compare their preparation and measurement bases for each state, discarding cases where they diverge. Results where the bases match form the sieved key. It is expected that the bases will match in approximately $\frac{1}{3}$ of cases.

5. Error Estimation and Post-Processing Phase (Classical Channel):

Alice and Bob publicly compare a random subset of the sieved key bits to calculate the Quantum Bit Error Rate (QBER).

- *If the QBER is acceptably low, they apply standard error correction and privacy amplification procedures to the remaining sieved key, obtaining the final secret key.*
- *If the QBER exceeds the security threshold, the protocol is aborted, and the potential key is discarded.*

Using Fibonacci anyons to implement the six-state protocol has potential advantages because qubits are topologically protected from local perturbations. However, the main challenge is the protocol's practical complexity. Achieving high precision in approximating the H and $S^\dagger$ gates requires very long and complex braiding sequences, which increases execution time and the probability of errors.

Despite these challenges, constructing the six-state protocol with Fibonacci anyons shows the flexibility and potential of this platform for quantum communication tasks.

4. Implementation of the LM05 Quantum Secure Direct Communication Protocol Using Fibonacci Anyons

As previously stated, the LM05 protocol is a deterministic quantum communication protocol that enables both direct secure message transmission and quantum key establishment. When implemented on a non-Abelian Fibonacci anyon platform, the protocol's security is further enhanced by the inherent topological protection of quantum information, encoded in degenerate fusion spaces, and the robustness of universal braiding operations against local perturbations.

For encoding and control within the LM05 protocol using Fibonacci anyons, two key mutually unbiased bases are utilized, formed from the logical states of a three-anyon qubit:

- The Z-basis consists of states $|0\rangle_\tau$ and $|1\rangle_\tau$, where $|0\rangle_\tau = ((\bullet,\bullet)_0,\bullet)_1, |1\rangle_\tau = ((\bullet,\bullet)_1,\bullet)_1$.
- The X-basis states are obtained by applying an approximated Hadamard operator H, implemented by the sequence of elementary braids B_H (Equation 3), to the Z-basis states..

Unlike quantum key distribution protocols, whose primary goal is to establish a shared secret from measurement results, the LM05 protocol involves an active message encoding phase. This means that Alice must apply at least two different unitary operations to the qubits she receives from Bob, which allows her to intentionally change their state.

One such fundamental operation used for encoding one of the logical values is the identity operation I, which in matrix representation is:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

One sequence of elementary braids B_I, which approximates the I gate with an error $\varepsilon \approx 1.5 \cdot 10^{-3}$, is defined as follows:

$$B_I = \sigma_2^3\sigma_1^{-2}\sigma_2^{-4}\sigma_1^2\sigma_2^4\sigma_1^2\sigma_2^{-2}\sigma_1^{-2} \sigma_2^{-4}\sigma_1^{-4}\sigma_2^{-2}\sigma_1^4\sigma_2^2\sigma_1^{-2}\sigma_2^2\sigma_1^2\sigma_2^{-2}\sigma_1^3.$$

To encode the other logical bit in the LM05 protocol using Fibonacci anyons, a combination of operations that approximates the Pauli σ_z and $i\sigma_x$ operators is used:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$i\sigma_x = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Unlike other operations that require complex approximating sequences, the σ_z operator on the Fibonacci anyon platform can be realized exactly using a short sequence of braids B_Z:

$$B_Z = \sigma^5$$

The corresponding sequence of braids B_{iX}, which approximates the $i\sigma_x$ operation with an error $\varepsilon \approx 8.6 \cdot 10^{-4}$, is defined as:

$$B_{iX} = \sigma_1^{-2}\sigma_2^{-4}\sigma_1^4\sigma_2^{-2}\sigma_1^2\sigma_2^2\sigma_1^{-2}\sigma_2^4 \sigma_1^{-2}\sigma_2^4\sigma_1^2\sigma_2^{-4}\sigma_1^2\sigma_2^{-2}\sigma_1^2\sigma_2^{-2}\sigma_1^{-2}.$$

Using this toolkit, the step-by-step procedure for the LM05 protocol is outlined in Protocol 3.

Algorithm 3.

1. Preparation Phase (Bob):

Bob creates a sequence of three-anyon qubits, randomly choosing the preparation basis and the specific state within that basis for each:

- *In the Z-basis, one of the following states is prepared:*

$$|0\rangle_\tau = ((\bullet,\bullet)_0,\bullet)_1, \quad |1\rangle_\tau = ((\bullet,\bullet)_1,\bullet)_1.$$

- *In the X-basis, one of the states defined by applying the Hadamard operation H to the Z-basis states is prepared:*

$$|+\rangle_\tau = H|0\rangle_\tau, \quad |-\rangle_\tau = H|1\rangle_\tau.$$

Operation H is approximately realized by the braid sequence B_H, given by Equation 3.

Bob records the sequence of prepared states and their corresponding bases.

2. First Transmission Phase (Quantum Channel):

Bob sends the prepared sequence of anyonic systems to Alice via the quantum channel.

