МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
Кафедра Програмної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження застосування методів пост-квантової криптографії для розподілених систем авторизації

Виконав:
студент 2 курсу, групи ІПЗм-21-1
Нікітченко Б.Ю.
(прізвище, ініціали)

Спеціальність 121 – Інженерія програмного забезпечення
Тип програми Освітньо-наукова
Керівник к.т.н., доц Лановий О.Ф.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ З.В. Дудар
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Програмної Інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 121 – Інженерія програмного забезпечення
(код і повна назва)

Тип програми освітньо-наукова програма

Освітня програма Інженерія програмного забезпечення
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри Дудар З. В.
(підпис)
«___» _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студента Нікітченку Богдану Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Дослідження застосування методів пост-квантової криптографії для розподілених систем авторизації»
затверджена наказом університету від « 29 » березня 2023 р. № 302 Ст

2. Термін подання студентом роботи до екзаменаційної комісії «19» травня 2023 р.

3. Вихідні дані до роботи описаний процес моделі комунікаційної архітектури, яка використовує переваги квантової криптографії для забезпечення безпечного зв'язку, пояснювальна записка.

4. Перелік питань, що потрібно опрацювати в роботі мета роботи, аналіз предметної галузі і постановка задачі, дослідження етапів квантового розподілу ключів, аналіз методів ефективного моделювання та впровадження системи контролю якості в цифровому середовищі, вивчення впливу підслуховування на безпеку систем QKD і як його можна зменшити, висновки, перелік джерел посилань.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Інструктаж з техніки безпеки	23.01 – 27.03.2023	Виконано
2	Ознайомлення зі структурою роботи	23.01 – 27.03.2023	Виконано
3	Аналіз предметної галузі та постановка задачі	29.01 – 05.02.2023	Виконано
4	Дослідження етапів квантового розподілу ключів	06.02 – 15.02.2023	Виконано
5	Дослідження процесу повної аутентицікації з пост квантовою криптографією та вектору атаки	17.02 – 10.03.2023	Виконано
6	Розробка архітектурної імітаційної моделі та її реалізації	11.03 – 02.04.2023	Виконано
7	Аналіз результатів експериментальної частини дослідження	03.04 – 15.04.2023	Виконано
8	Підготовка звіту	15.04 – 12.05.2023	Виконано
9	Проходження перевірки на антиплагіат та нормоконтроль	14.05 – 15.05.2023	Виконано
10	Рецензування	15.05 – 17.05.2023	Виконано
11	Підготовка презентації та доповіді	13.05 – 16.05.2023	Виконано
12	Попередній захист та отримання допуску до захисту	16.05 – 17.05.2023	Виконано
13	Захист	19.05.2023	Виконано

Дата видачі завдання 23.01.2022 р.

Студент _____ Нікітченко Б. Ю.
(підпис)

Керівник роботи _____ к.т.н., доц. Лановий О. Ф.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ / ABSTRACT

Пояснювальна записка до кваліфікаційної роботи магістра: 68 сторінок, 22 рисунка, 2 таблиці, 5 додатків, 23 джерела.

АВТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, BB84, КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ, КРИПТОАНАЛІЗ, КРИПТОГАРФІЯ, ПОСТ-КВАНТОВИЙ.

Об’єктом дослідження є оцінка пост-квантових безпечних методів автентифікації, придатних для квантового розподілу ключів.

Основною метою цього дослідження є вивчення та підвищення ефективності алгоритмів квантового розподілу ключів (QKD), зосереджуючись на їх здатності гарантувати безпечний зв'язок у цифрових системах.

У результаті роботи було здійснено аналіз предметної галузі, поставлена задача для дослідження, розроблена комунікаційна модель архітектури, змодельовано протокол BB84, виконано аналіз ефективності QKD для безпечного зв'язку та проведено дослідження впливу підслуховування на безпеку систем QKD.

The explanatory note to the master's thesis: 68 pages, 22 figures, 2 tables, 5 appendices, 23 sources.

AUTHENTICATION, AUTHORISATION, BB84, QUANTUM KEY DISTRIBUTION, CRYPTANALYSIS, CRYPTOGRAPHY, POST-QUANTUM.

The object of research is to evaluate post-quantum secure authentication methods suitable for quantum key distribution.

The main purpose of this study is to investigate and improve the efficiency of quantum key distribution (QKD) algorithms, focusing on their ability to guarantee secure communication in digital systems.

The work included analysing the subject area, setting the research problem, developing a communication architecture model, modelling the BB84 protocol, analysing the effectiveness of QKD for secure communication, and investigating the impact of eavesdropping on the security of QKD systems.

Умови публікації пояснювальної записки

Я,

Нікітченко Богдан Юрійович

(прізвище, ім’я, по батькові)

студент(ка) групи ІПЗм-21-1 здобувач вищої освіти на другому (магістерському) рівні

кафедра програмної інженерії ,

(повна назва кафедри)

заявляю: моя кваліфікаційна робота на тему

Дослідження застосування методів пост-квантової криптографії для розподілених систем авторизації ,

(назва роботи)

що буде представлена до ЕК для публічного захисту, виконана самостійно, в ній не містяться елементи плагіату і вона може бути опублікована в електронному архіві відкритого доступу ElArKhNURE. Всі запозичення з друкованих та електронних джерел мають відповідні посилання.

Я ознайомлений (а) з діючим положенням «Про протидію академічному плагіату в ХНУРЕ», згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування дисциплінарних заходів.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

BB84 – QKD protocol, Bennett and Brassard proposed in 1984.

ITS – Information-Theoretic Secure.

MAC – Message Authentication Code.

MITM – Man-In-The-Middle.

PQC – Post-quantum cryptography.

QKD – Quantum Key Distribution.

ВСТУП

Прагнення до безпечного спілкування сягає корінням у давні цивілізації, майже 2500 років тому, коли елементарні математичні та фізичні об'єкти використовувалися для створення криптосистем. Не дивно, що незабаром з'явилися спроби розшифрувати ці системи. Хоча перші спроби могли мати зловмисні наміри, сьогодні криптоаналіз відіграє вирішальну роль у визначенні безпеки криптосистем. З розвитком науки і техніки розвиваються криптосистеми і методи криптоаналізу, що робить базові шифри заміни і перестановки застарілими. Щоб підвищити стійкість до криптоаналізу, фахівці часто покладалися на заплутування своїх криптосистем.

Технологічний прогрес сприяв розвитку міжміського зв'язку, а отже, виникла потреба в безпечних методах обміну інформацією на величезні відстані. Першочерговою проблемою був обмін секретами між сторонами. Секрети можна було передавати або під час особистих зустрічей, що не завжди було можливим чи практичним, або через довірених кур'єрів, що вводило третю сторону і розширювало поверхню атаки системи. Інтуїтивно зрозуміло, що секрети є безпечнішими, коли ними володіє менша кількість осіб. Однією з причин застосування захисту через невідомість могла бути висока ймовірність витоку ключів у той час – приховування внутрішньої роботи криптосистеми могло діяти як контрзахід, ускладнюючи для супротивників використання викраденого ключа.

Однак в останні два століття криптографія вступила в еру сучасної криптографії. У 19 столітті, на тлі стрімкого розвитку науки і техніки, Кречхофф запропонував, щоб безпека криптосистеми покладалася виключно на секретність ключа, відкинувши необхідність його затушовування. Це підвищило важливість ключа і загострило проблему розподілу ключів. На сьогоднішній день стійкість криптографічного алгоритму безпосередньо пов'язана з проблемою отримання секретного ключа противником, що робить схеми розподілу ключів одним з найбільш чутливих аспектів систем безпеки в мережах зв'язку [1]. Іншим

позитивним наслідком принципу Кречхоффа стало поступове зміцнення глобальної співпраці між криптографами, що дозволило відкрито обмінюватися ідеями та дослідженнями, подібно до інших наукових дисциплін.

Безсумнівно, одним з найбільш значущих відкриттів у сучасній криптографії є асиметрична криптографія – революційна техніка, яка надає кожній стороні, що спілкується, пару ключів – один для шифрування, інший для дешифрування. У цих системах ключ шифрування (відкритий ключ) є загальнодоступним, тоді як ключ дешифрування (секретний ключ) залишається конфіденційним. Повідомлення шифруються за допомогою відкритого ключа одержувача і можуть бути розшифровані лише за допомогою відповідного секретного ключа. Асиметрична криптографія ефективно вирішує проблему розподілу ключів і слугує основою для інфраструктури відкритих ключів (PKI).

Іншою помітною подією 20-го століття стала поява теорії інформації та концепцій інформаційно-теоретичної безпеки і досконалої секретності. Інформаційно-теоретично безпечна (ITS) криптосистема вважається незламною для криптоаналізу, навіть якщо припустити, що супротивник має необмежені обчислювальні потужності – простіше кажучи, для криптоаналізу недоступна достатня кількість інформації. Більше того, якщо зашифрований текст, згенерований алгоритмом шифрування, не розкриває жодної інформації про відповідний відкритий текст, вважається, що криптосистема має ідеальну секретність. Клод Шеннон, батько теорії інформації, продемонстрував, що One Time Pad (OTP) є системою ITS з досконалою секретністю.

Пізніше було встановлено, що для досягнення ідеальної секретності система повинна мати розмір ключа, що дорівнює розміру повідомлення, і використовувати кожен ключ лише один раз, подібно до OTP. Здавалося б, логічно прийняти криптографічні алгоритми з такими ідеальними заходами безпеки, фактично припинивши конкуренцію між «Алісою», «Бобом» і «Євою» і залишивши атаки грубої сили єдиною життєздатною стратегією. Однак більшість сучасних криптосистем не використовують такі високі рівні безпеки, в першу чергу з наступних причин:

– більшість алгоритмів з такими рівнями безпеки не є ефективними – ні з точки зору обчислювальної потужності, ні з точки зору споживання ключів;

– необмежених обчислювальних потужностей, зрозуміло, не існує. Всі наші комерційно доступні обчислювальні потужності обмежені, і щорічні темпи їх зростання в майбутньому певною мірою передбачувані. Таким чином, для багатьох сценаріїв «промислових умов» достатньо обчислювальної безпеки або умовної безпеки, яка захищена від поточних і найближчих майбутніх обчислювальних потужностей.

Квантові обчислення здатні експоненціально прискорити розшифрування численних алгоритмів криптографії з відкритим ключем, таких як RSA, дискретний логарифм і алгоритми Діффі-Хеллмана. Це створює значний ризик для систем шифрування, що покладаються на ці алгоритми. Однак, квантовий розподіл ключів (QKD) і пост-квантова криптографія (PQC) є двома криптографічними структурами, стійкими до квантових загроз, і стають вирішальними для майбутньої інформаційної безпеки. Тим не менш, кожна з них має свої обмеження, і вони доповнюють одна одну. QKD забезпечує безумовну безпеку, чого немає в PQC, тоді як PQC полегшує безпечну і зручну автентифікацію для мереж QKD.

Це дослідження вивчає та ілюструє застосування QKD для безпечного розповсюдження криптографічних ключів через звичайний канал зв'язку. Особлива увага приділяється виконанню широко визнаного протоколу BB84 в рамках розробки імітаційної моделі.

1 АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ ТА ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

1.1 Аналіз предметної галузі

За останні десятиліття прогрес у квантовій фізиці призвів до появи квантової теорії інформації, яка вивчає інформацію, що зберігається у квантових системах. Квантова обробка інформації відкрила нові кордони як для криптографії, так і для криптоаналізу, проклавши шлях до створення та зламу криптосистем.

У 1994 році було розроблено квантовий алгоритм Шора, який ефективно розв'язує задачі цілочисельної факторизації, дискретного логарифмування та дискретного логарифмування еліптичних кривих за поліноміальний час. Ці задачі лежать в основі майже всіх існуючих алгоритмів розподілу ключів. Алгоритм Шора загрожує безпеці багатьох сучасних криптографічних алгоритмів, включаючи RSA і Діффі-Хеллмана, роблячи їх вразливими для квантових комп'ютерів. Наразі квантові комп'ютери обмежуються обчисленнями з невеликою кількістю кубітів у дослідницьких проектах, а розробка реальних квантових комп'ютерів все ще триває. Тим не менш, криптографи працюють над створенням класу криптосистем, стійких до квантових атак, відомих як пост-квантові безпечні системи. Ці системи не мають відомих ефективних квантових або класичних алгоритмів, здатних вирішити основні проблеми, але не пропонують безумовної безпеки (наприклад, AES є пост-квантовим захистом, але не ITS).

Під ефективністю пост-квантових алгоритмів мається на увазі здатність цих криптографічних методів забезпечувати безпечний зв'язок у присутності квантового комп'ютера.

Безпечний зв'язок – це спосіб захисту даних від доступу до них сторонніх осіб. Він передбачає використання шифрування та інших заходів безпеки для забезпечення безпечної передачі даних між двома або більше сторонами [2].

Пост-квантова криптографія включає алгоритми, які, хоча і виконуються на класичних комп'ютерах, але, як вважається, витримують атаки квантових

комп'ютерів. Ці алгоритми вважаються «квантово-стійкими». Їх ефективність в першу чергу вимірюється здатністю забезпечувати конфіденційність, цілісність і автентифікацію в світі пост-квантових обчислень.

Фактори, які впливають на ефективність пост-квантових алгоритмів:

– безпека, алгоритм повинен бути стійким як до класичних, так і до квантових атак;

– продуктивність, алгоритм повинен бути ефективним з точки зору обчислювальних ресурсів, що включає в себе такі фактори, як швидкість шифрування і дешифрування, розмір ключів і зашифрованих текстів;

– гнучкість, алгоритм повинен бути адаптований до різних систем і застосувань [3].

