

ПОБУДОВА ПРОТОКОЛІВ ЗАХИЩЕНОГО ПРЯМОГО ЗВ'ЯЗКУ В КВАНТОВІЙ МОДЕЛІ ТОПОЛОГІЧНИХ ОБЧИСЛЕНЬ

А. Ю. Зацаренко¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

В роботі побудовано реалізацію протоколу квантового захищеного прямого зв'язку LM05 на основі аніонних систем. Розглянуто представлення логічних кубітів та операцій протоколу через маніпуляції абелевими аніонами моделі Китаєва та неабелевими аніонами Фібоначчі. Проведено порівняльний аналіз аніонних реалізацій з класичним фотонним підходом щодо ключових характеристик, таких як точність, стійкість та складність. Обговорено переваги та експериментальні виклики аніонних платформ для квантового обміну інформації.

Ключові слова: квантовий захищений прямий зв'язок, топологічні квантові обчислення, аніони Китаєва, аніони Фібоначчі

Вступ

Розвиток квантових обчислень робить вразливими деякі примітиви класичної криптографії та вимагає нових підходів до безпечної комунікації, тоді як фундаментальна проблема декогеренції обмежує створення надійних квантових пристроїв. Перспективним шляхом подолання декогеренції є топологічні квантові обчислення — парадигма, запропонована Олексієм Китаєвим у 1997 році [1], яка побудована на кодуванні квантової інформації в глобальних топологічних властивостях системи, що є стійкими до локальних збурень.

У сфері квантової комунікації, альтернативою традиційному квантовому розподілу ключа є протоколи квантового захищеного прямого зв'язку. Одним з таких є протокол LM05 [2], який дозволяє реалізувати детерміновану передачу секретної інформації або встановити ключ за допомогою двостороннього квантового каналу без використання запутаності.

Метою роботи є побудова реалізації протоколу LM05 на основі абелевих аніонів Китаєва та неабелевих аніонів Фібоначчі, а також аналіз особливостей цих підходів.

1. Інструментарій для квантового захищеного прямого зв'язку на основі аніонів

Ключовими компонентами у топологічних квантових обчисленнях є екзотичні квазічастинкові збудження, відомі як аніони [3].

Означення 1.1. Аніони — це тип квазічастинок, що можуть існувати лише у двовимірних квантових системах і демонструють статистику обміну, яка відрізняється від статистики бозонів та ферміонів.

Статистика обміну визначає, як змінюється квантовий стан системи при переміщенні (переплетенні) двох однакових частинок. Операція переплетення, що відповідає обміну позиціями двох аніонів a та b , які потім зливаються у спільний канал c , математично описується оператором R_c^{ab} . Залежно від характеру цієї статистики, а також від правил злиття, аніони поділяються на два основні типи:

- Абелеві аніони характеризуються тим, що при їх обміні стан системи набуває лише фазового множника $e^{i\theta}$ для деякого $\theta \in [0, 2\pi)$.

Приклад 1.1 (Аніони моделі Китаєва). В цій моделі основними елементарними збудженнями над вакуумним станом 1 є аніони, такі як електричний заряд e , магнітний потік m та їхній зв'язаний стан — ферміон ϵ . Правила злиття:

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

Ці правила є детермінованими: в результаті злиття завжди виникає один конкретний аніон.

- Неабелеві аніони характеризуються тим, що при їх обміні стан системи зазнає унітарного перетворення, яке діє на виродженому просторі станів.

Приклад 1.2 (Аніони Фібоначчі). Модель містить два типи частинок: вакуум 1 та неабелевий аніон τ . Правила злиття:

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

Ці правила є недетермінованими: два аніони τ можуть або анігілювати (результат 1 — вакуум), або утворити новий аніон τ .

2. Протокол квантового захищеного прямого зв'язку LM05 на основі абелевих аніонів Китаєва

Логічний кубіт для аніонів Китаєва визначається через два базових фізичних стани системи [4]:

- Вакуумний стан $|0\rangle$, який відповідає відсутності будь-яких нетривіальних збуджень.
- Стан $|\epsilon\rangle$, що містить рівно один ферміонний аніон ϵ , який є зв'язаним станом електричного заряду e та магнітного потоку m ($\epsilon = e \times m$).