3. Encoding Phase (Alice):

For each received qubit, Alice randomly selects one of two modes:

- *Control Mode: Alice measures the qubit's state in a randomly chosen basis (Z or X) to check the channel's security. She records the measurement result and the basis used for each system in this sequence.*
- *Encoding Mode: Alice encodes a bit of her secret message $m \in \{0,1\}$ by applying the corresponding unitary operation to the received anyonic qubit:*
  - *If $m = 0$, she applies the braid sequence B_I, which approximates the identity operation I. Thus, in this case, the state remains unchanged.*
  - *If $m = 1$, she applies the braid sequence $B_Z B_{iX}$, which approximates a combination of the Pauli operators σ_z and $i\sigma_x$. As a result of this transformation, the states change according to the following principle:*

$$|0\rangle_\tau \to -i|1\rangle_\tau, \quad |1\rangle_\tau \to i|0\rangle_\tau,$$
$$|+\rangle_\tau \to i|-\rangle_\tau, \quad |-\rangle_\tau \to -i|+\rangle_\tau.$$

4. Second Transmission Phase (Quantum Channel):

Alice sends the modified sequence of anyonic systems back to Bob via the quantum channel.

5. Decoding Phase (Bob):

Bob measures each received qubit in the same basis in which he prepared it and records the results. By comparing the measurement result with the expected result for operations B_I and $B_Z B_{iX}$ in the corresponding basis, Bob unambiguously determines the bit m encoded by Alice.

6. Classical Verification Phase (Classical Channel):

After the quantum transmission is complete, Alice and Bob use an open authenticated classical channel. Alice publicly announces which qubits were control qubits and which were encoding qubits.

For the control qubits, she also declares the measurement basis she used. Alice and Bob compare results in cases where they randomly chose the same basis and estimate the Quantum Bit Error Rate (QBER).

- *If the QBER is acceptably low, the sequence of bits obtained by Bob in encoding mode is considered the securely transmitted message.*
- *If the QBER exceeds the security threshold, the protocol is considered compromised and immediately aborted to ensure security, and all potentially transmitted message bits are discarded.*

Using Fibonacci anyons to implement LM05 protocol can theoretically provide the advantages of topological protection. Encoding in non-local degrees of freedom and performing operations via braiding can increase robustness against local perturbations and errors compared to photonic implementations, and the universality of braiding ensures the possibility of implementing the necessary operations.

Thus, while the implementation of the LM05 protocol with Fibonacci anyons is theoretically possible and potentially advantageous in terms of topological protection, but it faces significant practical challenges related to the precision of operation approximation and the physical control over anyons.

Therefore, the implementation of the LM05 protocol with Fibonacci anyons demonstrates the use of their universal computational properties, but it underscores the practical complexity associated with the need to approximate quantum gates with long sequences of braids.

5. Comparative analysis of anyon-based protocol implementations

The security of quantum secure direct communication protocols largely depends not only on the theoretical foundations of quantum mechanics, but also on the physical features of their implementation. One of the most significant practical problems for QSDC systems using photons as information carriers is the imperfection of single-photon sources.

However, in the transition to the implementation of quantum cryptographic protocols on anyonic platforms, the key physical properties of information carriers change dramatically. This directly affects the possibility of a PNS attack.

Lemma 1. *The protocols implemented on the platform of abelian Kitaev and nonabelian Fibonacci anyons are resistant to attacks based on splitting the multiparticle states of the storage medium, similar to the photon number splitting (PNS) attack.*

Proof. Attacks based on multiparticle state splitting, such as the PNS attack in photonic systems, exploit the ability of an attacker to imperceptibly separate some of the redundant components of a quantum signal to obtain information about the transmitted state. Such attacks require several identical or easily separable copies of the logical state in one signal.

In anyonic protocol implementations, a logical qubit is encoded by manipulating the states of anyons. Anyons are collective excitations of the system or specific topological configurations (e.g., the presence of a certain type of anyon, the fusion state of a group of anyons, or the degenerate ground state of an anyon system). This encoding defines a logical qubit as a single, complete quantum system that does not contain redundant, easily separable copies of this logical state that could be used for PNS attacks. Therefore, due to the absence of a key prerequisite for such attacks, anyonic systems are invulnerable to such attacks. ■

In addition to being resistant to PNS attacks, anyonic implementations offer a fundamental advantage in the form of internal protection against local errors due to the nature of the storage media.

Lemma 2. *Compared to implementations on standard physical qubits (e.g., photons), anyon-based QSDC protocols provide increased robustness to local physical errors and decoherence due to topological protection.*

Proof. The key advantage of topological systems lies in how quantum information is encoded. Unlike standard qubits, which store information in local properties (such as the polarisation of a photon), in anyonic systems it is encoded in global topological degrees of freedom (e.g., in the degenerate merging space of non-Abelian anyons). This nonlocality provides built-in protection against local perturbations. Since random local interactions with the environment or minor control errors cannot instantly change the global topology of the system, the encoded information remains intact. Moreover, quantum operations implemented by intertwining anyons

are also topologically invariant: their result is determined by the topology of the resulting braid, not by the exact details of the particle trajectories. Thus, the intrinsic properties of anyonic systems provide a much higher level of built-in resistance to physical errors and decoherence, reducing the need for complex external correction mechanisms, unlike standard qubits such as photons, which remain vulnerable to such effects. ■

The considered advantages of anyonic systems, such as their internal resistance to certain types of attacks and local errors, highlight their potential for practical applications in quantum cryptography. Thus, the implementations of QSDC protocols based on Kitaev and Fibonacci anyons demonstrate the potential of topological approaches for quantum communication. These approaches offer an alternative to traditional photonic methods, as summarised in Table 1.

