Дослідження сучасного стану технологій квантового розподілу секретних ключів

Сергій Лєнков[1], Володимир Джулій[2], Ігор Муляр[3], Євген Лєнков[4]

[14]Військовий інститут Київського національного університету імені Тараса Шевченка
Юлії Здановської, 81, Київ, Україна, 03189
[1] lenkov_s@ukr.net https://orcid.org/0000-0001-7689-239
[2]Хмельницький національний університет
вул. Інститутська, 11, Хмельницький, Україна, 29000
[2]dzhuliivm@khmnu.edu.ua, http://orcid.org/0000-0003-1878-4301,
[3]muliariv@khmnu.edu.ua, 0000-0002-6659-605X,
[4]Міністерство енергетики України
вул. Хрещатик, 30, Київ, Україна, 01001
[4]lenkov85es@gmail.com, https://orcid.org/0000-0001-5819-2656

Received 03.02.2025, accepted 29.03.2025
https://doi.org/10.32347/st.2025.3.1201

Анотація. Робота присвячена дослідженню задач використання технології квантового розподілу секретних ключів, а саме задачам використання та формування нових секретних ключів, ґрунтуючись на виробленні квантових ключів та розподілу нових ключів у мережа складних топологій.

В системах захищеного зв'язку інформація передається мережами загального користування, і таким чином, доступна потенційному порушнику для проведення різного роду атак. Потенційний порушник здатний зберігати шифровані дані, що передаються по каналах мережі, а спробу дешифрування робити пізніше, коли технічні засоби та атаки на алгоритми захисту інформації дозволять, за прийнятний час, провести дешифрування. У цьому полягає основний принцип "Store now, decrypt later", що є однією з проблем систем захисту інформації [1, 2,19].

Для блокових шифрів існує параметр - навантаженням на ключ, який обмежує об’єм інформації, яку може обробити один ключ із використанням алгоритму захисту даних. NIST рекомендує часові рамки використання секретних ключів, що обчислюються роками [3,6].

У сфері інформаційної безпеки є суттєвіші обмеження навантаження на ключ, пов'язані з числом блоків, які можна на одному ключі обробити, обумовлені атаками на блокові шифри. При даних обмеженнях виникає необхідність регулярної зміни використовуваного секретного ключа, та пошук варіантів генерації та доставки ключів між двома вузлами мережі, що організовують захищений канал передачі інформації.

Зміна секретного ключа на новий ключ, незалежний від попереднього, дозволяє захистити передачу конфіденційної інформації при компрометації використовуваного ключа.

Сергій Лєнков
д.т.н. професор, головний науковий співробітник

Володимир Джулій
Доцент кафедри кібербезпеки

Ігор Муляр
к.т.н., доцент, ст. викладач кафедри кібербезпеки

Євген Лєнков
Провідний спеціаліст

Технологія створення квантового комп'ютера дозволяє атакувати ефективно відомі алгоритми генерації секретних ключів, що базуються на факторизації великих чисел, чи складності обчислення дискретного логарифму. Квантовий алгоритм Шора [3-5,15] дозволяє вирішувати дані задачі за поліноміальний час, тому необхідно шукати альтернативні варіанти вирішення задачі регулярної зміни в каналі мережі секретного ключа в парі вузлів.

Важливо враховувати необхідність забезпечення якості Perfect forward secrecy, при компрометації майстер-ключа, всі наступні секретні ключі повинні бути не скомпрометованими. Для досягнення такої властивості сучасних алгоритмів шифрування є періодичне оновлення майстер-ключів.

Для запобігання накопиченню інформації, для успішного здійснення атак порушником та дотримання вимоги навантаження на секретний ключ необхідно вирішити задачу регулярної зміни секрета, та регулярної генерації/доставки ключів у вузли мережі.

З урахуванням нагальних потреб, що на сьогоднішній день інтенсивно розвиваються, у захищеній та швидкісній передачі інформації, та не менш, стрімкому зростанні технічних можливостей, існує потреба розробляти заздалегідь варіанти, які забезпечуть при передачі інформації її захищеність. Регулярна зміна, у географічно рознесених системах захисту даних, загальних секретних ключів, у разі забезпечення незалежності секретних ключів дозволяє вирішити успішно поставлену задачу.

Ключові слова: інформаційна безпека, вразливості, атаки, квантовий секретний ключ, протокол квантового розподілу.

ВСТУП

Серед сучасних технологій генерації та доставки секретних ключів можна виділити два підходи: розподіл секретних ключів з використанням технології квантового розподілу ключів; генерація секретних ключів між двома учасниками мережі з використанням пост-квантових алгоритмів.