Національний інститут стандартів і технологій (NIST) зараз знаходиться в процесі стандартизації алгоритмів пост-квантової криптографії, що включає оцінку їх ефективності проти потенційних квантових загроз [4].

З іншого боку, принципи квантової механіки і квантової механіки поля дозволяють виконувати криптографічні завдання з безумовною безпекою. Ці принципи, які включають наслідки принципу невизначеності Гейзенберга і пов'язаного з ним ефекту спостерігача, квантову заплутаність і теорему про відсутність клонування, складають основу квантової криптографії. Принципи квантової фізики унеможливлюють непомітне для зловмисників підслуховування зв'язку по квантовому каналу і забороняють копіювання зв'язку, що робить квантову криптографію ITS.

У криптографії «зловмисник» або «противник» – це зловмисник або нападник, який намагається обійти заходи безпеки криптографічної системи. Це можуть бути спроби розшифрувати повідомлення без належного ключа, видати себе за законного користувача, підслухати захищений зв'язок або якимось чином порушити роботу системи. Метою криптографії є розробка систем, які залишаються безпечними навіть тоді, коли противник має значні обчислювальні ресурси або доступ до певної секретної інформації [5].

У 1984 році Чарльз Беннетт і Жиль Брассар продемонстрували одне з перших застосувань квантової криптографії, представивши квантовий розподіл ключів (QKD) як засіб обміну секретом (ключем) між двома сторонами, що використовують «елементарні квантові системи, такі як поляризовані фотони [...] для передачі цифрової інформації» [6]. Сьогодні існує безліч застосувань квантової криптографії, серед яких значну увагу привертає саме QKD. Технологічний прогрес сприяв практичному розвитку квантового зв'язку на відстані в сотні кілометрів. Оскільки безпека відомих алгоритмів розподілу ключів знаходиться під загрозою через квантовий алгоритм Шора, QKD є ідеальною альтернативою з огляду на його безумовну безпеку та доведену практичність.

1.2 Аналіз методів квантового розподілу ключів

Метод, запропонований Беннеттом і Брассардом, відомий як протокол BB84, надихнув на розробку різних протоколів QKD. На додаток до зв'язку через квантові канали, більшість з цих протоколів, включаючи BB84, вимагають зв'язку через класичний аутентифікований канал – забезпечення цього класичного аутентифікованого каналу є центральним фокусом цього дослідження. Оскільки BB84 лежить в основі багатьох протоколів QKD, він був обраний як протокол QKD для цього дослідження.

1.2.1 BB84

Цифрова інформація в протоколі BB84 кодується в елементарні квантові системи, такі як поляризація одного фотона, шляхом випромінювання окремих фотонів через різні фільтри. Семантика BB84, яка відображена на рисунку 1.1, включає чотири фільтри з двома різними основами - один прямолінійний (горизонтально-вертикальний), а інший ортогональний (діагональний), що

призводить до двох різних поляризацій як для біта 0, так і для біта 1 [7]. Аліса кодує випадковий бітовий рядок (тобто ключ) за допомогою описаного методу, випадковим чином вибираючи основу фільтра для кожного біта. Боб також випадковим чином вибирає між прямолінійним та ортогональним базисом детектора і вимірює кожен фотон. Після того, як Боб отримує всі фотони, комунікація по квантовому каналу завершується – як згадувалося раніше, ця комунікація є вразливою до невиявленого підслуховування.

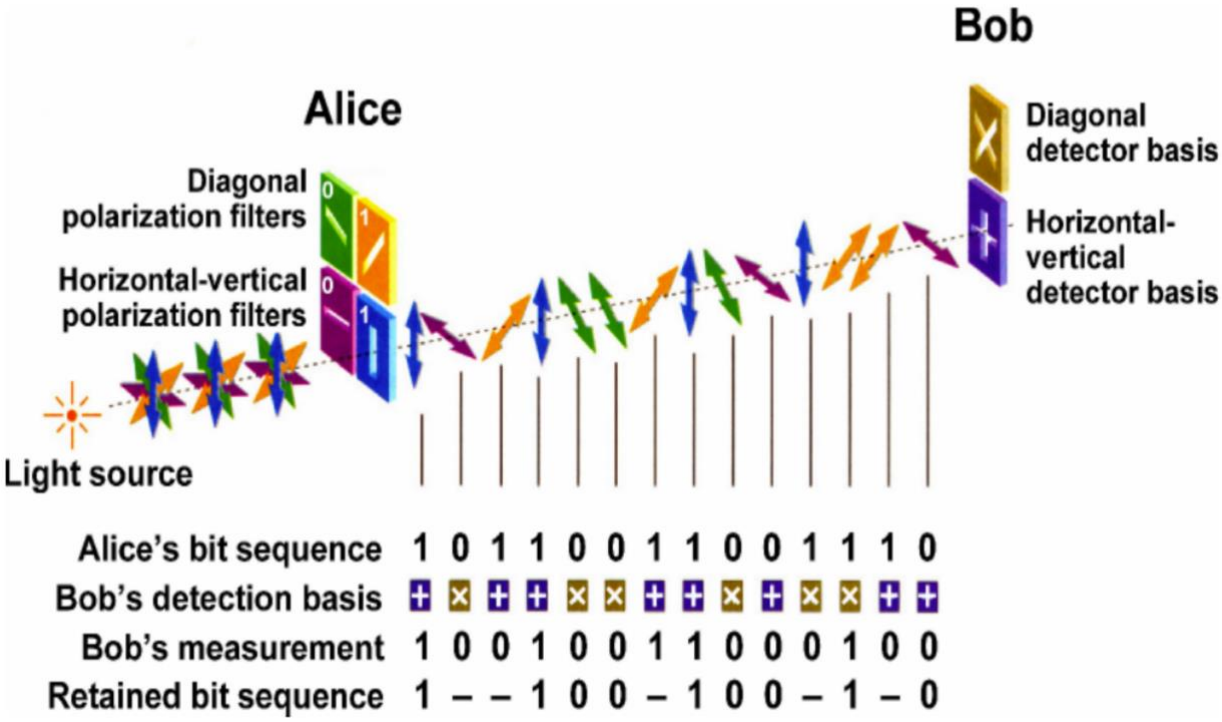

Рисунок 1.1 – Запуск схеми протоколу квантового розподілу ключів

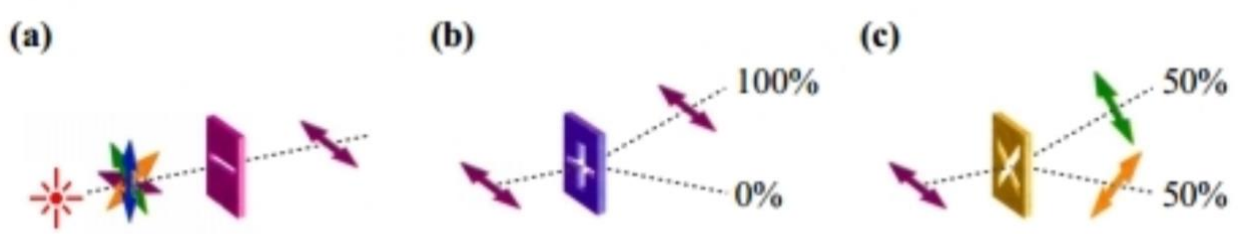

Рисунок 1.2 – Основи поляризації фотонів

Рисунок 1.2 ілюструє фундаментальні аспекти поляризованих фотонів. У частині (a) зображення, коли фотон проходить через поляризаційний фільтр, в даному випадку горизонтальний, результат завжди відповідає очікуваному. Якщо вимірювання проводиться з детектором в тому ж базисі, що і той, який спочатку використовувався для поляризації фотона, результат вимірювання, безсумнівно, буде точним і очікуваним. Це продемонстровано в частині (b), де один горизонтально поляризований фотон, виміряний за допомогою детектора з прямолінійним базисом, постійно дає правильний результат. Однак, коли базис, що використовується для поляризації, відрізняється від того, що використовується для детектування, результат стає імовірнісним. Як видно з частини (c) рисунка 1.2, використання детектора з ортогональним базисом для вимірювання фотона, поляризованого в прямолінійному базисі, з однаковою ймовірністю дає фотон, повернутий під кутом 45° або 135°.

Оскільки і Аліса, і Боб вибирають базис випадковим чином, очікуються розбіжності у базисі. Насправді, всі вимірювання, які Боб виконує з іншим базисом, ніж той, який використовувала Аліса для поляризації фотона, є імовірнісними і ненадійними, і повинні бути відкинуті обома сторонами. Крім того, можливо, що деякі фотони втрачаються під час передачі або неточно виявляються «недосконалими детекторами Боба». Процедура пост-обробки відбувається через класичний канал з відкритою автентифікацією, і після її завершення обидві сторони зберігають бітову послідовність, відому лише їм самим.

Варто зазначити, що постобробка є Ахіллесовою п'ятою BB84, оскільки зв'язок по квантовому каналу забезпечується принципами квантової фізики [8]. Якщо підслуховувач хоче перехопити квантовий канал непоміченим, він повинен поставити під загрозу автентичність зв'язку через класичний канал, ставлячи під загрозу безпеку всього протоколу.

Пост-обробка починається з публічної розмови між двома сторонами після завершення комунікації по квантовому каналу. Як підкреслювалося раніше, цей зв'язок повинен бути автентифікований, щоб одержувач був абсолютно впевнений в особі відправника і в тому, що зміст повідомлення не був змінений. Однак, зміст

повідомлення не потрібно шифрувати; знання інформації, що обговорюється через відкритий канал, не ставить під загрозу секретність спільного бітового рядка через квантовий канал [6].

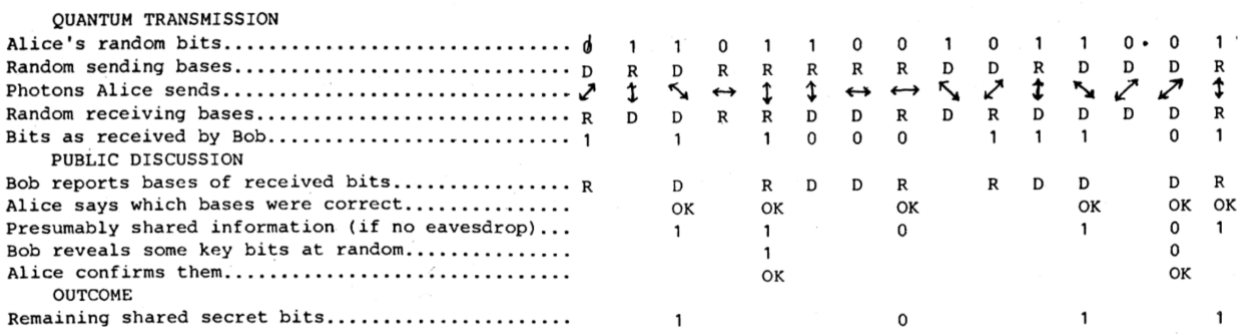

Рисунок 1.3 – Оригінальний потік протоколу BB84, включаючи квантовий зв'язок і постобробку

На рисунку 1.3 представлено оригінальний потік протоколу BB84, розділений на квантову передачу, про яку йшлося раніше, і публічне обговорення. У запропонованому методі Боб ініціює публічне обговорення після повідомлення Аліси про те, що він отримав фотони. Він починає процедуру з розкриття базису, який він використовував для детектування, а Аліса підтверджує його правильність. Цей крок, також відомий як просіювання ключів, призводить до того, що сторони отримують спільний бітовий рядок.

Під час постобробки наступним кроком є підтвердження, на якому Боб розкриває випадкові біти ймовірного спільного бітового рядка, а Аліса перевіряє їхню точність. Після цього кроку вони можуть обчислити приблизний рівень помилок на основі розбіжностей – високий рівень помилок може свідчити про підслуховування. З моменту появи BB84 було запропоновано численні варіанти та вдосконалення протоколу, в першу чергу для пост-обробки. Були запропоновані різні алгоритми і методи, і в оригінальному документі BB84 підтвердження є останнім кроком протоколу, без явної згадки про те, як обробляти ймовірні помилки в спільному ключі, спричинені помилками при передачі. Отже, наступні

документи часто включають виправлення помилок для усунення потенційних помилок. Посилення конфіденційності, ще один поширений етап постобробки в QKD, передбачає використання сторонами методів підвищення конфіденційності для збільшення секретності спільного ключа, що значно зменшує знання підслуховувача, навіть якщо він знає деякі біти спільного ключа.

Порядок виконання цих кроків відрізняється в різних роботах. Дехто вважає, що після завершення посилення конфіденційності спільний ключ є секретним, а виправлення помилок слугує остаточним підтвердженням точності ключа. Інші стверджують, що виправлення помилок може розкрити інформацію про ключ, тому після цього слід виконати посилення конфіденційності – це питання обговорюється далі.

1.3 Аналіз методів криптографічної автентифікації

Криптографічна автентифікація служить для встановлення цілісності та автентичності повідомлень. Як правило, алгоритми автентифікації мають дві основні функції: одна для автентифікації повідомлень, а інша для перевірки автентифікованих повідомлень. Ці функції використовують ключ разом з іншою інформацією як вхідні дані, щоб гарантувати автентичність і цілісність повідомлення - гарантуючи, що ніхто не змінив повідомлення або не видав себе за справжнього відправника, припускаючи, що ключ залишається конфіденційним.

Загалом, існує два типи алгоритмів криптографічної автентифікації: код автентифікації повідомлення (MAC) і цифровий підпис [9]. MAC – це симетричні алгоритми, в яких функції автентифікації та верифікації використовують один і той самий ключ. На відміну від них, алгоритми цифрового підпису є асиметричними і використовують пару ключів. Секретний ключ, відомий лише відправнику, використовується для підписання повідомлень, тоді як відкритий ключ використовується для перевірки.