Ці два стани $|0\rangle$ та $|\epsilon\rangle$ формують обчислювальний Z -базис, на який діють наступні базові операції:

- Тотожна операція $U_0 = I$ — не потребує жодних дій, стан залишається незмінним:

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

- Операція U_1 (фазовий зсув σ_z) — діє нетривіально лише на стан $|\epsilon\rangle$, надаючи йому фазу -1 . Це досягається шляхом переплетення аніона ϵ навколо самого себе, використовуючи властивість $R_1^{\epsilon\epsilon} = -1$. Стан $|0\rangle$ залишається незмінним:

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

- Операція U_2 (бітовий зсув σ_x) — взаємозамінює стани $|0\rangle$ та $|\epsilon\rangle$. Фізично це реалізується шляхом локального створення ферміона ϵ (якщо система у стані $|0\rangle$, згідно з $1 \times \epsilon = \epsilon$) або його анігіляції (якщо система у стані $|\epsilon\rangle$, згідно з $\epsilon \times \epsilon = 1$):

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

Реалізація протоколу LM05 для абелевих аніонів Китаєва з використанням цього кодування та базових операцій наведена в Протоколі 1.

Протокол 1.

1. Підготовка (Боб):

Боб створює послідовність аніонних кубітів, випадково обираючи для кожного з них базис підготовки та конкретний стан у цьому базисі:

- У Z -базисі готується один із станів: $|0\rangle$ (вакуум) або $|\epsilon\rangle$ (стан з одним ферміоном).
- У X -базисі готується один зі станів, які визначаються через дію оператора Адамара H на стани Z -базису:

$$|u\rangle = H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |\epsilon\rangle),$$

$$|v\rangle = H |\epsilon\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |\epsilon\rangle).$$

Для реалізації оператора H у контексті аніонів моделі Китаєва недостатньо лише операцій переплетення та злиття, необхідне застосування додаткових нетопологічних методів [5].

2. Перша передача (квантовий канал):

Боб надсилає підготовлені аніонні системи Алісі через квантовий канал.

3. Кодування/контроль (Аліса):

Аліса для кожного отриманого кубіта випадково обирає один з двох режимів:

- Режим контролю: вимірює стан кубіта у випадково обраному базисі (Z або X) для перевірки безпеки каналу.
- Режим кодування: кодує один біт свого секретного повідомлення $m \in \{0, 1\}$, застосовуючи до кубіта відповідну унітарну операцію:

Якщо $m = 0$: застосовує операцію U_0 (стан не змінюється).

Якщо $m = 1$: застосовує послідовність операцій $U_1 U_2$. В результаті цього перетворення стани змінюються за наступним принципом:

$$U_1 U_2 |0\rangle = -|\epsilon\rangle, \quad U_1 U_2 |\epsilon\rangle = |0\rangle,$$

$$U_1 U_2 |u\rangle = \frac{1}{\sqrt{2}} (U_1 U_2 |0\rangle + U_1 U_2 |\epsilon\rangle) =$$

$$= \frac{1}{\sqrt{2}} (-|\epsilon\rangle + |0\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |\epsilon\rangle) = |v\rangle,$$

$$U_1 U_2 |v\rangle = \frac{1}{\sqrt{2}} (U_1 U_2 |0\rangle - U_1 U_2 |\epsilon\rangle) =$$

$$= \frac{1}{\sqrt{2}} (-|\epsilon\rangle - |0\rangle) = -\frac{1}{\sqrt{2}} (|0\rangle + |\epsilon\rangle) = -|u\rangle.$$

4. Друга передача (квантовий канал):

Аліса надсилає змінену послідовність аніонних систем назад Бобу через квантовий канал.

5. Етап декодування (Боб):

Боб вимірює кожен отриманий кубіт у тому ж базисі, в якому він його готував. Порівнюючи результат вимірювання з очікуваним результатом для операцій U_0 та $U_1 U_2$, Боб однозначно визначає біт m , закодований Алісою.

6. Класична перевірка (класичний канал):

Аліса публічно повідомляє, які кубіти були контрольні, а які кодувальні. Для контрольних кубітів вони порівнюють результати (де базиси збіглися) та оцінюють рівень квантових бітових помилок QBER. Якщо рівень помилок низький, послідовність бітів, отриманих Бобом у режимі кодування, вважається безпечно переданим повідомленням.

Таким чином, побудований алгоритм демонструє, як протокол детермінованого квантового зв'язку LM05 може бути адаптований для реалізації на платформі абелевих аніонів Китаєва з використанням їхніх специфічних станів та операцій.

