УДК 004.002
DOI https://doi.org/10.32782/tnv-tech.2024.6.2

РОЗВИТОК ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ ЗА РАХУНОК ВИКОРИСТАННЯ АЛГЕБРИ ПІДПИСІВ (SIGNATURE ALGEBRA)

Богом'я В. І. *– доктор технічних наук, професор,*
професор кафедри кібербезпеки, інформаційних технологій та економіки
Київського університету інтелектуальної власності та права
Національного університету «Одеська юридична академія»
Scopus-Author ID: 51863292100
ORCID ID: 0000-0003-4403-3130

Бараненко О. О. *– здобувач вищої освіти*
Київського університету інтелектуальної власності та права
Національного університету «Одеська юридична академія»
ORCID ID: 0009-0005-1810-8102

Жуков Є. В. *– ад'юнкт Національного університету оборони України*
ORCID ID: 0009-0002-1251-946X

Відомо, що широке впровадження квантових технологій супроводжується серйозними викликами. Основна проблема полягає в крихкості квантових станів, які можуть легко змінюватись через вплив шуму, декогеренцію або неточності у виконанні квантових операцій. Це створює високі ризики для надійності квантових обчислень, особливо в умовах сучасних пристроїв проміжного масштабу (NISQ), які мають обмежену кількість кубітів і високий рівень шумів.

У статті було проаналізовано сучасні методи квантової корекції помилок, зокрема використання алгебри підписів, її впровадження в різні протоколи, системи та перспективи розвитку.

Визначено ключова роль квантової корекції помилок. Корекція помилок є фундаментальним елементом для забезпечення стабільності квантових обчислень, особливо на шумних пристроях проміжного масштабу (NISQ).

Проаналізовано існуючий метод корекції помилок – алгебра підписів (signature algebra) як універсальний інструмент. Визначено, що алгебра підписів продемонструвала свою ефективність у визначенні та корекції помилок у реальному часі; у перевірці стабільності квантових станів та інтеграції з сучасними квантовими протоколами, такими як BB84, E91, DI-QKD, BQC, QSS та ін.

Перспективами розвитку є: подальша стандартизація алгебри підписів як інструмента для тестування та корекції помилок; її інтеграції з постквантовою криптографією для забезпечення безпеки даних у квантовій ері; у розробленні нових моделей для систем NISQ, топологічних кодів і квантових мереж.

Робота може бути використана як навчальний матеріал для студентів і дослідників, що займаються квантовими обчисленнями. Використані у роботі приклади коду демонструють, як алгебра підписів інтегрується у квантові обчислення, забезпечуючи надійність обчислень навіть у зашумлених середовищах. Запропоновані підходи можуть бути використані для створення стійких квантових систем і протоколів для криптографії, комунікацій та машинного навчання.

Ключові слова: *постквантова криптографія, алгебра підписів (signature algebra), корекція помилок, квантові обчислення, сучасні пристрої проміжного масштабу (NISQ).*

Bohomia V. I., Baranenko O. O., Zhukov E. V. Development of post-quantum cryptography accounting for the possibilities of signature algebra

It is known that the widespread implementation of quantum technologies is accompanied by significant challenges. The main issue lies in the fragility of quantum states, which can easily change due to noise, decoherence, or inaccuracies in performing quantum operations. This poses high risks to the reliability of quantum computations, especially in the context of modern intermediate-scale devices (NISQ), which have a limited number of qubits and a high level of noise.

The article analyzed modern methods of quantum error correction, in particular, the use of signature algebra, its implementation in various protocols, systems, and development prospects.

The key role of quantum error correction is identified. Error correction is a fundamental element for ensuring the stability of quantum computing, especially on noisy intermediate-scale (NISQ) devices.

The existing error correction method – signature algebra – is analyzed as a universal tool. It is determined that signature algebra has demonstrated its effectiveness in identifying and correcting errors in real time; in checking the stability of quantum states and integrating with modern quantum protocols such as BB84, E91, DI-QKD, BQC, QSS, etc.

The development prospects are: further standardization of signature algebra as a tool for testing and error correction; its integration with post-quantum cryptography to ensure data security in the quantum era; in developing new models for NISQ systems, topological codes and quantum networks.