1.3.1 Автентифікація в QKD

Якщо зловмисник може вставити повідомлення на свій розсуд у класичну комунікацію пост-обробки, він може легко здійснити атаку типу «людина посередині» (MITM). Для цього зловмисник повинен позиціонувати себе «посередині» комунікаційного каналу сторін. Перебуваючи в середині як класичного, так і квантового зв'язку, зловмисник ініціює квантовий протокол з відправником, видаючи себе за одержувача, і одночасно запускає протокол з одержувачем, видаючи себе за відправника. Під час постобробки опонент видає себе за іншу сторону. Якщо автентифікація під час постобробки повідомлення є надійною, цей обман можна швидко виявити на етапі підтвердження (секції), де сторони розкривають частину обмінюваного ключа, також відому як «відсіяний ключ», що використовується з тією ж самою основою. Якщо більшість цих бітів не збігаються, це вказує на те, що зв'язок через квантовий канал був підроблений. Якби схема автентифікації була вразливою до підробки, зловмисник міг би маніпулювати повідомленнями на цьому етапі на свою користь, переконуючи обидві сторони, що вони поділилися секретним ключем один з одним, тоді як насправді вони розподілили ключі зі зловмисником.

Існує два основних підходи до виконання автентифікації після обробки повідомлень: відкладена та миттєва. Як випливає з назв, миттєва автентифікація автентифікує повідомлення під час комунікації, коли вони передаються, тоді як відкладена автентифікація відбувається на останньому кроці після того, як всі повідомлення надіслані. Більшість літературних джерел припускає, що спільний секрет, який використовується для автентифікації, присутній під час початкової взаємодії між сторонами, а згодом вони використовують ключі, згенеровані за допомогою QKD [10].

1.4 Постановка завдання дослідження

Основною метою цього дослідження є вивчення та підвищення ефективності алгоритмів квантового розподілу ключів (QKD), зосереджуючись на їх здатності гарантувати безпечний зв'язок у цифрових системах.

У зв'язку зі зростанням кіберзагроз потреба в надійних і безпечних системах зв'язку ніколи не була такою гострою, як зараз. Традиційні криптографічні методи, хоча і широко використовуються, стають все більш вразливими до витончених атак. Квантовий розподіл ключів (QKD) пропонує багатообіцяючу альтернативу, використовуючи принципи квантової механіки для забезпечення безпечного зв'язку. Однак практична реалізація та оптимізація систем QKD залишаються недостатньо дослідженими областями.

Були виявлені наступні завдання дослідження:

– детально дослідити етапи квантового розподілу ключів;

– проаналізувати методи ефективного моделювання та впровадження системи контролю якості в цифровому середовищі;

– проаналізувати вплив підслуховування на безпеку систем QKD і як його можна зменшити;

– розробити моделі комунікаційної архітектури, яка використовує переваги квантової криптографії для забезпечення безпечного зв'язку;

– реалізувати та моделювати протокол BB84 на python3;

– виконати аналіз ефективності QKD для безпечного зв'язку.

У цьому дослідженні будуть використані імітаційні моделі для вивчення реалізації систем QKD. Основна увага буде приділена генерації та передачі квантових бітів (кубітів), механізмам виявлення та виправлення помилок, впливу підслуховування та процесу посилення конфіденційності. Ефективність різних алгоритмів QKD буде оцінена на основі їх здатності підтримувати безпечний зв'язок в умовах потенційних кіберзагроз.

2 ДОСЛІДЖЕННЯ ЕТАПІВ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ

2.1 Пост-обробка QKD

Постобробка – це публічне обговорення, яке відбувається через аутентифікований канал одразу після квантового зв'язку, під час якого обидві сторони отримують бітову послідовність, також відому як сирий ключ [11]. На етапі постобробки виявляються невідповідності базису при передачі та вимірюванні, і відповідні біти видаляються з сирого ключа під час просіювання. Потім обчислюється коефіцієнт помилок в кубітах (QBER), причому обидві сторони розкривають частину просіяного ключа на етапі підтвердження. На цьому ж кроці оцінюється ймовірність підслуховування - якщо QBER перевищує певний поріг, ключ ігнорується, і зв'язок по квантовому каналу повинен бути перезапущений. Потім визначаються ймовірні помилки передачі та виявлення в решті підтвердженого ключа, і останній крок спрямований на мінімізацію потенційної обізнаності підслуховувача про спільний секрет. Життєвий цикл ключа під час пост-обробки зображено на рисунку 2.1, де кожна стрілка позначає один крок пост-обробки.

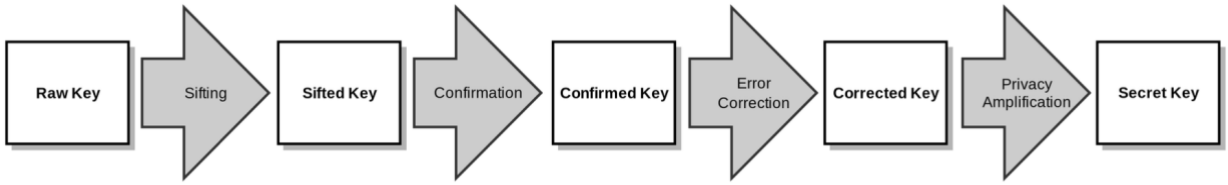

Рисунок 2.1 – Життєвий цикл ключів через пост-обробку, стрілки відображають етапи пост-обробки

Тут детально описано чотири основні етапи пост-обробки, запропоновані в оригінальному BB84, з відомими алгоритмами, описаними між відправником (який ініціює протокол) і одержувачем.

2.2 Відсіювання ключів

Перебір ключів – це перший крок постобробки, під час якого сторони виявляють використовувані базиси та усувають невідповідні [12]. Існують різні методи просіювання, але в їх основі лежить те, що сторони повинні розкрити всі базиси, використані під час квантової комунікації, щоб виконати просіювання. Щоб відсіяти всі базиси, одна сторона повинна надіслати рядок довжиною в сам ключ, кожен біт якого представляє вибір базису. Рядок бітів такої ж довжини від іншої сторони підтвердить правильність або відповідність основ. В оригінальному BB84 приймач ініціює просіювання.

Відмінності в ключових підходах до відсіювання є результатом різної політики завершення квантової комунікації. Хоча в оригінальній статті пропонувалася політика, заснована на часі, в якій одержувач повідомляє відправника про те, що всі кубіти були захоплені в кінці квантової комунікації, дехто пропонує ітеративне просіювання, в той час як інший неітеративний метод використовує фіксований базис для передачі ключа і використовує інший базис в якості приманки [13]. Ці модифікації мають на меті підвищити ефективність, практичність та частоту ключів.

У цьому дослідженні, однак, я дотримуюся оригінальної політики завершення на основі часу BB84 – приймач очікує на фотон протягом певного часового інтервалу, і як тільки час виявлення спливає, приймач розкриває основу, обрану під час вимірювання. Потім відправник повідомляє одержувачу, які з них є правильними. Як показано на рисунку 2.1, на вхід на цьому кроці подається необроблений ключ, а на виході – відсіяний ключ. На цьому кроці передаються два повідомлення, кожне з яких потенційно може бути таким же великим, як і сам необроблений ключ.

2.3 Підтвердження

На цьому етапі розкривається частина відсіяного ключа, що дозволяє сторонам обчислити рівень помилок у квантовому каналі, тобто QBER. Якщо рівень помилок перевищує певний поріг, сторони відмовляються від пост-обробки. Як ми вже обговорювали раніше, очікувані помилки є результатом втрат під час передачі та вимірювання. Крім того, якість майже будь-якого з'єднання погіршується зі збільшенням відстані, а якість використовуваного обладнання також впливає на якість зв'язку – вищий за очікуваний QBER є результатом підслуховування, коли зловмисник намагався виміряти і порушити кубіт або здійснити MITM-атаку [14].

Подібно до просіювання, існують різні пропозиції щодо кроку підтвердження, які біти і яка частина просіяного ключа повинна бути розкрита, а також хто повинен ініціювати цей крок. Однак, це дослідження слідує оригінальним рекомендаціям BB84, в яких відправник запитує випадкові індекси у відсіяному ключі, а одержувач розкриває ці біти [8]. Потім відправник повідомляє одержувачу, скільки з них правильні. Після цього вони можуть обчислити QBER і вирішити, продовжувати чи ні. В оригінальному документі не вказано, скільки бітів має бути розкрито, але наступні роботи запропонували до половини відсіяного ключа, а для підтвердження кожного біта потрібно повідомлення однакового розміру. На цьому кроці передається щонайменше три повідомлення. Звичайно, виявлені біти видаляються з просіяного ключа для формування підтвердженого ключа.

2.4 Виправлення помилок

В оригінальному документі BB84, як показано на рисунку 1.3, підтвердження вважається останнім кроком постобробки. Однак на практиці на цьому етапі сторони мають спільну бітову послідовність, яка містить помилки з дуже високою

ймовірністю, як вказує QBER. Тому для сторін дуже важливо виправити ці помилки.

Численні алгоритми виправлення помилок можуть бути обрані на основі конкретних вимог і потреб реалізації. Як правило, існує два основних підходи до цих алгоритмів:

– симетричний, коли обидві сторони беруть участь у процесі з однаковим навантаженням;

– асиметричний, в якому лише одна сторона відіграє головну роль [15].

Симетричні методи використовуються в сценаріях, коли обчислення для однієї сторони є дорогими, наприклад, супутники або вбудовані системи.

Кількість повідомлень, що передаються на цьому етапі, залежить від QBER, довжини спільного секрету та обраного алгоритму. Глибоке вивчення алгоритмів виправлення помилок, таких як BCH [16], LDPC, Cascade та інших, виходить за рамки цього дослідження.

2.5 Посилення конфіденційності

Оскільки помилки у підтвердженому ключі, ймовірно, пов'язані з причинами, згаданими раніше, виправлення помилок є дуже важливим. Однак, багато алгоритмів виправлення помилок розголошують інформацію про дані, які вони обробляють, в даному випадку, про підтверджений ключ. Тому необхідно мінімізувати поінформованість супротивника після такого витоку або будь-яких інших потенційних ризиків. Цього можна досягти за допомогою методів підвищення конфіденційності – найбільш часто згадуваним в літературі методом є використання сімейства хеш-функцій [17].

У квантовому розподілі ключів (QKD) посилення конфіденційності – це процедура, яка використовує сімейство хеш-функцій для зменшення інформації, яку може отримати підслуховувач про ключ. Після етапів відсіювання, виправлення помилок та верифікації сторони обмінюються сирим ключем, який

може бути відомий стороннім особам. Щоб усунути це, вони вибирають випадкову хеш-функцію з сімейства універсальних хеш-функцій і обидві сторони застосовують її до своїх ключів. Цей процес призводить до того, що кінцевий ключ стає коротшим, але гарантує, що будь-яка інформація, яку може мати підслуховувач про ключ, стає мізерно малою, що підвищує конфіденційність ключа.

В оригінальному документі BB84 також явно не розглядався крок підвищення конфіденційності. Насправді, це не є основною метою цього дослідження – оскільки, якщо відправник і одержувач вже домовилися про метод підвищення конфіденційності, решта включає в себе локальні обчислення для кожної сторони, і на цьому етапі не потрібно обмінюватися повідомленнями; отже, немає необхідності нічого автентифікувати. Оскільки для посилення конфіденційності зазвичай використовують сімейство хеш-функцій, можна з упевненістю припустити, що відправник і одержувач повинні домовитися про функцію з цього сімейства для цього кроку – це єдине повідомлення, необхідне для цього кроку, яке, звичайно, має відбутися до самого кроку.

3 ДОСЛІДЖЕННЯ ПРОЦЕСУ ПОВНОЇ АУТЕНТИЦІКАЦІ З ПОСТ КВАНТОВОЮ КРИПТОГРАФІЄЮ ТА ВЕКТОРУ АТАКИ

3.1 Повна автентифікація з PQC

Для досягнення повної автентифікації обробки даних QKD з використанням PQC та забезпечення безпеки кінцевого ключа, дуже важливо одночасно підписувати та шифрувати дайджести, згенеровані ключем з виправленими помилками та кінцевим ключем. Раніше для шифрування використовувалися заздалегідь надані симетричні ключі. Однак, оскільки PQC не має безумовної безпеки, і ми хочемо припустити його короткострокову, а не довгострокову безпеку, пропонується використовувати алгоритм PQC для підписання і шифрування дайджесту, створеного ключем з виправленими помилками і кінцевим ключем в початковому раунді QKD [18]. Згодом частина ключа, згенерованого в першому раунді, буде використана для автентифікації в другому раунді QKD з використанням симетричного шифрування ключа, як показано на рисунку 3.1. Починаючи з третього раунду, кожен раунд QKD буде використовувати частину ключа, згенерованого в попередньому раунді, для автентифікації на основі симетричного шифрування ключа [19]. Після завершення автентифікації ключ шифрування відкидається, а решта ключів зберігається в пулі ключів як безпечні ключі.

3.1.1 Протокол пост-обробки даних, варіант 1

Використовуючи протокол BB84 як приклад, відправник і одержувач називаються Аліса і Боб, відповідно. Єва – пасивний зловмисник, від англійського слова eavesdropper (підслуховувач). Вона може слухати повідомлення між Алісою та Бобом, але не може впливати на них. Для кожного раунду QKD, після модуляції, передачі та виявлення квантових сигналів, протокол пост-обробки даних виглядає наступним чином:

Крок 1. Боб повідомляє Алісу про дійсні позиції виявлення, а Аліса відкидає записи невиявлених квантових станів.