3. Протокол квантового захищеного прямого зв'язку LM05 на аніонах Фібоначчі

Кубіт на аніонах Фібоначчі τ кодується у станах трьох таких аніонів із загальним топологічним зарядом τ . Базисні стани визначаються каналом злиття a першої пари аніонів у діаграмній нотації $((\bullet, \bullet)_a, \bullet)_1$, де $\bullet$ позначає τ -аніон [6]:

- $a = 0$: перша пара аніонів зливається у вакуумний канал;
- $a = 1$: перша пара аніонів зливається у канал τ .

Зміна стану кубіта досягається переплетенням сусідніх аніонів. Базові операції обміну σ_1 (між 1-м і 2-м) та σ_2 (між 2-м і 3-м) представлені у відповідному просторі станів унітарними матрицями:

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

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

де $\phi = \frac{1+\sqrt{5}}{2}$ — константа золотого перерізу. Комбінації цих елементарних переплетень та їх обернених дозволяють реалізовувати довільні квантові операції.

З використанням цього інструментарію покрокова процедура протоколу LM05 наведена в Протоколі 2:

Протокол 2.

1. Підготовка (Боб):

Боб створює послідовність 3-аніонних кубітів, випадково обираючи для кожного з них базис підготовки та конкретний стан у цьому базисі:

- У Z -базисі готується один із станів:

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

- У X -базисі готується один зі станів, які визначаються через дію оператора Адама-ра H на стани Z -базису:

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

Оператор H реалізується наближено послідовністю переплетень B_H :

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

2. Перша передача (квантовий канал):

Боб надсилає підготовлені аніонні системи Алісі через квантовий канал.

3. Кодування/контроль (Аліса):

Аліса для кожного отриманого кубіта випадково обирає один з двох режимів:

- Режим контролю: вимірює стан кубіта у випадково обраному базисі (Z або X) для перевірки безпеки каналу.
- Режим кодування: кодує біт свого секретного повідомлення $m \in \{0, 1\}$, застосовуючи до кубіта відповідну унітарну операцію: Якщо $m = 0$: застосовує операцію B_I , що апроксимує тотожну операцію I :

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

Якщо $m = 1$: застосовує операції $B_Z B_{IX}$, що апроксимує комбінацію операторів Паулі σ_z

та $i\sigma_x$:

$$B_Z = \sigma^5,$$

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

В результаті цього перетворення стани змінюються за наступним принципом:

$$|0\rangle_\tau \rightarrow -i |1\rangle_\tau, \quad |1\rangle_\tau \rightarrow i |0\rangle_\tau,$$

$$|+\rangle_\tau \rightarrow i |-\rangle_\tau, \quad |-\rangle_\tau \rightarrow -i |+\rangle_\tau.$$

4. Друга передача (квантовий канал):

Аліса надсилає змінену послідовність аніонних систем назад Бобу через квантовий канал.

5. Етап декодування (Боб):

Боб вимірює кожен отриманий кубіт у тому ж базисі, в якому він його готував. Порівнюючи результат вимірювання з очікуваним результатом для операцій B_I та $B_Z B_{IX}$, Боб однозначно визначає біт m , закодований Алісою.

6. Класична перевірка (класичний канал):

Аліса публічно повідомляє, які кубіти були контрольні, а які кодувальні. Для контрольних кубітів вони порівнюють результати (де базиси збіглися) та оцінюють рівень квантових бітових помилок QBER. Якщо рівень помилок низький, послідовність бітів, отриманих Бобом у режимі кодування, вважається безпечно переданим повідомленням.

Отже, реалізація протоколу LM05 на аніонах Фібоначчі демонструє використання їх універсальних обчислювальних властивостей, але підкреслює практичну складність, пов'язану з необхідністю апроксимації квантових вентилів довгими послідовностями переплетень.

4. Порівняльний аналіз реалізацій протоколу LM05

Реалізації протоколу LM05 на абелевих аніонах Китаєва та неабелевих аніонах Фібоначчі демонструють потенціал топологічних систем для квантової комунікації, пропонуючи альтернативу традиційним фотонним підходам (Таблиця 1). Завдяки нелокальному кодуванню інформації в топологічних ступенях свободи, вони пропонують вищий рівень стійкості до локальних збурень, особливо у випадку неабелевих аніонів.