The work can be used as a teaching material for students and researchers involved in quantum computing. The code examples used in the work demonstrate how signature algebra is integrated into quantum computing, ensuring the reliability of calculations even in noisy environments. The proposed approaches can be used to create robust quantum systems and protocols for cryptography, communications, and machine learning.

Key words: *post-quantum cryptography, signature algebra, error correction, quantum computing, modern intermediate-scale devices (NISQ).*

Постановка проблеми. Квантові обчислення є одним із найперспективніших напрямів сучасної науки та техніки, що здатен радикально змінити способи вирішення складних завдань у багатьох сферах: криптографії, оптимізації, моделюванні молекулярної динаміки та аналізі великих даних. Використовуючи принципи суперпозиції та квантової заплутаності, квантові комп'ютери забезпечують значно вищу швидкість обчислень порівняно з класичними.

Проте широке впровадження квантових технологій супроводжується серйозними викликами. Основна проблема полягає в крихкості квантових станів, які можуть легко змінюватись через вплив шуму, декогеренцію або неточності у виконанні квантових операцій. Це створює високі ризики для надійності квантових обчислень, особливо в умовах сучасних пристроїв проміжного масштабу (NISQ), які мають обмежену кількість кубітів і високий рівень шумів.

Для вирішення цих проблем розроблені методи квантової корекції помилок, які дозволяють виявляти й виправляти помилки, забезпечуючи стійкість обчислень. Одним із перспективних інструментів у цій галузі є алгебра підписів (Signature Algebra), яка надає формалізований підхід до перевірки коректності квантових станів і дозволяє локалізувати та виправляти помилки у реальному часі.

Сьогодні квантові технології також стикаються із загрозами, пов'язаними з їхнім практичним застосуванням. Наприклад, поява квантових комп'ютерів ставить під загрозу сучасні криптографічні системи, такі як RSA і ECC. Це стимулює розвиток постквантової криптографії (PQC), яка доповнюється можливостями алгебри підписів для перевірки та захисту даних.

Таким чином, дослідження у сфері квантової корекції помилок і її інтеграції з найновішими протоколами, такими як QKD, BQC, DI-QKD, а також із PQC, є критично важливими для забезпечення надійності та безпеки майбутніх квантових систем.

Аналіз останніх досліджень і публікацій. За результатом аналізу джерел інформації [1–14] авторами було проаналізовано та визначено такі особливості дослідження у сфері квантової корекції помилок.

У [1–5, 10–14] проаналізовані теоретичні аспекти квантової корекції помилок, включаючи коди Шора, Steane та алгебру підписів.

У [6–9] авторами проаналізувати типи квантових помилок і наведено особливості способів їхнього виявлення.

У [1–5] наведено методи реалізації квантової корекції на практичних платформах, таких як IBM Qiskit.

У [10–13] проаналізована сумісність алгебри підписів із найновішими квантовими протоколами, такими як BB84, DI-QKD, QSS і BQC.

У [5–10] досліджено використання алгебри підписів для підтримки постквантової криптографії (PQC).

Проаналізувати перспективи застосування алгебри підписів у реальних квантових системах, включаючи NISQ-пристрої, гібридні квантово-класичні системи, квантові датчики та мережі.

Але у цих дослідженнях остається не повністю визначеними питання особливостей квантової корекції, а саме для забезпечення стабільності квантових обчислень, особливо на шумних пристроях проміжного масштабу (NISQ).

Мета статті. Тому метою статті є дослідження у сфері квантової корекції помилок і її інтеграції з найновішими протоколами щодо забезпечення надійності та безпеки майбутніх квантових систем.

При цьому актуальною є тема: «Розвиток постквантової криптографії за рахунок можливостей алгебри підписів».

Методи досліджень. Одним із фундаментальних підходів до виправлення помилок у квантових системах є використання спеціальних кодів (Шора, Стена, топологічних кодів) [5, 7, 9]. Вони дозволяють захищати квантову інформацію шляхом розширення одного логічного кубіта до більшої кількості фізичних кубітів.

Код Шора є першим розробленим квантовим кодом і забезпечує захист від двох основних типів помилок: фліп біта та фазовий зсув. Він використовує дев'ять фізичних кубітів для представлення одного логічного кубіта. Кодовані стани виглядають наступним чином [1, 2].

$$|0_L\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)^{\otimes 3}, |1_L\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)^{\otimes 3}.$$

Механізм функціонування коду Шора полягає в наступному [5, 6]:

1. У кодуванні, коли логічний стан перетворюється на дев'ять фізичних кубітів.
2. У детекції, коли стабілізатори, такі як Z_1 та Z_2 або X_2 та X_3, виявляють помилки, не руйнуючи квантовий стан.
3. У корекції, коли виправлення виконується шляхом застосування зворотних операцій для відповідного типу помилки.