Крок 2. Аліса і Боб проводять двостороннє базисне просіювання, аутентифікуючись за допомогою алгоритму підпису PQC. Якщо аутентифікація пройшла успішно, продовжуємо, якщо ні – перериваємо.

Крок 3. Аліса і Боб оцінюють квантовий коефіцієнт бітових помилок. Якщо рівень бітових помилок перевищує поріг, протокол завершується. В іншому випадку сторони виправляють сирий ключ після базисного просіювання, щоб отримати ключ з виправленими помилками.

Крок 4. Аліса і Боб виконують двосторонню перевірку з виправленням помилок, дайджест якої підписується і шифрується за допомогою алгоритмів PQC. Якщо перевірка пройшла успішно, продовжуємо роботу, якщо ні - перериваємо.

Крок 5. Аліса генерує рядок з 2n випадкових бітів і відправляє їх Бобу. Сторони домовляються використати ці n бітів для побудови матриці Тепліца для посилення конфіденційності, при цьому процес буде автентифіковано за допомогою алгоритму підпису PQC. Якщо автентифікація пройшла успішно, продовжуємо, якщо ні – перериваємо.

Крок 6. Аліса і Боб одночасно виконують посилення конфіденційності, щоб згенерувати безпечний ключ. При обчисленні коефіцієнту посилення конфіденційності слід враховувати не тільки частоту бітових помилок, але й кількість інформації, яка може бути витоком через дайджест, зашифрований PQC на кроці 4.

Крок 7. Аліса і Боб проводять двосторонню перевірку фінального ключа, дайджест якого підписано і зашифровано за допомогою алгоритмів PQC. Якщо перевірка пройшла успішно, продовжуємо роботу, якщо ні – перериваємо її.

Крок 8. Аліса і Боб створюють нову матрицю Тепліца, використовуючи ще n біт випадкових чисел з кроку 5. Обидві сторони використовують посилення конфіденційності, щоб зменшити кількість інформації, яку Єва може отримати з кроку 7, і вивести остаточний ключ.

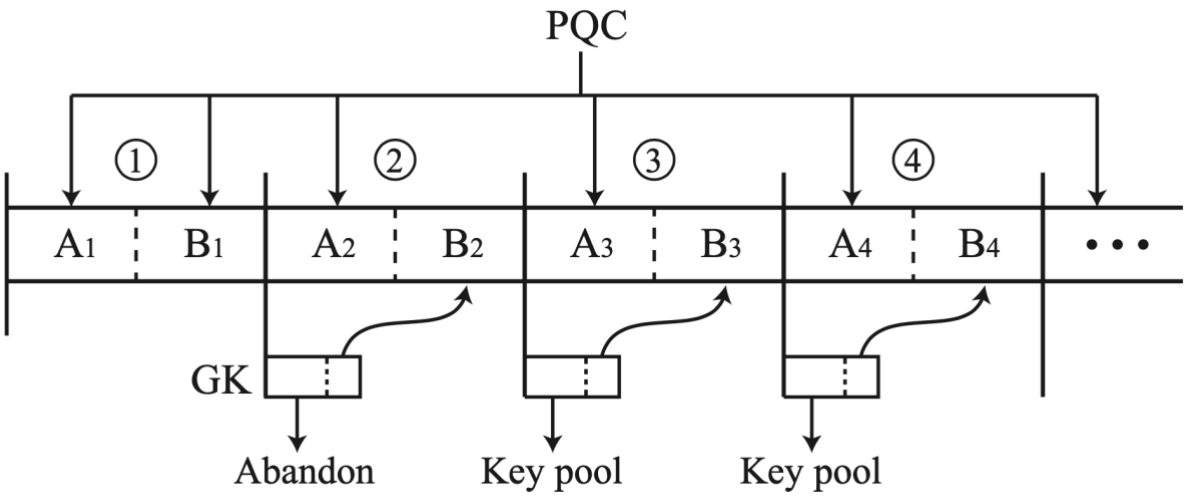

Рисунок 3.1 – Автентифікація для кожного раунду QKD, а також генерація та споживання ключів

Постобробка даних для другого раунду QKD подібна до першого раунду, з відмінностями на кроках 4 і 7, де підпис і шифрування PQC не використовуються для автентифікації. Замість цього, частина ключа, згенерованого в першому раунді, використовується для автентифікації за допомогою симетричного шифрування. На кроці 5 Аліса генерує лише n випадкових бітів і надсилає їх Бобу; на кроці 6 при обчисленні коефіцієнта посилення конфіденційності враховується лише частота бітових помилок; на кроці 7 виводиться остаточний ключ, а крок 8 пропускається.

Починаючи з третього раунду, постобробка даних кожного раунду QKD відбувається аналогічно до другого раунду. Однак у кожному раунді Аліса і Боб домовляються використовувати однакову частину остаточного ключа, отриманого у попередньому раунді, для перевірки виправлення помилок і перевірки остаточного ключа у поточному раунді. Після завершення аутентифікації ключ аутентифікації відкидається і не може бути використаний повторно.

Важливо зазначити, що алгоритми підпису та шифрування PQC, як правило, відрізняються. У наведеному вище протоколі ми припускаємо безпеку як алгоритму підпису PQC, так і алгоритму шифрування PQC, але це припущення ґрунтується на короткому часовому інтервалі. Наприклад, якщо типовий час, необхідний для постобробки даних в кожному раунді QKD, становить близько 1

секунди, то нам потрібно вірити, що алгоритм PQC є безпечним лише в межах цього 1-секундного вікна. Поки кількість ключів, що генеруються в кожному раунді QKD, більша, ніж необхідна для наступного раунду симетричної ключової автентифікації, можна підтримувати безпечну та безперервну роботу QKD.

Щоб мінімізувати споживання ключів, враховуючи, що просіювання базису та передача випадкових чисел для посилення конфіденційності не розголошують ключову інформацію, алгоритм підпису PQC можна використовувати для завершення автентифікації для цих двох процесів у кожному раунді QKD, як показано на рисунку 3.1. Якщо, починаючи з другого раунду QKD, для автентифікації просіювання базису та передачі випадкових чисел не використовуватиметься PQC, а буде застосовуватися симетричний ключ для автентифікації, можна припустити, що довжина кожного дайджесту становить n біт (наприклад, SHA-256 має 256 біт) [20]. Отже, згідно з формулою (1), ці два процеси будуть споживати n біт ключів, зменшуючи безпечну частоту ключів і максимальну відстань.

$$\Delta R = \frac{n}{T} \text{ біт/с} \tag{1}$$

де n – довжина ключа у бітах;

T – тривалість кожного раунду QKD;

ΔR – швидкість, з якою безпечні ключі можуть бути згенеровані за допомогою квантової механіки [21].

Автентифікація постобробки даних QKD за допомогою PQC показана на рисунку 3.2, де Аліса є відправником, а Боб - одержувачем. Відповідно до алгоритму пост-квантового криптографічного підпису, кожен вузол генерує пару пар відкритих і закритих ключів, наприклад, Аліси (S_A, P_A) і Боба (S_B, P_B), де S_A і S_B – закриті ключі, а P_A і P_B – відкриті ключі. Відповідно до протоколу інфраструктури відкритих ключів, кожен користувач надійно зберігає свій приватний ключ. Відкриті ключі передаються довіреній третій стороні – центру сертифікації (ЦС),

який підписує їх і видає цифрові сертифікати користувачам. ЦС також використовує алгоритм пост-квантового підпису.

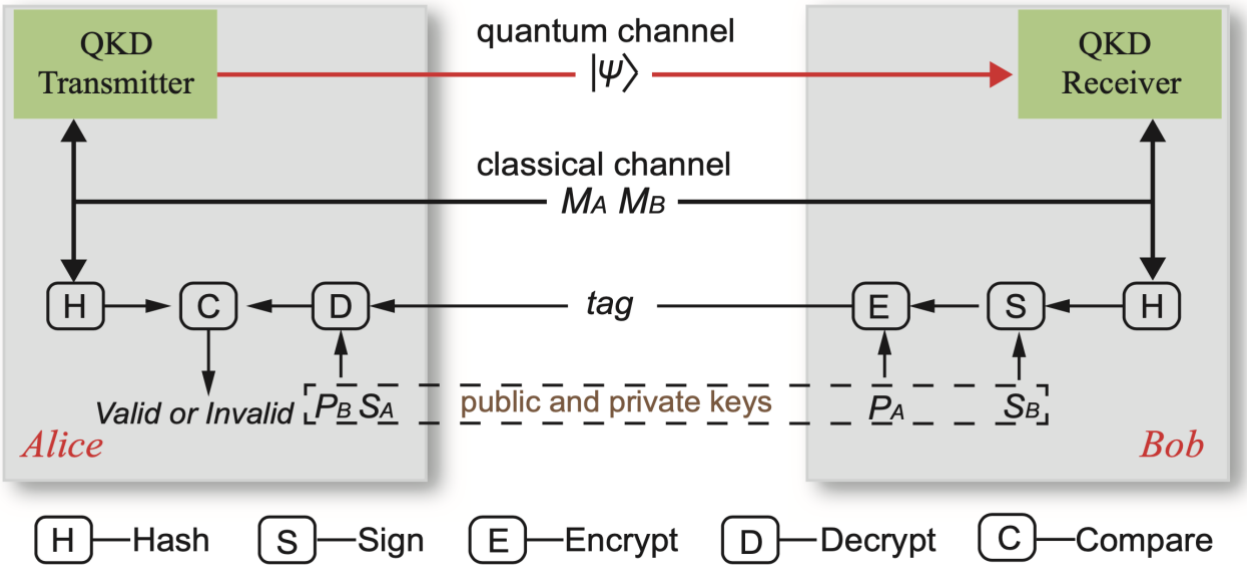

Рисунок 3.2 – Схема підпису та шифрування даних постобробки квантового розподілу ключів постквантовою криптографією

На початку аутентифікації Аліса і Боб обмінюються цифровими сертифікатами, перевіряючи їх автентичність за допомогою відкритого ключа ЦС, щоб отримати відкритий ключ іншої сторони. Для двох процесів просіювання базису і передачі випадкових чисел, необхідних для посилення конфіденційності, система QKD спочатку генерує короткий дайджест повідомлення, що підлягає перевірці автентичності, за допомогою хеш-алгоритму. Потім алгоритм PQC завершує процеси підпису, шифрування, передачі, розшифрування і порівняння, як показано на рисунку 3.2. Якщо Аліса хоче автентифікувати повідомлення Боба, Боб підписує дайджест своїм закритим ключем S_B і надсилає його Алісі разом з класичним повідомленням. Аліса розшифровує дайджест за допомогою відкритого ключа Боба P_B і порівнює його з дайджестом, отриманим шляхом хешування отриманого повідомлення. Якщо вони збігаються, автентифікація пройшла успішно, в іншому випадку – ні. Алгоритм PQC надає зворотній зв'язок про

результати автентифікації системі QKD, завершуючи цей раунд автентифікації. Важливо зашифрувати підписані дайджести для двох процесів – перевірки виправлення помилок і остаточної перевірки ключа. Використовуючи алгоритм відкритого ключа, Боб шифрує дайджести за допомогою відкритого ключа P_A Аліси і надсилає зашифрований текст Алісі. Очевидно, що ключ з виправленими помилками і остаточний ключ не можуть бути надіслані. Отримавши зашифрований текст, Аліса розшифровує його своїм закритим ключем S_A, щоб отримати підписаний дайджест, після чого виконує процес перевірки підпису, згаданий вище. Процес автентифікації аналогічний, якщо Боб хоче автентифікувати повідомлення Аліси.

3.1.2 Протокол пост-обробки даних, варіант 2

У цьому протоколі PQC використовується виключно для підписів, а не для шифрування. Спочатку алгоритм підпису PQC перевіряє автентичність відсіювання базису. Після корекції необробленого ключа підпис PQC підтверджує автентичність процесу перевірки узгодженості ключа після корекції, але дайджест залишається незашифрованим. Подальше посилення конфіденційності стискає будь-яку потенційну витік інформації. Коли перевірка виправлення помилок підтверджується, Аліса і Боб володіють ідентичними ключами. Алгоритм підпису PQC підтверджує автентичність передачі випадкових чисел, необхідних для посилення конфіденційності. Згодом обидві сторони використовують ці випадкові числа для побудови однієї і тієї ж матриці Тепліца і виконують посилення конфіденційності на ключі з виправленими помилками. Дуже важливо врахувати кількість інформації, що просочилася в попередньому дайджесті, щоб Єва не змогла отримати жодної інформації. Хоча остаточний ключ після посилення конфіденційності є безпечним, це не гарантує, що ключі Аліси і Боба ідентичні; таким чином, необхідна остаточна перевірка ключа, що вимагає автентифікації. Після цього Аліса і Боб можуть використовувати невелику симетричну частину

остаточного ключа, заздалегідь узгоджену, для перевірки решти остаточного ключа, забезпечуючи безпеку автентифікації. Автентифікація є успішною лише у випадку, якщо ключі автентифікації, отримані Алісою і Бобом, та решта ключів, що підлягають перевірці, співпадають; у протилежному випадку автентифікація завершиться невдачею. Це відповідає вимогам до остаточної перевірки ключів. Хоча для автентифікації використовується симетричне шифрування ключів, воно не вимагає ні попередньо наданого симетричного ключа, ні шифрування PQC. У порівнянні з першим протоколом, цей протокол зменшує припущення щодо безпеки алгоритму шифрування PQC, зберігаючи при цьому ту ж саму частоту ключів.

Варто зазначити, що хоча Аліса і Боб мають однакову випадкову базову інформацію після просіювання базису, ця інформація не є конфіденційною і не може бути використана для автентифікації інших трьох процесів з симетричним шифруванням.