Другий варіант полягає в складних математичних обчисленнях. Сучасний рівень опрацювання пост-квантових алгоритмів недостатній для їхнього впровадження в існуючі системи. Існує небезпека, що після створення ефективного квантового комп'ютера будуть запропоновані квантові алгоритми, що дозволяють ефективно вирішувати задачі, використовувані в пост-квантових алгоритмах, створять нові вектори атак на пост-квантові алгоритми та вимагатимуть нові підходи регулярної доставки секретних ключів.

Проблема розподілу секретних ключів між парами вузлів мережі є актуальною науковою проблемою, яка потребує вирішення в умовах розробки нових загроз, пов'язаних зі створенням квантового комп'ютера.

Існуючі на сьогодні рішення розроблялися до розвитку квантових обчислень і комунікацій, не враховують із застосуванням квантових пристроїв нові вектори атак.

Варіант розподілу секретних ключів із застосуванням технології квантового розподілу є найперспективнішим для вирішення поставленої проблеми. Генерація ідентичних квантових секретних ключів на двох кінцях вузлів мережі квантового каналу ґрунтується на інших фізичних принципах, що надає можливість запобіганню проведення ефективних атак (загроз) із застосуванням квантового комп'ютера, також не дозволяє проводити атаки із накопиченням об’єму захищеної інформації.

Технологія квантового розподілу ключів має істотні обмеження, які необхідно враховувати під час проектування систем генерації/доставки секретних ключів з урахуванням квантового розподілу. Технологія квантового розподілу ключів здійснює розподіл ключів на обмеженій відстані (визначається протоколом квантового розподілу ключів) та якістю квантового каналу.

Для протоколів на InGaAs/InP граничним є відстань близько 100 км [5,6,13,14].

Найпростішим прикладом із застосуванням квантового розподілу ключів є використання двох екземплярів квантової апаратури, з'єднаних квантовим каналом. Для вирішення задачі обмеження довжини квантового каналу апаратура квантового розподілу ключів об'єднується, у так звані,

мережі квантового розподілу ключів. Для отримання дійсно квантового ключа між двома вузлами мережі, які не пов'язані квантовим каналом, необхідно використання технології квантових повторювачів, які на сьогодні далеко від практичної реалізації.

Реалізований на сьогодні підхід, полягає у побудові мереж квантового розподілу ключів з урахуванням довірених проміжних вузлів мережі. При такому підході секретні квантові ключі виробляються тільки між вузлами мережі з'єднаними безпосередньо квантовим каналом.

На інші вузли квантової мережі квантові секретні ключі передаються під захистом інших згенерованих секретних квантових ключів.

У мережах квантового розподілу ключів необхідно передавати не тільки ключову інформацію із застосуванням секретних квантових ключів по ланцюжку вузлів квантової мережі, але також здійснювати дані процеси в мережах зв'язку змішаної топології загального користування. Змішана топологія - топологія зв'язків вузлів квантовими каналами, так і топологія класичних зв'язків між вузлами мережі (мережа зв'язків загального користування), також захищені канали взаємодії між вузлами квантової мережі, при цьому граф, що відображає зв'язки квантовими каналами, має бути зв'язковим.

З урахуванням нагальних потреб, що на сьогоднішній день інтенсивно розвиваються, у захищеній та швидкісній передачі інформації, та не менш стрімкому зростанні технічних можливостей, існує потреба розробляти заздалегідь варіанти, які забезпечуть при передачі інформації зберегти її захищеність.

Регулярна зміна, у географічно рознесених системах захисту даних, загальних секретних ключів, у разі забезпечення незалежності секретних ключів дозволяє вирішити успішно поставлену задачу.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПОСТАНОВКА ЗАДАЧІ

Технологія квантового розподілу ключів-отримання ідентичних випадкових послідовностей абонентами, отриманих із використанням передачі між абонентами деякої інформації, з використанням квантових частинок. Абоненти використовують квантові пристрої, що реалізують протокол квантового розподілу ключів.

Протокол квантового розподілу ключів включає: підготовку та перетворення інформаційних квантових станів в пристрої, який повинен мати джерело квантових станів; спосіб передачі квантовим каналом інформаційних квантових станів; спосіб інтерпретації, реєстрації та перетворення результатів вимірювань на з'єднаному пристрої; спосіб обробки отриманої за результатами вимірювань, послідовності, із застосуванням відкритого автентифікованого каналу зв'язку. Результатом роботи протоколу квантового розподілу ключів є отримання секретного квантового ключа, ідентичного на обох вузлах мережі квантового каналу.