Код Steane базується на класичному коді Хемінга і використовує сім фізичних кубітів для одного логічного. Він забезпечує ефективний захист від помилок і дозволяє одночасно виявляти бітові та фазові зсуви. Кодованими станами є [3, 7].

$$|0_L\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |1111111\rangle), \qquad |1_L\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle - |1111111\rangle).$$

Топологічні коди (surface codes). Топологічні коди використовують геометричні властивості квантових систем для локалізації помилок. Вони є перспективними для апаратної реалізації на квантових комп'ютерах через їхню стійкість до локальних шумів.

Практична реалізація на квантових воротах. Квантові ворота є основними елементами обчислень у квантових системах. Реалізація корекції помилок базується на використанні таких воріт, як CNOT, Hadamard, і Pauli.

CNOT (Controlled-NOT). CNOT-ворота створюють кореляцію між двома кубітами, що необхідно для виявлення та виправлення помилок [11]. Оператор CNOT виконує перетворення

$$|a, b\rangle \rightarrow |a, a \oplus b\rangle.$$

Hadamard (H). Ворота Hadamard створюють суперпозиції й дозволяють переходити між базисами [12]

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

Оператори Паулі (X, Y, Z). Оператори Паулі відповідають за обертання та фазові зміщення [13]

$$X: \text{фліп біта } (X|0\rangle - |1\rangle);$$

$$Z: \text{фазовий зсув } (Z|+\rangle - |-\rangle).$$

Приклад коду Шора з CNOT і Hadamard наведений на рис. 1.

```
from qiskit import QuantumCircuit, Aer, execute
from qiskit.visualization import plot_histogram

# Створення квантового ланцюга
qc = QuantumCircuit(3, 1)

# Кодування
qc.h(0)
qc.cx(0, 1)
qc.cx(0, 2)

# Внесення помилки
qc.x(1)  # фліп біта

# Корекція помилки
qc.cx(0, 1)
qc.cx(0, 2)
qc.ccx(1, 2, 0)

# Вимірювання
qc.measure(0, 0)

# Симуляція
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, simulator).result()
counts = result.get_counts()
plot_histogram(counts)
```

Рис. 1. Приклад коду Шора з CNOT і Hadamard

IBM Qiskit пропонує платформу для моделювання та тестування алгоритмів квантової корекції помилок [9, 10].

Реалізація квантової корекції помилок можлива завдяки розробці спеціалізованих кодів і використанню квантових воріт. Тестування на платформах, таких як IBM Qiskit, демонструє практичну ефективність цих методів. Впровадження таких підходів на реальних пристроях дозволить забезпечити стабільність і точність квантових обчислень у майбутньому.

Виклад основного матеріалу дослідження. Квантові обчислення складаються з послідовності операцій, кожна з яких змінює стан квантової системи. Для забезпечення точності обчислень необхідний контроль послідовностей, який дозволяє виявляти помилки на будь-якому етапі та коригувати їх у режимі реального часу. У цьому контексті алгебра підписів виступає інструментом для формалізації та перевірки станів системи.

1. Контроль послідовностей у квантових системах з використанням алгебри підписів

Контроль послідовностей у квантових обчисленнях базується на наступних принципах:

1. Відстеження стану системи. Кожен стан системи описується у вигляді підпису *SSS*, що представляє вектор стану кубітів [3, 13].

$$S=\{s_1, s_2, \ldots, s_n\},$$

де s – стан і-го кубіта.

2. Верифікація операцій. Кожна операція, виконана над системою, змінює її стан згідно з очікуваними підписами. Якщо стан після операції не відповідає очікуваному, це сигналізує про наявність помилки.

3. Локалізація помилок. Використання стабілізаторів дозволяє визначити, в якому місці послідовності виникла помилка.