3.1.3 Атака повторного відтворення на автентифікацію

У повторній атаці Єва перехоплює повідомлення і дайджести автентифікації, надіслані Алісою і Бобом в минулому, а потім повторно використовує цю інформацію в атаці «людина посередині», намагаючись видати себе за Алісу або Боба і встановити QKD з іншими сторонами. Оскільки автентифіковані повідомлення для таких процесів, як відсіювання базису, передача випадкових чисел для посилення конфіденційності, перевірка виправлення помилок і остаточна перевірка ключа, є випадковими числами, повідомлення і дайджест кожної автентифікації відрізняються. Таким чином, Єва повинна успішно виконати атаки на відтворення всіх чотирьох процесів. Для автентифікації з використанням попередньо наданих ключів, оскільки ключ між будь-якими двома користувачами є випадковим, а симетричні ключі, що використовуються для ініціювання QKD в різний час оновлюються, Єва не може використовувати раніше перехоплені

зашифровані дайджести для атаки на QKD-автентифікацію між будь-якими двома легітимними сторонами. Єва може лише потенційно запускати атаки з повтором на автентифікацію, засновану на алгоритмах з відкритим ключем, включаючи алгоритм PQC.

3.1.4 Просіювання основи

У двосторонньому процесі Єва видає себе за Алісу, перехоплює історичну інформацію про просіювання базису та підписані дайджести і намагається встановити QKD-зв'язок з іншими користувачами. Припустимо, що Єва отримала рядок базису $\{B_i,\ i = 1, 2, 3, ..., n\}$, $B_i \in \{0,1\}$, а n – довжина рядка базису. Використовуючи поляризаційне кодування як приклад, $B_i = 0$ представляє Z базис, включаючи стан горизонтальної поляризації H і стан вертикальної поляризації V, а $B_i = 1$ представляє X базис, включаючи стан +45°, вирівняний +, і стан -45°, вирівняний –. Зауважимо, що Єва не може визначити, який стан надсилати, ґрунтуючись лише на інформації про базис. У реальному QKD-зв'язку як ефективність передачі, так і ефективність виявлення є меншими за 1, тому деякі сигнали можуть бути не виявлені приймачем. Щоб імітувати реальність, Єва може випадковим чином вставляти вакуумні стани між ефективними станами сигналу. Водночас, всі стани сигналу повинні бути виявлені приймачем, щоб гарантувати, що підписаний дайджест може бути відтворений під час перевірки автентичності методом просіювання за основою.

3.1.5 Перевірка виправлення помилок

У цьому процесі надсилається лише підписаний дайджест, а ключ з виправленими помилками не надсилається.

Єва, як загальна ідентичність, не може отримати ключ з виправленням помилок, а квантові стани, що відповідають раніше перехопленому базису, невідомі. Щоб успішно виконати атаку відтворення в цьому процесі, Єва повинна попередньо встановити QKD як легітимну ідентифікацію з іншою стороною. Наприклад, Боб встановив QKD з Алісою, і в якийсь момент Боб стає зловмисником, Євою, яка намагається встановити QKD з іншим користувачем, Чарлі, видаючи себе за Алісу. Єва володіє всією інформацією про автентифікацію з Алісою, включаючи ключ з виправленими помилками та остаточний ключ, що дозволяє здійснити атаку повторного відтворення. Однак, як приймач, Чарлі має випадкову базу вимірювань, і результати вимірювань також випадкові. Навіть без врахування коефіцієнта бітових помилок, отримання однакового ключа з виправленими помилками, необхідного для атаки на повторне відтворення, є малоймовірним. Ймовірність того, що два ключі збігаються, становить приблизно 2^{-k}, де k – довжина ключа з виправленими помилками. Отже, Єва не може відтворити підписаний дайджест перевірки виправлення помилок, і навіть дайджест, підписаний алгоритмом відкритого ключа, не може бути відтворений. Аналогічно, якщо Аліса стає зловмисником, Євою, і намагається встановити QKD з Чарлі, видаючи себе за Боба, Чарлі, як передавач, модулює стани сигналу випадковим чином, і Єва не може відтворити попередній дайджест автентифікації.

Передача випадкових чисел для посилення конфіденційності: Аліса генерує випадкове число і надсилає його Бобу через автентифікацію. У цьому процесі Бобу потрібно підтвердити особу Аліси. Зловмисник може видати себе за Алісу, відтворивши випадкове число і підписаний дайджест, перехоплений раніше, поділившись тим самим випадковим числом з Бобом і побудувавши ту саму матрицю для посилення конфіденційності.

Оскільки Єва не може отримати той самий виправлений ключ, навіть після того ж процесу посилення конфіденційності, Єва не може отримати той самий остаточний ключ, що і перехоплений, що робить атаки на відтворення неможливими в цьому процесі.

4 ОПИС АРХІТЕКТУРНОЇ ІМІТАЦІЙНОЇ МОДЕЛІ ТА ЇЇ РЕАЛІЗАЦІЇ

4.1 Концепція архітектурної моделі

Потенційна можливість перехоплення квантової передачі через квантовий канал виникає через збурення. Очевидно, що такі дії можна виявити через рівень помилок квантового протоколу та присутність підслуховувача. Поєднуючи ці основні принципи з математичним доказом того, що декодування випадкового одноразового ключа з однаковою довжиною ключа і повідомлення неможливе, ефективний безпечний розподіл ключів QKD гарантує абсолютну конфіденційність між сторонами.

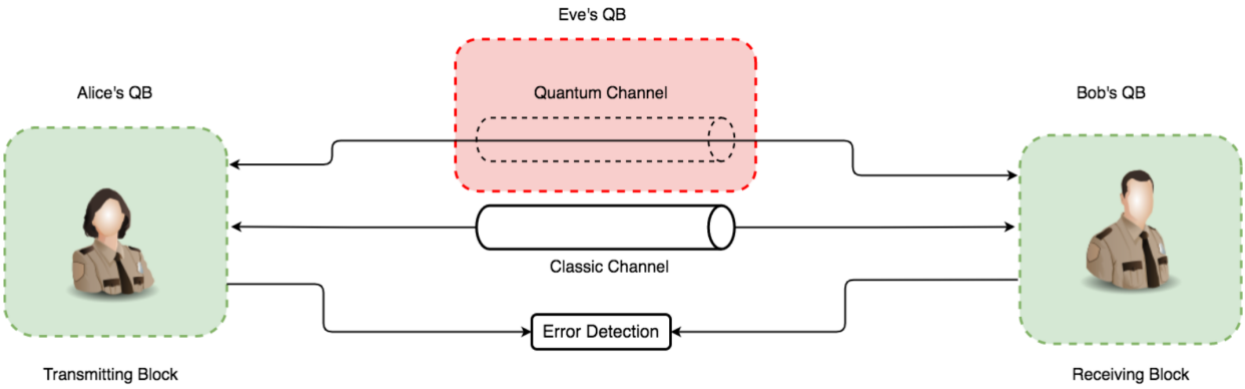

Рисунок 4.1 – Базовий огляд концепції моделювання для наступних ітерацій моделювання

Щоб продемонструвати підтвердження концепції, засноване на цих особливостях, модель архітектури зв'язку на рисунку 4.1 представляє загальну концептуальну імітаційну модель з трьома основними компонентами, які називаються квантовими блоками (QB). Ці квантові блоки представляють передавач (QB Аліси), приймач (QB Боба) і блок підслуховування (QB Єви) як несанкціонований доступ до квантового каналу.

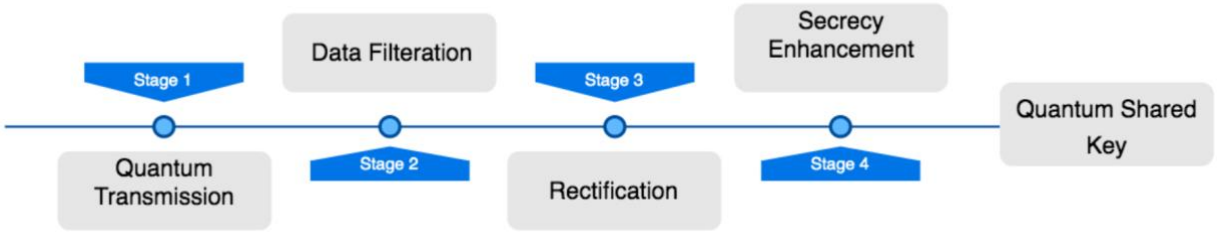

Рисунок 4.2 – Основна процедура моделювання

Комплексний процес моделювання на рисунку 4.2 демонструє фотонні детектори, які фільтрують поляризований фотон, що передається в квантовому каналі, який потім виправляється передавальними сторонами за допомогою порівняння бітів, швидкості виявлення помилок і виправлення помилок. Вихідні дані оптимізуються для підвищення безпеки, що дозволяє повному квантовому ключу спільного використання задовольнити точні вимоги безпеки за допомогою ряду процедур посилення конфіденційності.

4.2 Архітектурна модель

Модель архітектури зв'язку, показана на рисунках 4.3 і 4.4, складається з незалежних компонентів у кожному QB, що мають специфічні функції кодової бази. Кожен QB має генератор на основі фотонів (PG_b) і компонент кодера/декодера на основі фотонів (PE/D_b). Однак лише Сторони A і B мають генератор ключів (KG_b) з виходом. Два канали працюють на різних принципах: квантовий канал (безпека заснована на законах природи) і класичний канал (безпека залежить від математичної та обчислювальної складності).

Потік і схема припускають, що QB Єви може перехоплювати і повторно передавати квантовим каналом за допомогою атаки «перехоплення-відправлення».

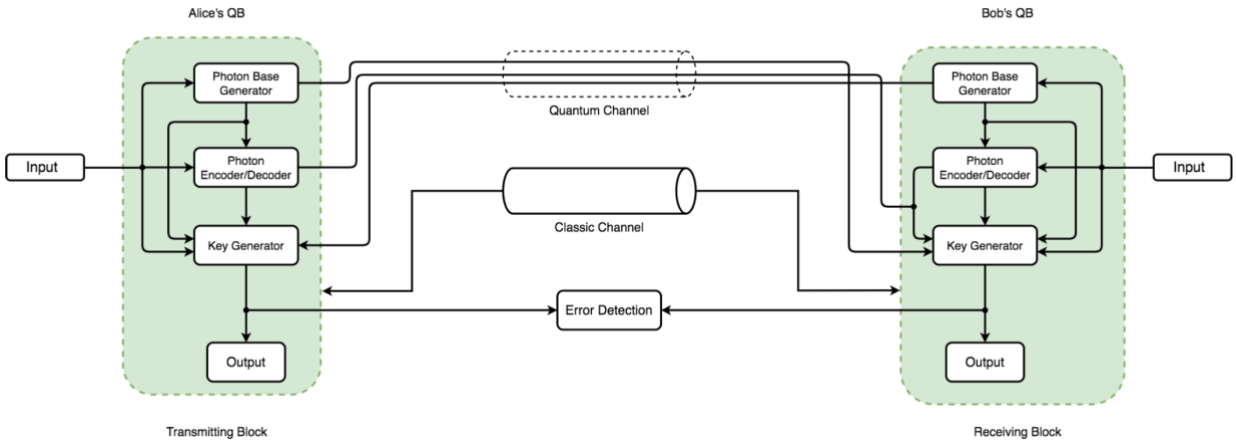

Рисунок 4.3 – Дизайн імітаційної моделі, що використовується для імітації екземпляра без присутності підслуховування (квантовий блок Єви)

Це припущення справедливе лише при обговоренні підслуховування і його впливу на канал – помилки між сторонами, що спілкуються, які контролюються за допомогою блоку виявлення помилок. Оскільки присутність Єви вимагає як фотонного генератора, так і фотонного кодера/декодера для виконання операцій повторного надсилання і перехоплення, на це вказують дві стрілки, що ведуть до квантового каналу на рисунку 4.5. Бітові потоки від роботи Єви можуть бути надіслані до приймача через квантовий канал, що ще раз надає значну перевагу для порівняння, оцінки та перевірки фундаментальної концепції, що QKD може виявити підслуховування (квантовий блок Єви) втручання в передачу даних.

4.3 Реалізація

Реалізація використовує середовище Linux, що пропонує значні переваги з точки зору кодової бази та гнучкості реалізації. Це дозволяє використовувати програмні бібліотеки та модулі з відкритим кодом. Ця симуляція моделі архітектури зв'язку використовує спеціальне середовище розробки коду Python3, як показано на рисунку 4.6. На цьому рисунку показано конфігурацію налаштування середовища моделювання та розробки. На ньому представлено стек

шарів, що складають вимоги до моделювання. Основний мовний фреймворк знаходиться поверх базової операційної системи (ОС) у базовій бібліотеці, тоді як всі зовнішні мовні модулі слугують базовими залежностями. Користувацькі бібліотеки та залежності представляють код моделювання для даної реалізації. Кожна структура коду для класів, функцій та пакетів дотримується тієї самої угоди про імена, яка використовується на рисунках 4.3 та 4.4 для забезпечення узгодженості потоку коду. Наприклад, PG_b у QB Аліси буде єдиним класом, а подальші операції будуть розділені на функції та перетворені у власний пакет. Було застосовано два різних підходи до симуляції. Перший екземпляр працював без блоку Єви як стандартний режим роботи, як показано на рисунку 4.3, тоді як другий екземпляр на рисунку 4.4 розглядав присутність QB Єви. Алгоритм у вигляді псевдокода для цієї реалізації наведено на рисунку 4.6.