Квантовий комплекс, що реалізує протокол квантового розподілу ключів, є апаратура з двох пристроїв, з'єднаних квантовим каналом. Архітектура комплексу наведена на Рис. 1. Клієнт квантового розподілу ключів містить джерело (генератор) одиночних фотонів. Під'єднаний пристрій, що містить приймач (детектор) одиночних фотонів, називають

Сервер квантового розподілу ключів. Кожен із вузлів квантового каналу містить датчик випадкових чисел. Таким чином, можна отримати випадкову істинну послідовність, з якої в подальшому буде формуватиметься квантовий секретний ключ.

Сервер та Клієнт квантового розподілу ключів з'єднані двома логічними каналами: класичним та квантовим. Квантовий канал, зазвичай реалізується оптоволокном, призначений для передачі фотонів, квантових інформаційних станів. Існують системи квантового розподілу ключів, в

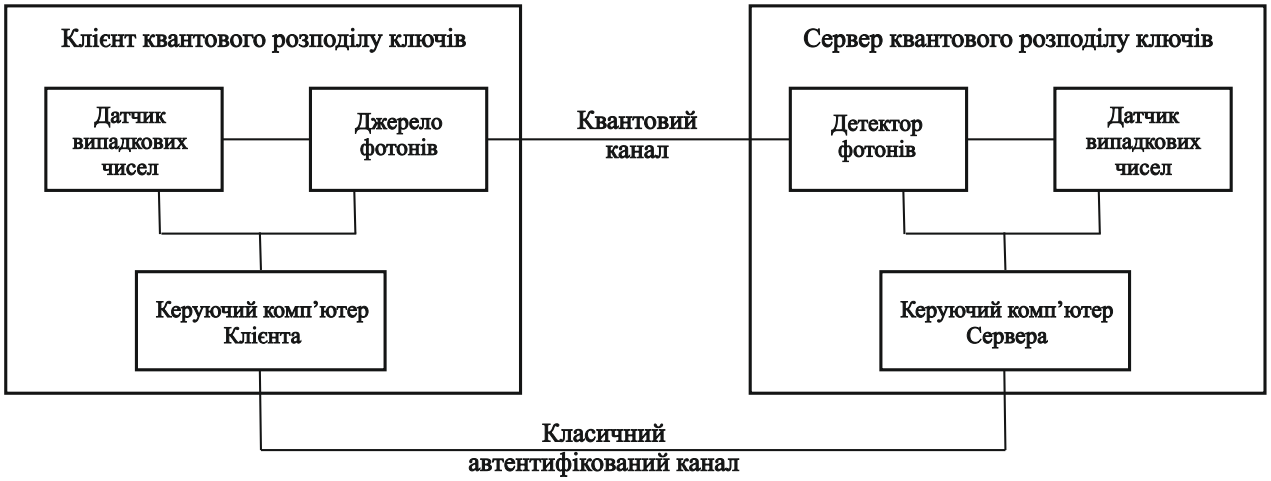

Рис. 1. Спрощена архітектура комплексу квантової апаратури

яких використовується повітряне середовище передачі, як квантовий канал, проте вони зна-ходяться ще в стадії лабораторних розробок [5,10,15,17,20].

Важливою особливістю технології квантового розподілу ключів є повна доступність потенційого порушника до квантового каналу, цей канал не захищається і не контролюється від доступу порушника до квантового каналу

Крім квантового каналу Клієнт і Сервер квантового розподілу ключів повинні з'єднуватися класичною лінією зв'язку мережі, в якій реалізується класичний логічний канал зв'язку - класичний автентифікований канал.

До автентифікованого каналу пред'являються вимоги щодо забезпечення автентифікації відправника інформації та цілісності даних.

Реальна система квантового розподілу ключів, також має логічний службовий канал, що з'єднує Сервер та Клієнт квантового розподілу ключів, по якому передаються дані моніторингу апаратури та управління, команди, які не пов'язані безпосередньо з протоколом квантового розподілу ключів. Залежно від конкретної реалізації системи квантового розподілу ключів, склад цих даних і команд може вимагати забезпечення не тільки цілісності інформації, також її конфіденційності. Для функціонування системи квантового розподілу ключів в апаратуру необхідно завантажити попередньо розподілені секретні ключі, які будуть використанні при побудові класичного автентифікованого каналу мережі до першої успішної генерації достатньої кількості квантових секретних ключів.

Одна ітерація реалізації протоколу квантового розподілу ключів - сеанс квантового розподілу ключів. Сеанс квантового розподілу ключів складається з наступних етапів: підготовка квантового каналу; передача одиночних фотонів квантовим каналом мережі; пост-обробка переданої послідовності даних.

Перші два етапи задіють квантовий канал мережі. Результатом передачі квантовим каналом є сирий ключ у обох пристроїв.

Останній етап протоколу квантового розподілу ключів виконується з використанням класичного автентифікованого каналу без квантового каналу мережі.