Алгебра підписів описує зміни стану системи за допомогою операторів і стабілізаторів. Елементами алгебри підписів є такі:

1. Підпис: Поточний стан кубітів, описаний стабілізаторами. Наприклад, стан заплутаних кубітів [5, 9]:

$$S=\{Z_1, Z_2, X_1, X_2\}.$$

2. Оператори: Моделюють зміни стану системи. Для воріт Hadamard справедливо [3–5, 9]

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

3. Контрольні точки: Встановлюються на кожному етапі обчислення для перевірки відповідності стабілізаторів [10, 13].

$$S_{\text{initial}} \rightarrow S_{\text{intermediate}} \rightarrow S_{\text{final}}.$$

Алгоритм контролю складається з декількох етапів [14]:

1. Ініціалізація, коли система отримує початковий підпис S-initial.
2. Операції, коли кожна операція змінює підпис згідно з очікуваним перетворенням.
3. Перевірка, коли на кожному етапі система порівнює поточний підпис із очікуваним.

Приклад контролю послідовностей у квантовій системі наведений на рис. 2.

Опис роботи коду полягає у ініціалізації (створюється заплутаний стан); у внесенні помилки (кубіт 1 зазнає фазового зсуву Z) та відновлення (стабілізатори використовуються для корекції стану).

Контроль послідовностей із використанням алгебри підписів забезпечує точність і надійність квантових обчислень. Інтеграція цього підходу з платформами, такими як IBM Qiskit, дозволяє моделювати складні сценарії й забезпечувати ефективне виправлення помилок у реальному часі.

```python
from qiskit import QuantumCircuit, Aer, execute
from qiskit.visualization import plot_histogram

# Створення квантового ланцюга
qc = QuantumCircuit(2, 2)

# Ініціалізація (початковий підпис S_initial)
qc.h(0)  # Hadamard створює суперпозицію
qc.cx(0, 1)  # CNOT створює заплутаність

# Перевірка першого стабілізатора (S_intermediate)
qc.measure_all()

# Внесення помилки (імітація шуму)
qc.z(1)

# Відновлення (перевірка S_final)
qc.cx(0, 1)
qc.h(0)

# Вимірювання
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, simulator, shots=1024).result()
counts = result.get_counts()
plot_histogram(counts)
```

Рис. 2. контроль послідовностей у квантовій системі

2. Приклади використання корекції помилок у квантових протокола

Квантова корекція помилок знаходить широке застосування в сучасних квантових протоколах, які використовуються для безпечної передачі інформації, квантового обчислення та мережевого зв'язку. У цьому розділі розглянуто приклади використання методів корекції помилок у ключових квантових протоколах.

2.1.1. Квантова телепортація

Квантова телепортація дозволяє передавати невідомий квантовий стан від однієї сторони (Аліси) до іншої (Боба) за допомогою заплутаного стану та класичного каналу зв'язку. Вона є основою багатьох квантових комунікаційних протоколів.

Етапами телепортації є ініціалізація заплутаного стану, коли Аліса та Боб спільно створюють заплутану пару кубітів

$$|\Phi^+\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$$

Також, наступним етапом є вимірювання кубіта Аліси, коли Аліса виконує вимірювання Белла над своїм кубітом і кубітом, що передається. В результаті Боб отримує стан, ідентичний початковому.

Приклад реалізації телепортації на IBM Qiskit наведений на рис. 3.

Кінцевий етап – це класичний обмін, коли Аліса передає результати вимірювання Бобу, який застосовує корекцію до свого кубіта (наприклад, за допомогою операторів Паулі X та Z).

У процесі телепортації проводиться корекція помилок, яка полягає у захисті заплутаності, коли стабілізатори, такі як Z_1 та Z_2, перевіряють, чи зберігся зв'язок між кубітами під час передачі та у корекції шумів, коли шум руйнує стан $|\Phi+\rangle$, корекція помилок дозволяє відновити заплутаність.

2.1.2. Квантова криптографія (BB84)

Протокол BB84 є одним із перших і найпоширеніших квантових криптографічних протоколів для безпечного розподілу ключів.

Послідовність етапів цього протоколу складається з:

1. Генерація випадкових базисів: Аліса генерує послідовність кубітів у ректилінійному ($|0\rangle$,$|1\rangle$) або діагональному ($|+\rangle$,$|-\rangle$) базисі.

2. Передача кубітів: Кубіти передаються Бобу через квантовий канал.

3. Вибір базисів Бобом: Боб виконує вимірювання у випадкових базисах.