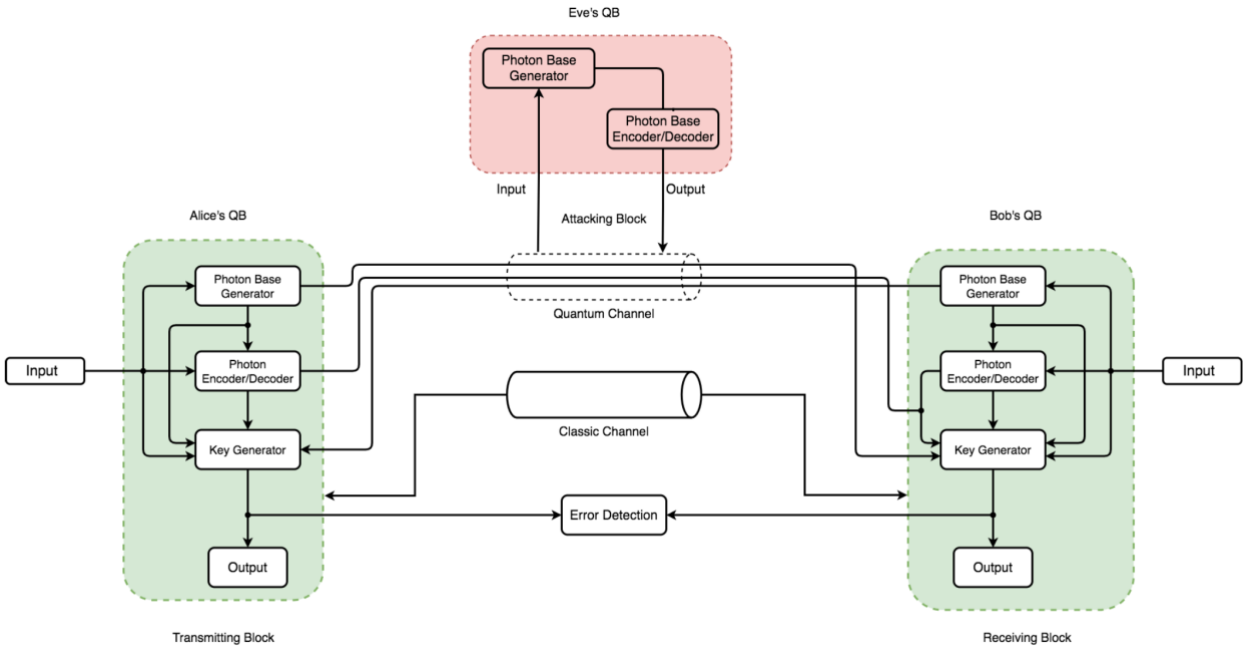

Рисунок 4.4 – Дизайн імітаційної моделі, що використовується для симуляції екземпляра з наявністю підслуховування (квантовий блок Єви)

Початкове визначення генерації бітового потоку відбувається під час симуляції для визначення точної кількості квантових базисів, необхідних для

процесу кодування. Кожен біт, що надсилається до PG_b, проходить декілька етапів. Перший крок включає в себе аналіз та оцінку каналів для точного визначення необхідних однофотонних основ для генерації. Він випадковим чином призначає квантову базу для кожного біта окремо, або горизонтально зміщену, або ортогонально зміщену. Цей крок є класом заданого поляризаційного базису, який викликає випадковий вибір зі списку, що містить квантовий базис. Кожного разу, коли виконується крок заданої поляризації, біту, присутньому в цьому конкретному екземплярі, випадковим чином присвоюється основа. Другий крок ітеративно зберігає вихідні базиси з попереднього кроку у кожному екземплярі, оскільки результат повинен досягти KG_b.

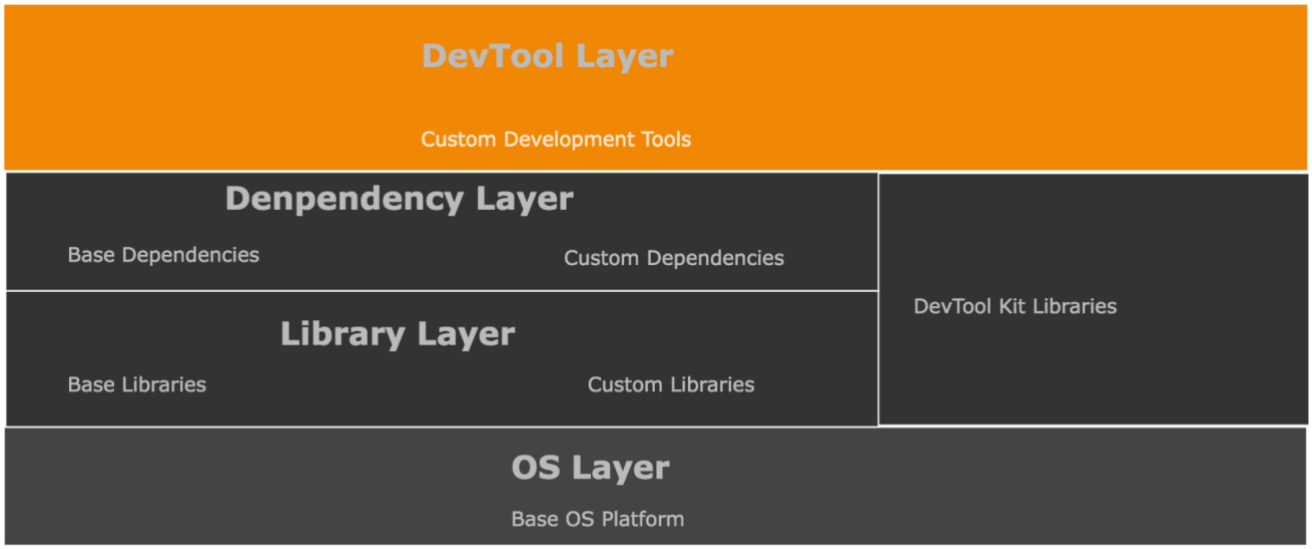

Рисунок 4.5 – Дизайн імітаційної моделі, що використовується для симуляції екземпляра з наявністю підслуховування (квантовий блок Єви)

Таким чином, ця реалізація демонструє ефективність QKD для захисту каналів зв'язку, моделюючи взаємодію між сторонами, що спілкуються (Аліса і Боб) і підслуховуючим пристроєм (Єва). Модель архітектури зв'язку, що складається з квантових блоків для кожного учасника, висвітлює процес фільтрації поляризованих фотонів, виявлення та виправлення помилок для підвищення безпеки. Завдяки використанню середовища Linux та спеціальної кодової бази

Python3, ця симуляція ефективно демонструє сильні сторони QKD у виявленні підслуховування та забезпеченні абсолютної конфіденційності між сторонами.

```
1: procedure SIMULATION PROCEDURE
2:     label: top.
3:     LBR gen ← Lower bound range of bit Random
4:     HBR gen ← Higher bound range of bit Random
5:     Base ← Base Base-MID gen – (0.5x10^10)
6:     if Base > LBR gen then return |0⟩
7:     end if
8:     if Base < HBR gen then return |1⟩
9:     end if
10:    Assign a polarization base for each iteration of bit
11:    Assign a polarization state for each iteration of bit
12:    Compare each parties' generated bit, polarization base, and polarization state
13:    Calculate mismatch rate, error correction rate, error detection rate, and total error
   rate
14:    if Errorrate > error threshold then
15:        goto top.
16:    else
17:        Strengthen the final shared key via privacy amplification
18:    end if
19:    Final shared key is ready
20: end procedure
```

Рисунок 4.6 – Моделювання коду з використанням протоколу BB84

На третьому кроці, який називається випадковою поляризацією, кожному поляризованому біту з першого кроку присвоюється окремий квантовий стан (↑→ ↖↗) за допомогою серії шаблонів прийняття рішень. Спочатку на цьому кроці перевіряються поляризаційні базиси біта і попередньо узгоджене представлення біта між сторонами, що спілкуються. Ці параметри визначають необхідний квантовий стан для кожного конкретного біта і поляризаційної основи. Результати цього етапу зберігаються для реплікації та пошуку. При цьому відправник використовує PE_b, а одержувач – декодер на основі фотонів (PD_b), і навпаки. PG_b забезпечує генерацію відповідного поляризаційного базису для початкової серії бітів. PE_b переходить до оцінки квантових основ від PG_b для кодування бітів. На цьому етапі перевіряється, чи відповідає поляризаційний базис квантовому стану

кожного біта згенерованої інформації з кроку 1 в PG_b, а потім виводиться відповідний біт. Щоб гарантувати, що дані, які використовує PE_b, походять з правильного джерела, метод, відповідальний за цю операцію, виконує перевірку довжини, типу даних, перевірки елементів і тверджень до і під час виконання коду.

По суті, відправник і одержувач погоджують біти, що представляють чотири квантові стани. Згодом сторона А генерує випадкові потоки бітів і подає їх до QB для проведення квантових операцій. Результати потім надсилаються одержувачу (Стороні Б) на початковому етапі за допомогою квантового каналу. QB Сторони В також виконує певні квантові операції і виводить результати на основі критеріїв вимірювання Сторони В. Б встановлює зв'язок по класичному каналу, інформуючи А про поляризаційні основи вимірювання. Сторона А повідомляє сторону Б тим же класичним каналом про поляризаційні базиси надісланих однофотонних імпульсів. Відправник і одержувач обмінюються інформацією один з одним, не розкриваючи ніякої конфіденційної інформації по класичному каналу. Точний процес може бути зворотньо двонаправленим, коли одержувач стає відправником і навпаки. Сторони А і В порівнюють бітові потоки з інформацією один одного на класичному каналі. Якщо обидва ключі з обох сторін рівні, результати стають квантовим ключем. Якщо рівень бітових помилок перевищує допустиме порогове значення для процесу QKD-зв'язку, процес перезапускається.

Секція KG_b в реалізації коду займається процесами фільтрації та виправлення даних. Відповідальність KG_b полягає у порівнянні даних відправника та одержувача для генерування фактичного ключа в обох половинах після виконання процесів фільтрації та виправлення даних. Він порівнює поляризаційну базу відправника та одержувача, базу вимірювань і бітовий потік з кожної сторони, а також квантові стани. Компонент виявлення помилок цієї реалізації оцінює відхилення в бітових потоках, якими обмінюються відправник і одержувач. Цей процес забезпечує генерацію загального вилучення квантового ключа, що розділяється. Цей компонент включає посилення конфіденційності та інші операції, пов'язані з остаточним квантовим ключем.

5 АНАЛІЗ РЕЗУЛЬТАТІВ ЕКСПЕРИМЕНТАЛЬНОЇ ЧАСТИНИ ДОСЛІДЖЕННЯ

Метою обох сценаріїв моделювання було надати підтвердження концепції QKD на основі принципу невизначеності та відсутності клонування, продемонструвавши переваги використання квантової криптографії для захисту інтернет-комунікацій, платформ та інфраструктур. Результати розділені на розділи, що стосуються етапів моделювання та залучених процесів. Кожен наступний розділ представляє результат на відповідному етапі моделювання та обговорює його значення.

5.1 Результати етапу комунікації

Імітаційні моделі на рисунках 4.3 і 4.4 зображують два канали комунікації, що представляють об'єкти класів. У класичному каналі відбувається узгодження параметрів, наведених у таблиці 1, між відправником та одержувачем. В літературі та теоретичних дослідженнях моделювання ККД на практиці на корекцію помилок [22] впливають фактори, пов'язані з помилками передачі, атаками, неправильними конфігураціями діодних імпульсів, часовими зсувами, недосконалими вимірюваннями та іншими аспектами загальних квантових помилок. Як наслідок, точність невизначеності в моделюванні досліджень ККД коливається від 90 до 99 відсотків. Однак у цій роботі, хоча поріг похибки з присутністю Єви перевищує цей поріг, за поріг похибки було обрано 0.11, що відповідає теорії та літературі [23]. Обидві сторони роблять це, не розкриваючи жодної критичної інформації. В результаті відправник генерує бітові потоки і пов'язані з ними квантові вихідні дані, як показано на рисунку 5.1, використовуючи нижню (0.0) і верхню (1.0) межі з точністю до десяти цифр і ймовірністю біта 0.5. Ця межа дозволяє генерувати бітові потоки для генерації основи з 50-відсотковою ймовірністю $|0\rangle$ або $|1\rangle$ для кожного примірника вибірки.

У таблиці 5.1 наведено список початкових параметрів, що використовуються при моделюванні

Таблиця 5.1 – Початкові параметри, що використовуються при моделюванні

Параметри	Значення
Довжина кубіта (біт)	256
Імовірність біта відправника	0.5
Імовірність біта приймача	0.5
Ймовірність біта зловмисника	0.5
Поріг помилки	0.11
Довжина вибірки для виявлення помилок (біт)	128

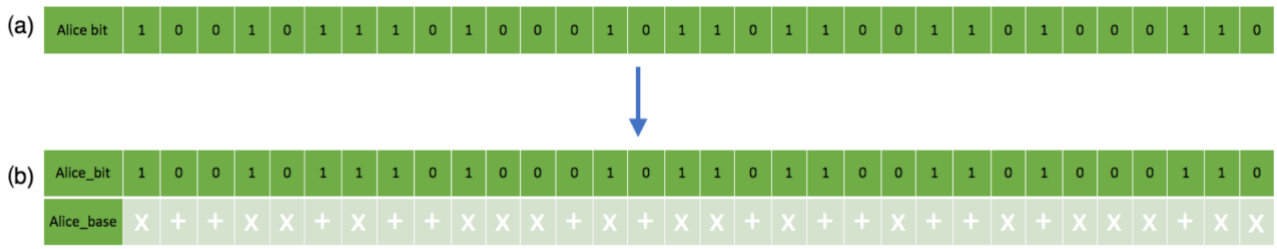

Рисунок 5.1 – Генерація бітових потоків при моделюванні: (a) – випадковий бітовий потік відправника, (b) – випадковий бітовий потік відправника з відповідними поляризаційними станами

На рисунках 5.2 і 5.3 зображено стохастичну природу процесу генерації кубітів у квантових блоках (QB) як відправника, так і отримувача для кожного бітового потоку. Рисунок 5.4 об'єднує обидва ці процеси генерації кубітів. Цей метод імітує реальні умови роботи фотонного генератора, який можна точно налаштувати для отримання потрібного окремого фотона. Початкові параметри і значення керували функцією і результатами користувацького коду протягом усього експерименту.