Постобробка включає наступні три підетапи: узгодження базисів виміру на стороні Сервера з базисами шифрування квантових станів на стороні Клієнта. Під час узгодження позицій сирого ключа, у яких базиси не співпали, відкидаються, в результаті сирий ключ перетворюється на просіяний ключ; в отриманих просіяних ключах виправлення помилок з метою отримання ідентичні послідовності даних на Клієнті та Сервері квантового розподілу ключів. Результатом виправлення помилок є очищений ключ; посилення секретності, представляє стиск отриманих ідентичних послідовностей даних з метою зменшення

інформації про згенерований квантовий ключ, доступної порушнику.

Результатом посилення секретності очищений квантовий ключ перетворюється на секретний ключ.

Результатом сеансу квантового розподілу ключів є випадкова квантова гама, ідентична у абонентів квантового каналу, таким чином даний результат має змінну довжину, яка не завжди співпадає з довжиною секретних ключів, які використовуються в алгоритмах шифрування. Результат виконання протоколу квантового розподілу ключів істотно відрізняється з високими та низькими втратами для квантових каналів мережі, які впливають на величину помилок при передачі в квантовому каналі мережі, що в свою чергу впливає на величину квантової гамми, та доступна порушнику на етапі посилення секретності.

Для шифрування інформаційного стану протоколу квантового розподілу ключів необхідно щонайменше два біти інформації, один біт визначає базис вимірювання (шифрування), другий значення інформаційного біта 1 або 0. Більш складні протоколи квантового розподілу ключів [5,6,21] можуть мати 3 і більше біт для шифрування інформації в однофотонному стані. На основі експериментальних даних для одного сеансу квантового розподілу ключів необхідна випадкова послідовність даних довжиною не менше біт. Швидкість генерації датчика випадкових чисел для отримання 256 бітного ключа за секунду має бути не менше біт/с або 400 Мбіт/с. Якщо, при цьому, врахувати, що частина квантового секретного ключа використовується для аутентифікації наступного сеансу квантового розподілу ключів мережі, тому необхідно враховувати розмір ключа аутентифікації, що, в свою чергу, збільшить нижню оцінку швидкості датчика генерації випадкових чисел.

До датчиків генерації випадкових чисел в системах квантового розподілу ключів пред'являють відповідні вимоги, до природи випадковості та якості формуємої послідовності даних [15,17,23]. Швидкість фізичних датчиків, в основі яких лежать квантові процеси, обмежена, в результаті призводить до обмеження швидкостей генерації квантових ключів швидкостями датчиків випадкових послідовностей [6,17,21].

Для коректної побудови протоколу квантового розподілу ключів та отримання відповідної якості квантових секретних ключів необхідна передача інформації по квантовому каналу мережі, побудова автентифікованого класичного каналу та наявність датчика випадкових послідовностей відповідної якості для створюваних квантових ключів.

Проведене дослідження робіт, що описують фізичну сторону технології квантового розподілу ключів, не приділяють відповід-ної уваги побудові аутентифікованого класичного каналу мережі. Для створення квантового каналу зв’язку необхідно визначити підхід до забезпечення аутентифікації джерела даних та цілісності інформації. Відповідним рішенням є обчислення імітовставки від послідовностей, для забезпечення цілісності інформації.

Аутентифікація відправника послідовностей здійснюється за рахунок використання секретного загального ключа, відомого, при цьому, лише парі легітимних абонентів.

Квантові пристрої не використовуються самі по собі, а є джерелом загальних секретів легітимних абонентів для систем захисту, апаратури. Автентифікований класичний канал з’єднання, через різні причини, (для економії числа фізичних каналів), може бути реалізований з використанням системи захисту інформації.

У роботі квантових пристроїв необхідно враховувати, що можливі множинні та одноразові переривання сеансу квантового розподілу ключів, через порушення у автентифікованому класичному каналі цілісності даних у зв'язку з випадковими збоями чи діями порушника. Повторний запуск сеансу квантового розподілу ключів веде до втрат секретних ключів автентифікації.

Іншою проблемою, є передача згенерованого квантового ключа від

квантових пристроїв легітимним абонентам, (пристроям, які використовуватимуть квантовий ключ). На відміну від класичних систем, взаємодія квантових пристроїв із системою захисту відбувається у двох парах пристроїв одночасно:

Сервер квантового розподілу ключів – система захисту та Клієнт квантового розподілу ключів – система захисту інформації. Квантовий секретний ключ створюється в одній парі квантових пристроїв, а передаватися повинен в пару інших пристроїв, систему захисту. При цьому, небезпечно застосування алгоритмів шифрування, не стійких до загроз (атак) із застосуванням квантового комп'ютера.