Переплетення та злиття абелевих аніонів моделі Китаєва в поєднанні з нетопологічними методами дозволяють реалізувати необхідні для більшості протоколів QSDC операції з високою точністю. У випадку неабелевих аніонів Фібоначчі, необхідні для LM05 операції реалізуються лише наближено довгими послідовностями переплетень, що знижує точність та ускладнює реалізацію. Проте, фундаментальною перевагою цих аніонів є їхня універсальність: їх переплетення дозволяють реалізувати будь-які квантові операції та алгоритми. Однак, фізична реалізація, контроль над аніонами та процесами їх переплетення

Таблиця 1. Порівняльний аналіз реалізацій протоколу LM05

Характеристика	аніони Китаєва (абелеві)	аніони Фібоначчі (неабелеві)	фотони (фазове кодування)
Фізичний носій	топологічні збудження (e, m, ϵ)	топологічні збудження (канали злиття аніонів τ)	слабкі когерентні імпульси
Точність операцій	висока	наближена	висока (в теорії)
Стійкість до помилок	часткова (абелева статистика)	висока	низька
Стійкість до PNS атаки	не застосовується	не застосовується	низька
Універсальність	обмежена	так	так (для окремих методів)
Складність реалізації	висока	дуже висока	низька

залишається надзвичайно складним експериментальним завданням.

Окрім потенційного топологічного захисту від помилок, аніонні системи пропонують ще одну фундаментальну перевагу у безпеці: їхня природа неподільних квазічастинок не робить їх вразливими до атак розщеплення числа фотонів (PNS), що є актуальною загрозою для реалізацій квантової комунікації, які базуються на слабких когерентних імпульсах.

Таким чином, хоча реалізація протоколів квантового захищеного прямого зв'язку на аніонних платформах наразі стикається зі значними практичними труднощами, вони безперечно є надзвичайно перспективним напрямком досліджень. Унікальні властивості аніонів можуть у майбутньому призвести до створення принципово нових, більш надійних та безпечних систем квантового зв'язку.

Висновки

У роботі розроблено та теоретично обґрунтовано реалізацію протоколу квантового захищеного прямого зв'язку LM05 на основі аніонних систем, зокрема з використанням абелевих аніонів моделі Китаєва та неабелевих аніонів Фібоначчі.

Проведено порівняльний аналіз цих аніонних підходів за ключовими характеристиками, такими як точність операцій, системна стійкість та складність реалізації. Результати демонструють потенціал аніонних платформ для побудови систем квантової комунікації з підвищеною стійкістю до локальних збурень та певних типів атак.

Перелік використаних джерел

1. Kitaev A. Fault-tolerant quantum computation by anyons // *Annals of Physics*. — 2003. — Січ. — Т. 303, № 1. — С. 2—30. — ISSN 0003-4916. — DOI: [10.1016/s0003-4916\(02\)00018-0](https://doi.org/10.1016/s0003-4916(02)00018-0).
2. Lucamarini M., Mancini S. Secure Deterministic Communication without Entanglement // *Phys. Rev. Lett.* — 2005. — Квіт. — Т. 94, вип. 14. — С. 140501. — DOI: [10.1103/PhysRevLett.94.140501](https://doi.org/10.1103/PhysRevLett.94.140501).
3. Kitaev A. Anyons in an exactly solved model and beyond // *Annals of Physics*. — 2006. — Січ. — Т. 321, № 1. — С. 2—111. — ISSN 0003-4916. — DOI: [10.1016/j.aop.2005.10.005](https://doi.org/10.1016/j.aop.2005.10.005).
4. Shen Y., Zhou C.-C., Zhang F.-L. Realization of quantum secure direct communication by Kitaev Abelian anyons // *Physics Letters A*. — 2024. — Листоп. — Т. 525. — С. 129941. — ISSN 0375-9601. — DOI: <https://doi.org/10.1016/j.physleta.2024.129941>.
5. Wootton J. R., Pachos J. K. Universal Quantum Computation with Abelian Anyon Models // *Electronic Notes in Theoretical Computer Science*. — 2011. — Т. 270, № 2. — С. 209—218. — ISSN 1571-0661. — DOI: <https://doi.org/10.1016/j.entcs.2011.01.032>.
6. Field B., Simola T. Introduction to topological quantum computation with non-Abelian anyons // *Quantum Science and Technology*. — 2018. — Лип. — Т. 3, № 4. — С. 045004. — ISSN 2058-9565. — DOI: [10.1088/2058-9565/aacad2](https://doi.org/10.1088/2058-9565/aacad2).