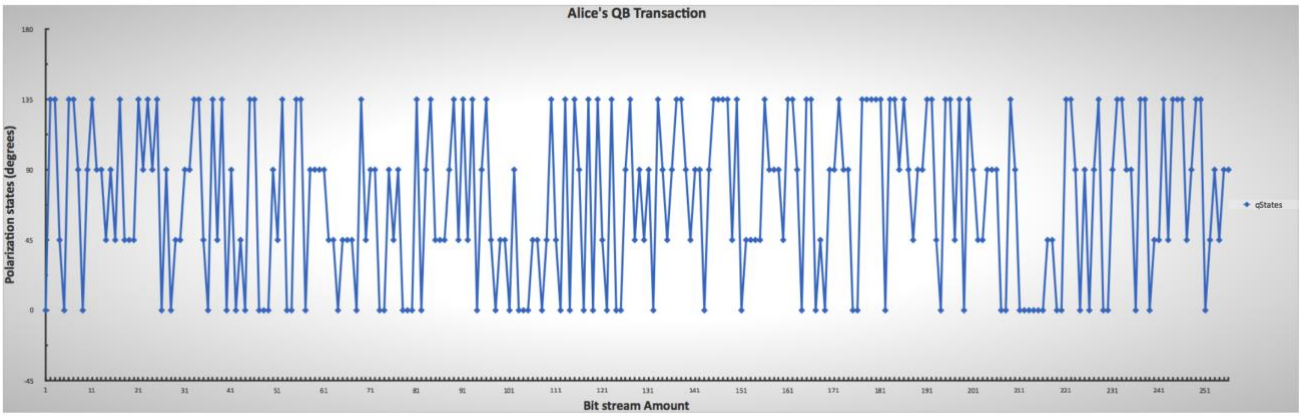

Рисунок 5.2 – Нижній і верхній граничні діапазони відправника для моделювання обраного фотонного кодування через поляризацію

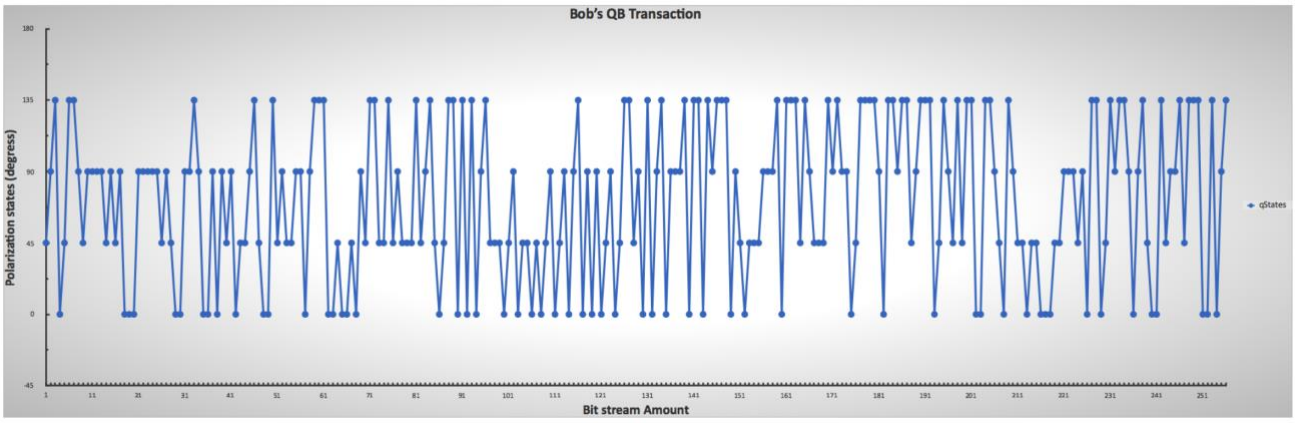

Рисунок 5.3 – Нижній і верхній граничні діапазони приймача для імітації обраного фотонного кодування через поляризацію

Що стосується приймача, то на рисунку 5.5 показано бітові та поляризаційні показники, отримані з вимірювань, проведених відправником, а також відповідні поляризаційні стани. Розбіжність між рисунками 5.5(b) і 5.1 пояснюється принципами квантової механіки (теорема про відсутність клонування і принцип невизначеності Гейзенберга). Той факт, що приймач вимірює всі однофотонні імпульси, створює збурення, змінюючи таким чином квантові стани. Приймач також припускає випадкові квантові базиси і поляризаційні квантові стани, дзеркально відображаючи базиси під бітом на рисунку 5.1(b) з випадковістю, показаною на рисунку 5.3.

5.2 Результати етапу узгодження

На етапі узгодження для перехресної перевірки коду реалізації та результатів симуляції використовується метод тверджень. Це гарантує, що кожен вузол може розрізнити специфічні для каналу операції між різними квантовими вузлами. Бази квантових вимірювань, надіслані обома сторонами, не містять відповідних квантових станів.

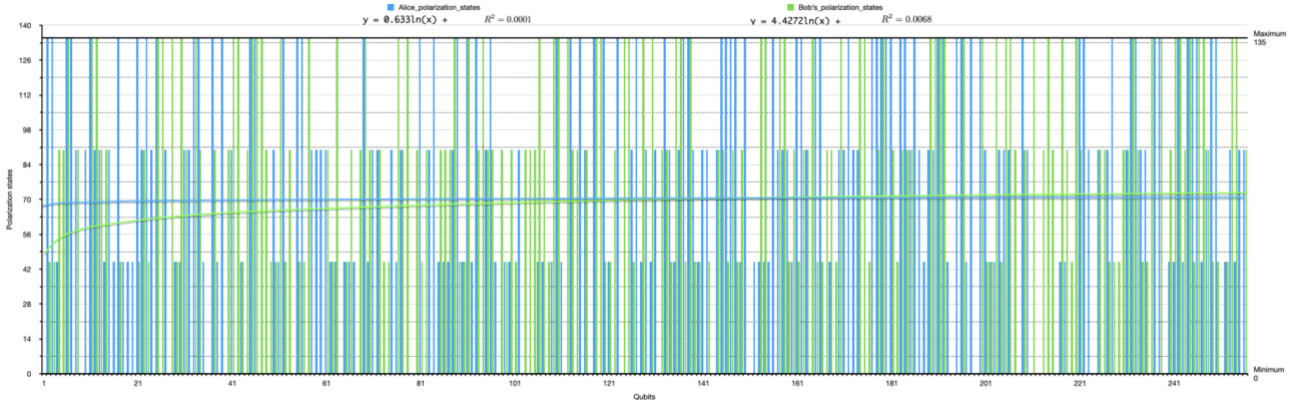

Рисунок 5.4 – Гістограма стану поляризації відправника та отримувача в першому випадку моделювання (без присутності Єви)

Відправник і одержувач звіряють вимірювання один одного, відкидаючи невідповідні бази, щоб отримати остаточний результат, як показано на рисунку 5.6.

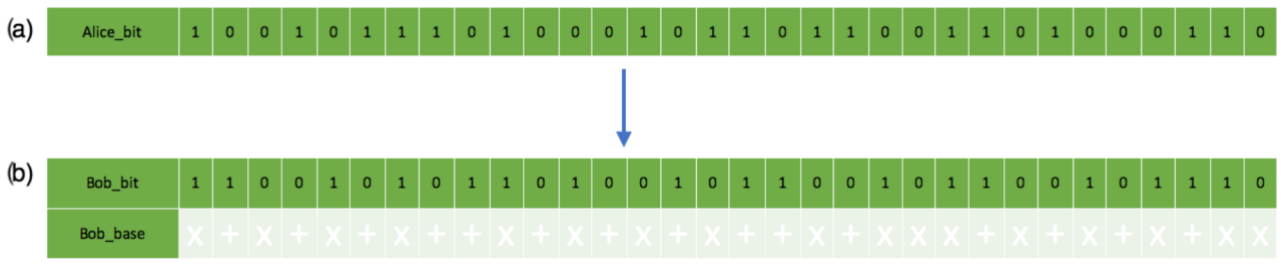

Рисунок 5.5 – Порівняння вибраних бітових потоків: (a) – опис вибраних бітових потоків відправника, (b) – опис вимірювань одержувача та обраного бітового потоку з відповідними поляризаційними станами

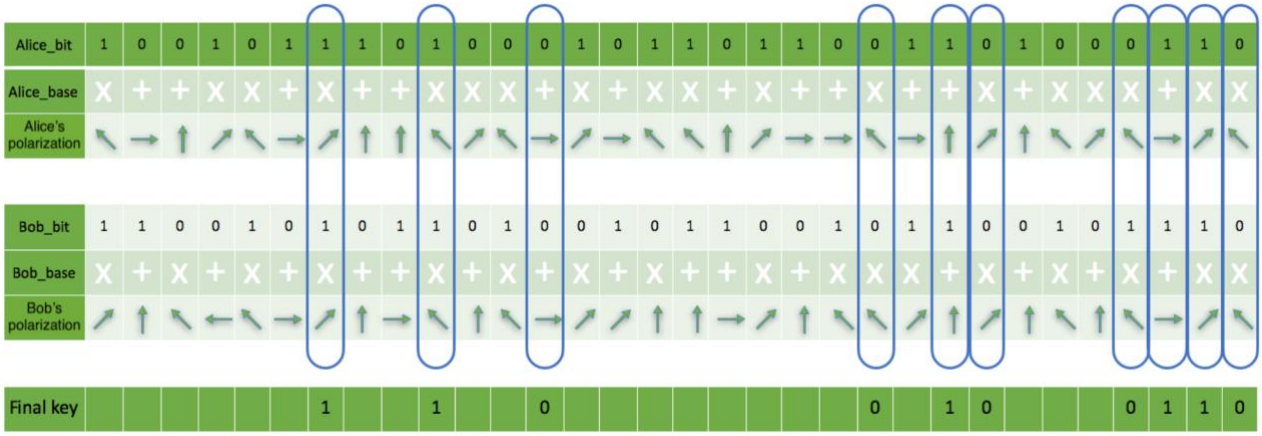

Рисунок 5.6 – Вибірка відправника та одержувача, які порівнюють вибрані результати один одного

Під час симуляції обидві сторони виявили приблизно 0,546875 неспівпадінь на основі пошуку базису в каналі зв'язку, з коефіцієнтом підслуховування 0,04296875 і коефіцієнтом виправлення помилок 0,2421875. Тим не менш, це не мало суттєвого впливу на остаточний спільний секретний ключ у повторних симуляціях. Після процесу узгодження 116 з початкових 256 кубітів залишилися в якості бітів (спільного ключа) з обох сторін.

5.3 Виявлення підслуховувача

Симуляція включала два типи операцій з перевірки помилок. Перший тип стосується кубітової помилки кожної сторони під час передачі, яка може виникнути через такі фактори, як шум, спека, умови навколишнього середовища, серед іншого. Другий тип перевірки помилок виявляє підслуховування комунікації між сторонами шляхом порівняння підключів. Для цього береться випадкова вибірка певної довжини зі спільних ключів і перевіряється, чи збігається база з початковим бітовим потоком і відправленими базами для виявлення помилок. Незважаючи на те, що помилки підслуховування і передачі вважаються однаковими в цій

симуляції, сумарні помилки не можуть перевищувати поріг помилок, зазначений в таблиці 5.1.

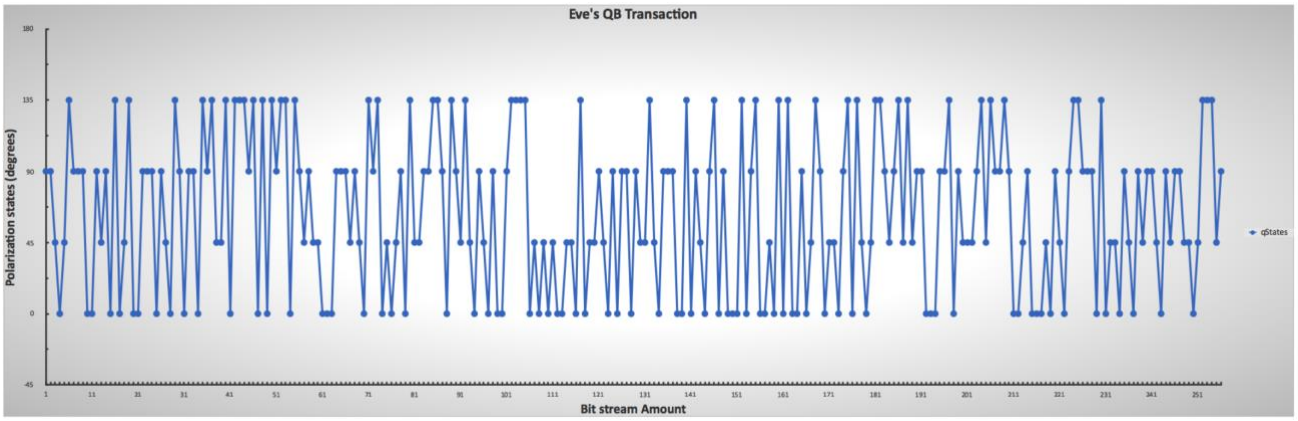

Рисунок 5.7 – Нижній і верхній граничні діапазони Єви для модулювання вимірювання фотонів і обраного кодування через поляризацію

На рисунку 5.7 показано випадковість здогадок Єви та вибраних вимірювань під час атаки перехоплення-передачі, а на рисунку 5.8 показано всі комбінації всіх сторін, де присутня Єва.