Формування асиметричними методами загальних секретів небезпечне через загрози із використанням квантового комп'ютера. Отже, можна визначити ряд невирішених проблем у розподілі спільних секретів із застосуванням квантового розподілу ключів в мережі: спосіб організації автентифікованого класичного каналу апаратури квантового розподілу ключів, що включає підхід до формування імітовставки для забезпечення цілісності даних та джерело секретних ключів для формування імітовставки; організація захищеної передачі загальних секретів абонентів у системах захисту інформації, стійкою до загроз (атак) квантовим комп'ютером; необхідність синхронізації ключової гами, в умовах відсутності можливості взаємодії систем захисту до отримання первинних ключів.

Вирішення перерахованих проблем дозволить застосовувати технологію квантового розподілу ключів для систем топології «крапка-крапка» для розподілу загальних секретів абонентів в пристрої користувача.

ДОСЛІДЖЕННЯ МЕТОДІВ ПОБУДОВИ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЙ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ

Протоколи квантового розподілу ключів мають граничну довжину квантового каналу мережі, де можливо створення спільних квантових ключів. У середньому максимальна довжина квантового каналу мережі для волоконних систем квантового розподілу ключів становить 100 км [5,6,13]. Пристрої, на які необхідно передати квантові ключі, розташовуються довільно.

Таким чином, постає задача подолання граничної віддаленості пристроїв квантової апаратури мережі з метою генерації загальних секретів для пар легітивних абонентів з необмеженою відстанню між ними.

Вирішення проблеми максимальної віддаленості легітимних абонентів є використання одного з двох підходів: застосування мереж квантового розподілу ключів на основі недовірених проміжних вузлів мережі; застосування мереж квантового розподілу ключів на основі довірених проміжних вузлів мережі. У кожному випадку використовуються мережі змішаної топології, в яких необхідно розподіляти квантові ключі.

В основі мереж квантового розподілу ключів з недовіреними проміжними вузлами лежить застосування комірок квантової пам'яті, розташованих на проміжних вузлах [4,6,15,17].

На сьогодні квантова пам'ять є абстрактним об'єктом, не має фізичного втілення, мережі з недовіреними проміжними вузлами і є перспективним, але з не реалізованим підходом найближчим часом.

Основа мереж квантового розподілу ключів з довіреними проміжними вузлами мережі є послідовна передача загального секрета (квантового ключа), отриманого на сегменті мережі квантового розподілу ключів через проміжні вузли мережі на відповідні вузли, на які розподіляється загальний секрет [6,11,14].

На кожному вузлі квантової мережі відбувається перекодування квантового ключа (загального секрету), і він доступний у відкритому вигляді на проміжних вузлах квантової мережі.

Таким чином, вузли квантової мережі повинні бути довіреними та забезпечений неможливий доступ порушника до квантових ключів, які у відкритому доступі на вузлах квантової мережі. Як алгоритм шифрування, в технології квантового

розподілу ключів, вибирають One-Time Pad Encryption (одноразовий шифроблокнот) [16 – 18,21].

Одним із варіантів вирішення проблеми появи загального секрету у відкритому виді на проміжних вузлах квантової мережі є застосування класичних стандартизованих підходів для захищеного представлення загального секрету на проміжних вузлах квантової мережі. Загальна схема магістральної мережі квантового розподілення ключів, представлена на Рис. 2.

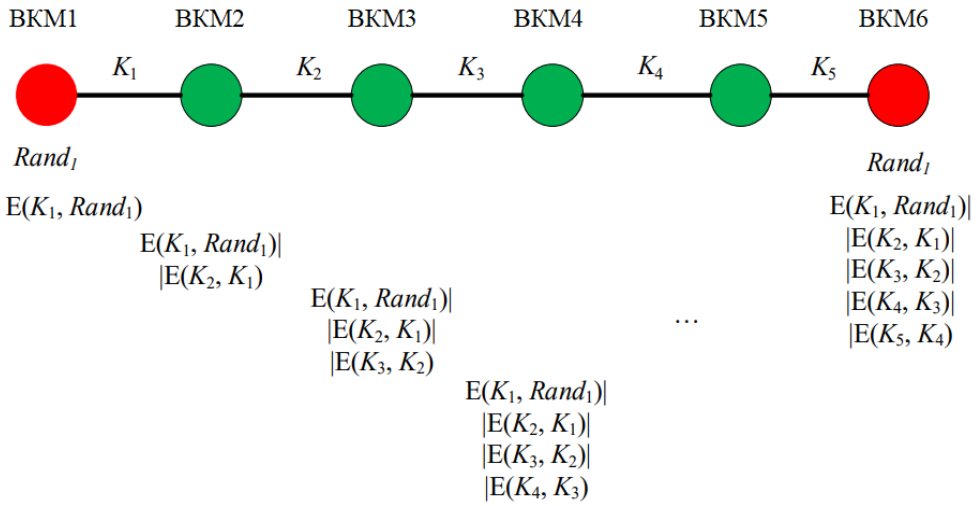

Рис.2. Метод формування квантового ключа «стеком»

Для захисту ключової інформації (загальний секрет) цільових вузлів квантової мережі, використовується загальний секрет першого сегмента мережі квантового розподілу ключів.