For Kitaev Abelian anyons, basic topological manipulations, including fusion and braiding, used to implement the necessary single-qubit operations $\{U_0, U_1, U_2, U_3\}$, are inherently precise. However, to obtain a complete set of operations for constructing QSDC protocols, additional non-topological methods are required, the precision of which can vary. In contrast, non-Abelian Fibonacci anyons offer a path to universal quantum computation exclusively through braiding. Yet, the implementation of the required operations here is typically achieved by approximating them with long sequences of elementary σ_1 and σ_2 braids. Achieving high precision for such approximations may demand a significant number of braids, complicating practical implementation. For comparison, in photonic systems, the theoretical precision of operations performed using ideal optical elements is high, and universality can be achieved with an appropriate set of optical components. In practice, however, precision is significantly limited by the imperfection of these components, the accuracy of their alignment, and the overall stability of the experimental setup.

Another significant advantage, thoroughly substantiated in Lemma 2, is error resistance, particularly to local perturbations and decoherence, which is inherent to anyonic systems. For both Kitaev anyons and Fibonacci anyons, quantum information is encoded in global topological degrees of freedom. This approach means that local perturbations, which affect only a limited part of the system, cannot instantly destroy globally encoded information. A particularly high level of intrinsic robustness is characteristic of non-Abelian Fibonacci anyons, where information is encoded in degenerate fusion spaces, making the system fault-tolerant by design. In contrast, photonic qubits are extremely sensitive to interaction with the environment, leading to significant losses in the transmission channel, phase distortions, and other types of errors that require the application of active and often complex correction protocols.

In addition to protection against physical errors, the key properties of anyonic information carriers also provide resistance to attacks based on the splitting of multi-particle states, similar to the photon number splitting (PNS) attack, as proven in Lemma 1. This fundamentally distinguishes them from WCP-based photonic systems, where vulnerability to PNS attacks remains a relevant issue.

The main advantage of the photonic approach for quantum communication is its maturity, evidenced by the availability of commercial QKD protocol implementations. Anyonic platforms, on the other hand, despite being at the stage of theoretical research, show rapid development. However, their practical implementation, ensuring stable control over anyons, and precise manipulation of their braids still remain an extremely complex experimental challenge. Nevertheless, their unique advantages, such as topological protection and the potential for universal computations, open prospects for creating fundamentally new, more reliable systems for quantum communication and computation.

Conclusions

This paper develops and theoretically substantiates the implementation of the LM05 quantum secure direct communication protocol based on anyonic systems, particularly using abelian anyons of the Kitaev model and non-abelian Fibonacci anyons. Additionally, we explore the six-state quantum key distribution protocol based on non-abelian Fibonacci anyons.

A comparative analysis of these anyonic approaches is performed based on key character-

Table 1
Comparative Analysis of QSDC Protocol Implementations

Characteristic	**Kitaev anyons (Abelian)**	**Fibonacci anyons (Non-Abelian)**	**Photons (Phase Encoding)**
Physical Carrier	topological excitations (e, m, ε)	topological excitations (fusion channels of τ anyons)	single photons (in practice WCP)
Operation Accuracy	high	approximate	high (in theory)
Error Resistance	partial (Abelian statistics)	high	low
Resistance to PNS Attack	not applicable	not applicable	low
Universality	limited	yes	yes (with appropriate set of operations)
Implementation Complexity	high	very high	medium

istics such as operational accuracy, system stability, and implementation complexity. The results demonstrate the potential of anyonic platforms for building quantum communication systems that are more resistant to local disturbances and certain types of attacks.

References

[1] A. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, p. 2–30, Jan. 2003.

[2] M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," *Phys. Rev. Lett.*, vol. 94, p. 140501, Apr 2005.

[3] A. Kitaev, "Anyons in an exactly solved model and beyond," *Annals of Physics*, vol. 321, p. 2–111, Jan. 2006.

[4] Y. Shen, C.-C. Zhou, and F.-L. Zhang, "Realization of quantum secure direct communication by kitaev abelian anyons," *Physics Letters A*, vol. 525, p. 129941, Nov. 2024.

[5] J. R. Wootton and J. K. Pachos, "Universal quantum computation with abelian anyon models," *Electronic Notes in Theoretical Computer Science*, vol. 270, no. 2, pp. 209–218, 2011.

[6] B. Field and T. Simula, "Introduction to topological quantum computation with non-abelian anyons," *Quantum Science and Technology*, vol. 3, p. 045004, July 2018.

[7] D. Bruss, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, p. 3018–3021, Oct. 1998.