Таблиця 5.2 – Порівняння використаних базових параметрів та отриманих результатів двох основних випадків моделювання.

Параметри	Звичайний	З підслуховуванням
Початкові біти (біти)	256	256
Кінцева довжина ключа (біти)	54	36
Коефіцієнт виправлення помилок	0.2421875	0.265625
Коефіцієнт підслуховування	0.04296875	0.125
Імовірність біта сторони A, B	0.5	0.5
Імовірність біта Єва	0.5	0.5
Невідповідність (%)	0.546875	0.5234375

Результати показують, що коефіцієнт виправлення помилок 0,265625 призвів до змінної довжини спільного ключа з початкових бітів після розбіжності в основі, як показано на рисунку 5.9. Було виявлено значну різницю в швидкості підслуховування 0,125 при загальній довжині розбіжності ключа 36 після посилення конфіденційності, як показано на рисунку 5.10. У таблиці 5.2 наведено деякі ключові значення, що стосуються обох симуляцій реалізації архітектурної моделі зв'язку.

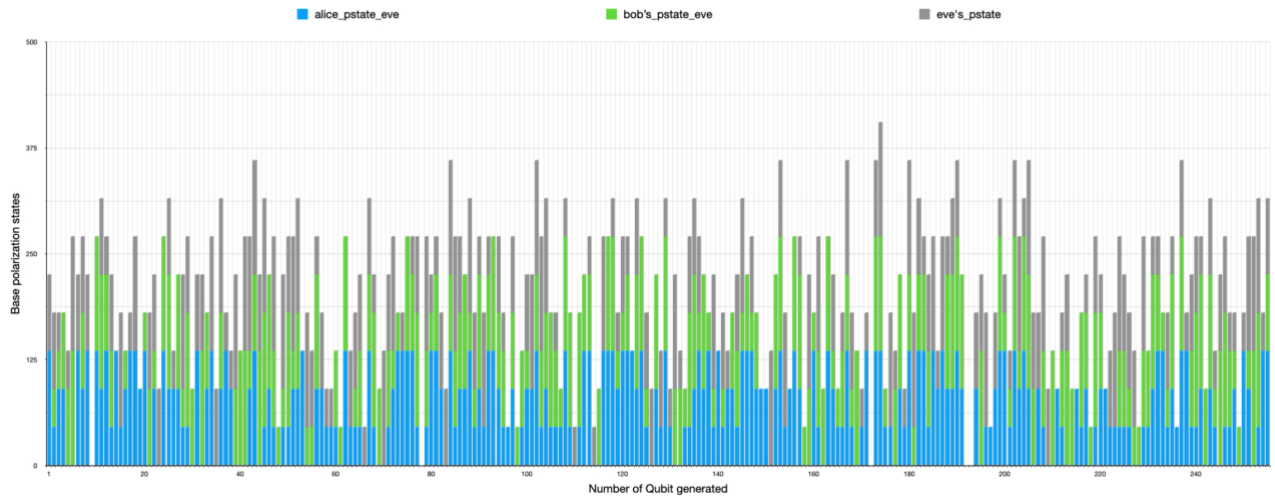

Рисунок 5.8 – Двомірна гістограма з поляризаційними станами відправника, одержувача та Єви у другому прикладі моделювання (з присутністю Єви) із зазначенням вибраної та виміряної випадковості кубітів

Як видно з рисунку 5.9, довжини двох бітових потоків відрізняються до посилення конфіденційності через присутність Єви. Єва перехоплює кубіт на квантовому каналі за допомогою атаки перехоплення-відправки, яка може бути виявлена або залишитися непоміченою, залежно від довжини ключа.

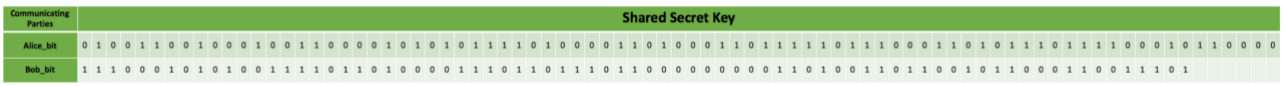

Рисунок 5.9 – Відправник і одержувач остаточно обмінюються ключем на етапі звірки в присутності підслуховувача

Communicating Parties	Shared Secret Key																																			
Alice_final	0	1	1	1	0	0	0	1	0	0	0	1	1	0	1	1	1	1	1	0	0	1	1	1	0	1	1	1	1	1	0	1	1	0	0	0
Bob_final	0	1	1	0	1	1	0	1	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	1	1

Рисунок 5.10 – Відправник і одержувач фінально повідомляють про розбіжність ключів, що свідчить про присутність підслуховувача

У цій ітерації симуляції здогадка Єви, під впливом випадковості та ймовірності, виявилася недостатньо вдалою, щоб змінити початковий спільний ключ, виміряний Бобом до посилення конфіденційності, що видно по зміні довжини/розміру.

5.4 Операції з посилення конфіденційності

Операції з посилення конфіденційності слідують за етапом виявлення і мають на меті усунення будь-якого витоку інформації через канал під час комунікаційних операцій. Присутність підслуховувача під час атаки на канал означає, що ймовірність того, що Єва вгадає правильно, дорівнює 1/4. Тому простий процес посилення конфіденційності використовує два окремі випадкові біти для операції XOR, щоб зменшити цю ймовірність. Після посилення конфіденційності залишається 54 з початкових 80 ключів від операції виявлення. Потім обидві сторони порівнюють свої результати; якщо вони збігаються, спільний ключ від виявлення залишається незмінним. Однак, якщо вони не збігаються, біт за цим конкретним індексом видаляється.

По суті, цей процес гарантує, що спільний ключ є захищеним і приватним, навіть у присутності підслуховувача. Він використовує принципи квантової механіки для побудови надійної основи для безпечної комунікації, демонструючи значний потенціал квантової криптографії у захисті цифрових інформаційно-комунікаційних систем.

ВИСНОВКИ

Основною метою цього дослідження було вивчення ефективності алгоритмів квантового розподілу ключів (QKD) у забезпеченні безпеки цифрових систем зв'язку. QKD – це процес створення і розподілу секретних ключів між двома віддаленими вузлами, використовуючи квантову механіку для забезпечення безпеки передачі ключів. Один з основних елементів QKD – це автентифікація, яка забезпечує додатковий рівень безпеки шляхом перевірки автентичності вузлів, що беруть участь у передачі ключів.

Пост-квантові безпечні алгоритми аутентифікації – це алгоритми, які можуть бути ефективно використані в умовах розвитку квантових комп'ютерів та інших квантових технологій. Ці алгоритми забезпечують безпеку, яка не може бути порушена навіть квантовими атаками.

Для QKD аутентифікація необхідна для забезпечення безпеки передачі ключів. Вона дає змогу переконатися, що вузли, які беруть участь у передачі ключів, є дійсними і не були підмінені зловмисником. Для цього можуть використовуватися різні методи автентифікації, такі як автентифікація на основі пароля, автентифікація на основі сертифікатів тощо.

В результаті дослідження було зроблено такі висновки:

– дослідження продемонструвало, що системи контролю якості можна успішно моделювати в цифровому середовищі за допомогою спеціального коду та імітаційних моделей. Результати дослідження підтвердили концепцію систем QKD, заснованих на принципі невизначеності та відсутності клонування, демонструючи потенціал квантової криптографії для захисту цифрових комунікаційних платформ та інфраструктур;

– дослідження показало, що компоненти виявлення та виправлення помилок в системах QKD відіграють вирішальну роль у підтримці безпечного зв'язку. Порівнюючи дані відправника та отримувача, ці механізми можуть

ефективно виявляти відхилення та забезпечувати генерацію точного спільного квантового ключа;

– присутність підслуховувача суттєво впливає на безпеку систем QKD. Однак, впроваджуючи процеси посилення конфіденційності та безперервної перевірки на наявність потенційного підслуховування під час процесу комунікації, безпеку спільного ключа можна значно підвищити;

– дослідження показало, що посилення конфіденційності може ефективно зменшити ймовірність того, що підслуховувач вгадає правильний ключ. Виконуючи певні операції над випадковими бітами, можна значно підвищити безпеку спільного ключа;

– дослідження підтвердило, що збереження випадковості при генерації бітового потоку є важливим для ефективної роботи систем QKD. Процес генерації Qubit відправником і одержувачем продемонстрував високий ступінь випадковості, імітуючи умови в реальному фотонному генераторі.

Загалом, це дослідження надало цінну інформацію про ефективну реалізацію та оптимізацію систем QKD. Отримані результати можуть мати значні наслідки для широкого кола галузей, пропонуючи надійне рішення для зростаючого виклику кіберзагроз. Майбутні дослідження повинні бути спрямовані на подальшу оптимізацію механізмів виявлення та виправлення помилок і процесів посилення конфіденційності в системах QKD для забезпечення ще більшої безпеки цифрових систем зв'язку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Architecture and protocols of the future European quantum key distribution network / Mehrdad Dianati, Romain Alléaume, Maurice Gagnaire, and Xuemin (Sherman) ShenMilton. // John Wiley & Sons, Ltd., Paris, France, security comm. networks – 2008.

2. Secure Communication Using Cryptography and Covert Channel / Tamer S.A. Fatayer // Computer and Network Security – 2020

3. Механізми підвищення швидкодії криптографічних бібліотек для кінцевих користувачів у хмарних технологіях / Качко О.Г., Аулов І.Ф. // Міжнародна наукова школа – семінар Питання оптимізації обчислень (ПОО-XLII) 21-25 вересня 2015. Україна, Закарпатська область, Мукачівський район, смт Чинадієво

4. The problem of standardization of cryptotransformations for the post-quantum period and the state of its solution at the international and national levels / I.D. Gorbenko, O.G.Kachko, M. V. Yesina // Міжнародна науково-технічна конференція Захист інформаці і безпека інформаційних систем Праці Науково-технічної конференції, 11–12 листопада 2021 р. – Л. : Національний університет «Львівська політехніка!»

5. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / R.L. Rivest, A. Shamir, L. Adleman // Communications of the ACM, Volume 21, Issue 2, New York – 1 February 1978

6. Quantum cryptography: Public key distribution and coin tossing. / C. H. Bennett and G. Brassard. // IEEE International Conference on Computers, Systems and Signal Processing, New York – 1984.

7. Quantum Cryptography: An Emerging Technology in Network Security. / Mehrdad S. Sharbaf. // IEEE, California – 2011.

8. Simple proof of security of the bb84 quantum key distribution protocol. / Shor, P. W. & Preskill, J. // Physical review letters 85, 441 –2000

9. Quantum cryptography with imperfect apparatus. / Mayers, D. & Yao, A. // In Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), 503–509 (IEEE) – 1998

10. Practical issues in quantum-key-distribution postprocessing. / H. F., Ma, X. & Chau, H. F. Phys. // Rev. A 81, 012318 – 2010

11. Quantum key distribution in the classical authenticated key exchange framework. / Mosca, M., Stebila, D., Ustaoglu B. // In Gaborit, P. (ed.) Post-Quantum Cryp- tography, vol. 7932 of Lecture Notes in Computer Science, 136–154 (Springer Berlin Heidelberg) – 2013

12. Unconditional security of quantum key distribution over arbitrarily long distances / Lo, H.-K. & Chau, H. F.. // science 283, 2050–2056 – 1999

13. Finite-key security analysis for quantum key distribution with leaky sources / Weilong Wang, Kiyoshi Tamaki, and Marcos Curty // arXiv, Japan – 2018.

14. The security of practical quantum key distribution. / Scarani, V. // Rev. Mod. Phys. 81, 1301 – 2009

15. Algorithms of Asymmetric Encryption and Encapsulation of Keys of Post Quantum Period of 5-7 Levels of Stability and their Applications / I.D. Gorbenko, O.G.Kachko, A.N. Aleksiychuk, O.O. Kuznetsov // ISSN 0485-8972 Радіотехніка, вып. 198 – 2019

16. On A Class of Error Correcting Binary Group Codes. / R. C. Bose and D. K. Ray-Chaudhuri // Information and Control, North Carolina, 3 (1): 68–79, issn 0890-5401 edition – 1960.

17. Two Practical and Provably Secure Block Ciphers: BEAR and LION / Rose Anderson and Eli Biham // Springer, England, 3rd international workshop on fast software encryption edition – 1996.

18. Authentication of quantum key distribution with post-quantum cryptography and replay attacks / Liu-Jun Wang, You-Yang Zhou, Jian-Ming Yin, Qing Chen // School of Physics and Astronomy and Yunnan Key Laboratory for Quantum Information, Yunnan University, Kunming 650500, China – 2022

19. Experimental authentication of quan- tum key distribution with post-quantum cryptography / Wang, L.-J. et al. // npj quantum information 7, 1–7 – 2021

20. New hash functions and their use in authentication and set equality / J. Lawrence Carter and Mark N. Wegman // Journal of computer and system sciences, USA, 22.3 p: 265-279 edition – 1981.

21. Performance Analysis of Post-Quantum Algorithms / F. Lauterbach, P. Burdiak, F. Richter, M. Voznak // 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia – 2021

22. R.P. Quantum Information Science / Swan, M.; Witte, F.; dos Santos // *IEEE Internet Comput. 26*, 7–14, – 2022

23. Security Analysis of QKD Protocols: Simulation and Comparison / Khan, E.; Meraj, S.; Khan, M.M. // In Proceedings of the 2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 14–18 January 2020; pp. 383–388