Формується зашифрований текст Зашифрований текст передається ланцюжком вузлів мережі до другого цільового вузла квантової мережі (ВКМ6). Для дешифрування на ВКМ6 необхідний квантовий ключ. Він передається від ВКМ2 мережі квантового розподілення ключів, із захистом на квантовому ключі. Передача та формування триває до тих пір, поки не буде переданий квантовий ключ зашифрований на ключі сегмента.

Тепер цільовий вузол мережі ВКМ6 може у зворотному порядку дешифрувати отримані зашифрованні тексти, в результаті отримати ключову інформацію.

Перевагами даного підходу є: відсутність перешифрування загальних секретів на проміжних вузлах квантової мережі, вирішує проблему появи загальних секретів на проміжних вузлах квантової мережі у відкритому виді; інформаційна стійкість захисту під час передачі квантових ключів; можливість скорочення зашифрованих текстів, при формуванні обчислювально стійких квантових ключів для магістральної підмережі квантового розподілу ключів з метою підвищення швидкості рознесення квантових ключів.

Недоліком даного підходу є пропорційне збільшення об’єму зашифрованих послідовностей, що передаються від сегментів в мережі квантового розподілу ключів.

Таким чином, визначено підхід до розподілу загального секрету та розглянуті спроби усунення недоліків даного підходу.

Вдосконалення розлянутого підходу до розподілу загального секрету на сьогодні є невирішеною задачею.

ДОСЛІДЖЕННЯ СТРУКТУРИ МЕРЕЖІ КВАНТОВОГО РОЗПОДІЛЕННЯ ЗАГАЛЬНОГО СЕКРЕТУ

На теперішній час ведуться роботи в галузі стандартизації мереж квантового розподілу ключів щодо способів їх функціонування та архітектури мереж. Група стандартизації ETSI в області квантового розподілу секретних ключів з 2010 року почала розробляти стандарти технології квантового розподілу ключів, базуючись на результатах

проекту SECOQC. Стандарти відносяться до різних областей застосування квантового розподілу ключів: реалізацій квантового розподілу ключів, секретності протоколів, методів вимірю-вань, інтерфейсів взаємодії.

Перший варіант мережі квантового розподілу ключів представлений в описі інтерфейсу взаємодії системи захисту інформації та квантової апаратури. Мережа квантового розподілу ключів побудована на основі довірених вузлів, наведених на рис. 3. У наведеному сценарії взаємодії відпо-відно до ETSI GS QKD беруть участь: апаратура квантового розподілення ключів – QKD; сервер керування ключами – KMS; сервер управління квантовими ключами мережі – KML; додатки користувача, клієнти мережі – App.

Структура мережі квантового розподілу побудована із незалежних частин. Довірений вузол квантової мережі містить кілька екземплярів квантових пристроїв, сервера керування ключами та сервери керування квантовими ключами. В довірений вузол мережі включається додаток користувача, для якого генеруються секретні ключі, проводиться аналіз об'єктів довіреного вузла мережі та його функції.

Базовим елементом мережі квантового розподілення ключів є квантова апаратура.

Пари комплектів квантової апаратури, пов'язані з автентифікованим класичним каналом та квантовим каналом, є самодостатнім елементом. Генерація квантових ключів відбувається незалежно від інших процесів у мережі квантового розподілення ключів. Квантова апаратура генерує випадкову послідовність нефіксованої довжини, а не квантовий ключ. Для формування із випадкових послідовностей квантових ключів використовуються KML (сервери керування квантовими ключами). В кожному вузлі квантової мережі використовується по серверу керування квантовими ключами. Сервер керування квантовими ключами містить сформовані квантові ключі з необхідною метаінформацією. Ідентичність квантових ключів, що генеруються в сусідніх вузлах квантової мережі, ґрунтується на довірі до протоколу квантового розподілу ключів, який гарантує ідентичність сгенерованих послідовностей.