4. Обмін інформацією: Аліса й Боб публічно обмінюються інформацією про базиси та зберігають лише ті біти, де базиси збіглися.

Роль корекції помилок у BB84 полягає у:

– захисті від шуму, коли корекція помилок виключає кубіти, які були пошкоджені під час передачі;

– виявленні атак, коли стабілізатори алгебри підписів допомагають виявити спроби перехоплення зловмисником, наприклад, через фазові зміщення.

2.2 Розподіл квантових ключів у зашумлених середовищах

Квантовий розподіл ключів (QKD) стикається зі значними викликами у зашумлених середовищах, таких як атмосферні канали або оптоволоконні лінії. Корекція помилок забезпечує збереження ключа навіть за наявності шуму.

Методи корекції в QKD є:

1. Стабілізатори для виявлення помилок: Наприклад, у фазових зміщеннях стабілізатори $Z_1Z_2Z_{-1}$ $Z_{-2}Z_1Z_2$ забезпечують коректність стану.

```python
from qiskit import QuantumCircuit, Aer, execute
from qiskit.visualization import plot_histogram

# Квантовий ланцюг для телепортації
qc = QuantumCircuit(3, 2)

# Ініціалізація заплутаного стану
qc.h(1)
qc.cx(1, 2)

# Передача стану через вимірювання Белла
qc.cx(0, 1)
qc.h(0)
qc.measure([0, 1], [0, 1])

# Корекція стану Боба
qc.cx(1, 2)
qc.cz(0, 2)

# Симуляція
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, simulator, shots=1024).result()
counts = result.get_counts()
plot_histogram(counts)
```

Рис. 3. реалізація телепортації на IBM Qiskit

2. Перевірка сумісності станів, коли система виконує синдромний аналіз для визначення відхилень стану.

3. Фільтрація пошкоджених станів, коли кубіти, які не відповідають очікуваним підписам, видаляються з ключа.

Приклад стабілізації ключів у шумному середовищі наведений на рис. 4.

```python
from qiskit import QuantumCircuit, Aer, execute

# Створення заплутаного стану
qc = QuantumCircuit(2)
qc.h(0)
qc.cx(0, 1)

# Внесення шуму
qc.z(1)

# Корекція стану
qc.cx(0, 1)
qc.h(0)

# Симуляція
simulator = Aer.get_backend('statevector_simulator')
result = execute(qc, simulator).result()
statevector = result.get_statevector()
print("Corrected Statevector:", statevector)
```

Рис. 4. стабілізація ключів у шумному середовищі

Квантова корекція помилок відіграє ключову роль у квантових протоколах, таких як телепортація, BB84 і QKD. Використання стабілізаторів і алгебри підписів дозволяє забезпечувати точність і безпеку квантової інформації навіть у зашумлених середовищах. Ці методи становлять основу для подальшого розвитку квантових комунікаційних технологій.

Висновки й перспективи подальших досліджень. У статті було проаналізовано сучасні методи квантової корекції помилок, зокрема використання алгебри підписів, її впровадження в різні протоколи, системи та перспективи розвитку.

1. Визначено ключова роль квантової корекції помилок. Корекція помилок є фундаментальним елементом для забезпечення стабільності квантових обчислень, особливо на шумних пристроях проміжного масштабу (NISQ). Існуючі

методи корекції, такі як код Шора, Steane та топологічні коди, забезпечують стійкість до основних типів помилок.

2. Проаналізовано існуючий метод корекції помилок – алгебра підписів як універсальний інструмент. Визначено, що алгебра підписів продемонструвала свою ефективність у визначенні та корекції помилок у реальному часі; у перевірці стабільності квантових станів та інтеграції з сучасними квантовими протоколами, такими як BB84, E91, DI-QKD, BQC, QSS та ін.

3. Перспективами розвитку є: подальша стандартизація алгебри підписів як інструмента для тестування та корекції помилок; її інтеграції з постквантовою криптографією для забезпечення безпеки даних у квантовій ері; у розробленні нових моделей для систем NISQ, топологічних кодів і квантових мереж.

4. Рекомендаціями для подальших досліджень є такі:

– моделювання систем із високим рівнем шуму;

– поширення на нові протоколи, такі як DI-QKD, а також у гібридні системи;

– побудова квантових мереж;

– оптимізація ресурсів – розроблення методів, що знижують енергетичні та обчислювальні витрати корекції помилок.

Квантова корекція помилок є ключовим напрямом для успішного розвитку квантових технологій. Алгебра підписів виступає як ефективний інструмент для забезпечення стабільності, безпеки та точності квантових обчислень. Її подальше вивчення та впровадження сприятиме вирішенню викликів, пов'язаних із шумами, масштабуванням і безпекою, відкриваючи нові горизонти для квантових досліджень і технологій

5. Робота може бути використана як навчальний матеріал для студентів і дослідників, що займаються квантовими обчисленнями. Використані у роботі приклади коду демонструють, як алгебра підписів інтегрується у квантові обчислення, забезпечуючи надійність обчислень навіть у зашумлених середовищах. Запропоновані підходи можуть бути використані для створення стійких квантових систем і протоколів для криптографії, комунікацій та машинного навчання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Nielsen, M. A., & Chuang, I. L. Quantum Computation and Quantum Information. Cambridge University Press. 2010. 256 p.

2. Shor, P. W. "Scheme for reducing decoherence in quantum computer memory." Physical Review A, 1995. 52(4), R2493-R2496. 320 p.

3. Steane, A. M. "Error Correcting Codes in Quantum Theory." Physical Review Letters, 1996. 77(5), P. 793–797.

4. Bennett, C. H., & Brassard, G. "Quantum Cryptography: Public key distribution and coin tossing." Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984. 498 p.

5. Gottesman, D. "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation." arXiv preprint quant-ph/0904.2557. 2009. 420 p.

6. IBM Quantum Experience Documentation. https://docs.quantum.ibm.com/

7. Google Sycamore Research Papers. https://arxiv.org/abs/2103.03074

8. Post-Quantum Cryptography: NIST Round 3 Standardization. National Institute of Standards and Technology (NIST), 2022. 320 p.

9. Raussendorf, R., & Harrington, J. "Fault-tolerant quantum computation with high threshold in two dimensions." Physical Review Letters, 2007. 98(19), 190504, 2007.

10. Preskill, J. "Quantum Computing in the NISQ era and beyond." Quantum, 2018. No. 2, P.79–87.

11. Qiskit Textbook. IBM Quantum Team, 2023. https://www.ibm.com/quantum/qiskit

12. Broadbent, A., Fitzsimons, J., & Kashefi, E. "Universal blind quantum computation." Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, 2019. No. 3, 400 p.

13. Ekert, A. K. "Quantum cryptography based on Bell's theorem." Physical Review Letters, 1991. 67(6), 661–663.

14. DiVincenzo, D. P. "The Physical Implementation of Quantum Computation." Fortschritte der Physik, 2020. 48(9-11), P. 771–783.

REFERENCES:

1. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press. 256 p.

2. Shor, P. W. (1995). "Scheme for reducing decoherence in quantum computer memory." Physical Review A, 52(4), R2493-R2496. 320 p.

3. Steane, A. M. (1996). "Error Correcting Codes in Quantum Theory." Physical Review Letters, 77(5), P. 793–797.

4. 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, Bangalore, India, 498 p.

5. Gottesman, D. (2009)."An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation." arXiv preprint quant-ph/0904.2557. 420 p.

6. IBM Quantum Experience Documentation. https://docs.quantum.ibm.com/

7. Google Sycamore Research Papers. https://arxiv.org/abs/2103.03074

8. Post-Quantum Cryptography: NIST Round 3 Standardization. National Institute of Standards and Technology (NIST), 2022. 320 p.

9. Raussendorf, R., & Harrington, J. (2007). "Fault-tolerant quantum computation with high threshold in two dimensions." Physical Review Letters, 98(19), 190504, 2007.

10. Preskill, J. (2018). "Quantum Computing in the NISQ era and beyond." Quantum, No. 2, P.79–87.

11. Qiskit Textbook. IBM Quantum Team, 2023. https://www.ibm.com/quantum/qiskit

12. Broadbent, A., Fitzsimons, J., & Kashefi, E. (2019). "Universal blind quantum computation." Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, No. 3, 400 p.

13. Ekert, A. K. (1991). "Quantum cryptography based on Bell's theorem." Physical Review Letters, 67(6), P.661–663.

14. DiVincenzo, D. P. (2020). "The Physical Implementation of Quantum Computation." Fortschritte der Physik, 48(9-11), P. 771–783.