Для передачі квантових ключів у системи захисту інформації користувача, закріплених за вузлами квантової мережі, які не з'єднані напряму з квантовим каналом, використовується KMS (сервер керування ключами). Канали зв'язку (рис. 3) формування квантового ключа відокремлені від каналу апаратури квантової генерації

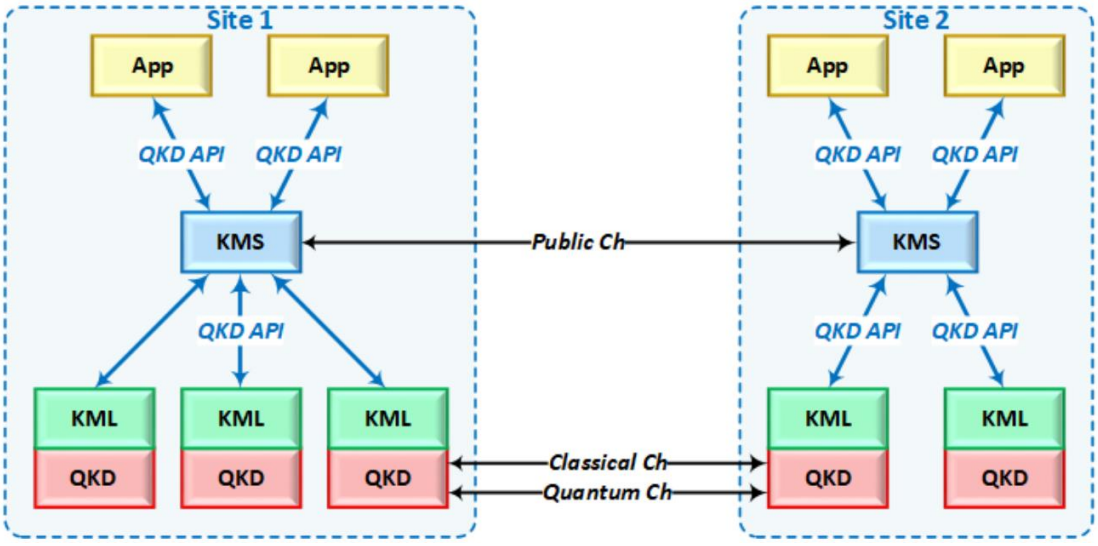

Рис. 3. Структура мережі квантового розподілу за версією ETSI GS QKD

ключів, забезпечення цілісності квантового ключа під час передачі не розглядається. Мережа квантового розподілення ключів допускає підключення декілька систем захисту інформації до одного вузла квантової мережі.

Перший варіант мережі квантового розподілення ключів за версією ETSI є чотирирівневою структурою. Два рівні квантової мережі оперують квантовими ключами, третій рівень - передача квантових ключів, згенерованих в сегменті мережі квантового розподілення ключів на інші сегменти квантової мережі. Четвертий рівень квантової мережі – рівень додатків користувача.

На сьогодні реалізований стандарт ETSI GS QKD V1.1, в якому внесено суттєві зміни до структури мережі квантового розподілення ключів. Схематично мережі квантового розподілення ключів представлено на рис. 4.

У сценарії роботи мережі квантового розподілення ключів беруть участь: апаратура квантового розподілення ключів – QKDE; клієнти мережі-SAE; пристрою керування ключами – KME.

В структурі мережі (рис.4) відбулося суттєве спрощення шляхом об'єднання сервера керування ключами та сервера керування квантовими ключами в єдиний об'єкт, систему захисту винесено за межі вузла квантової мережі, але для забезпечення безпечної передачі секретних ключів, повинна розташовуватися в межах контрольованої зони системи захисту. Довірений вузлом містить у собі клієнта мережі SAE та пристрій керування ключами KME. Квантова апаратура генерує квантові ключі нефіксованої довжини.

Згенерована квантова гамма передається на рівень керування секретними ключами, де з квантової гами формуються квантові ключі заданої, для мережі квантового розподілу ключів, довжини. До сгенерованих квантових ключів додаються метадані, дозволяють у мережі контролювати життєвий цикл квантових ключів (ідентифікатори вузлів, час створення ключа, довжину, час переміщення від квантової апаратури до рівня керування ключами).

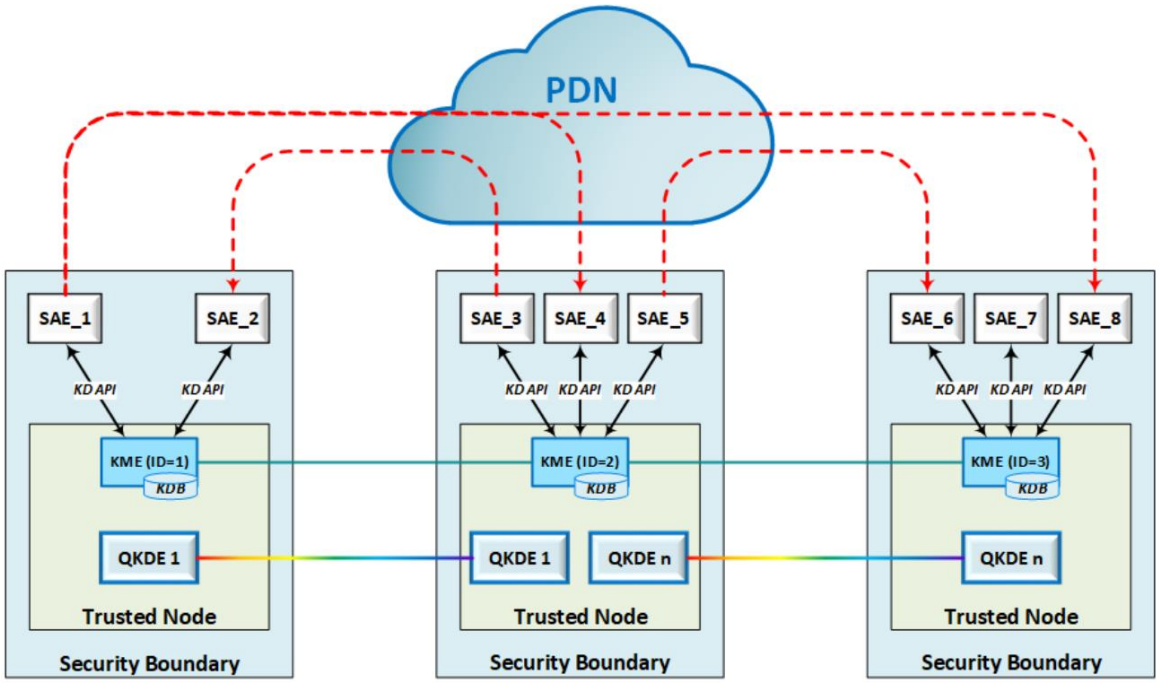

Рис. 4. Структура мережі квантового розподілення ключів ETSI-014

Мережі квантового розподілення ключів, мають багаторівневу структуру із централізованим управлінням, що описуються в європейських рекомендаціях. Взаємодія із системою захисту інформації, зовнішніми по відношенню до мережі квантового розподілу ключів, та розподілу загального секрету для пари вузлів квантової мережі відносяться до одного рівня мережі квантового розподілу ключів. Централізоване управління мережею квантового розподілу ключів, призведе до точки відмови у зв'язку з підвищеним навантаження на єдиний центр управління.

З 2019 року ведуться активні роботи зі створення рекомендацій щодо управління квантовими ключами в мережах КРК, включаючи наступні питання: зберігання згенерованих у мережі КРК ключів; розподіл ключів між вузлами у мережі КРК; передача ключів від апаратури КРК користувачам.

В даний час випущено документ [15], що містить короткий опис основних положень, що містяться в розроблених рекомендаціях, а також ряд документів, що конкретизує приватні аспекти, такі як управління ключами в мережі КРК, а саме процеси розподілу загальних секретів через ВКМ, функціональні вимоги до мереж КРК та їх елементів. Причому питання безпеки взаємодії ВКМ найчастіше винесені за рамки документів. На рис. 5 представлена загальна структура мережі КРК, що пропонується в рекомендаціях ITU-T.

Вузли мережі КРК (довірені вузли) складаються із двох логічних рівнів (Рис. 5):

1. Рівень квантових сигналів (Quantum layer) відповідає: за вироблення квантових ключів каналом квантового зв'язку між сусідніми вузлами; за передачу виробленого квантового ключа рівню управління ключами.

2. Рівень управління ключами (Key management layer) відповідає: за розподіл спільних секретів у мережі між несусідними вузлами; за видачу спільних секретів користувачу.

Розподіл спільних секретів між несусідними вузлами є складним процесом, що включає: керування розміром загального секрету; зміна формату розподіленого секрету та метаданих (ідентифікатор загального секрету, дата формування, довжина тощо) для управління секретами; зберігання спільних секретів; отримання характеристик квантового каналу QBER, швидкість генерації квантових ключів, статус квантового каналу зв'язку; безпечну (тобто стійку в теоретико-інформаційному сенсі) передачу спільних секретів між вузлами на рівні управління ключами; синхронізацію отриманих загальних секретів на вузлах; формування ключового контейнера та видачу загальних секретів користувачеві

Істотна зміна щодо попередніх пропозицій структури мережі КРК в описі архітектури ITU-T полягає у виділенні спеціалізованого рівня управління мережею КРК (QKD network management layer), що реалізується центром управління мережею, та рівня контролю за мережею КРК (QKD control layer).

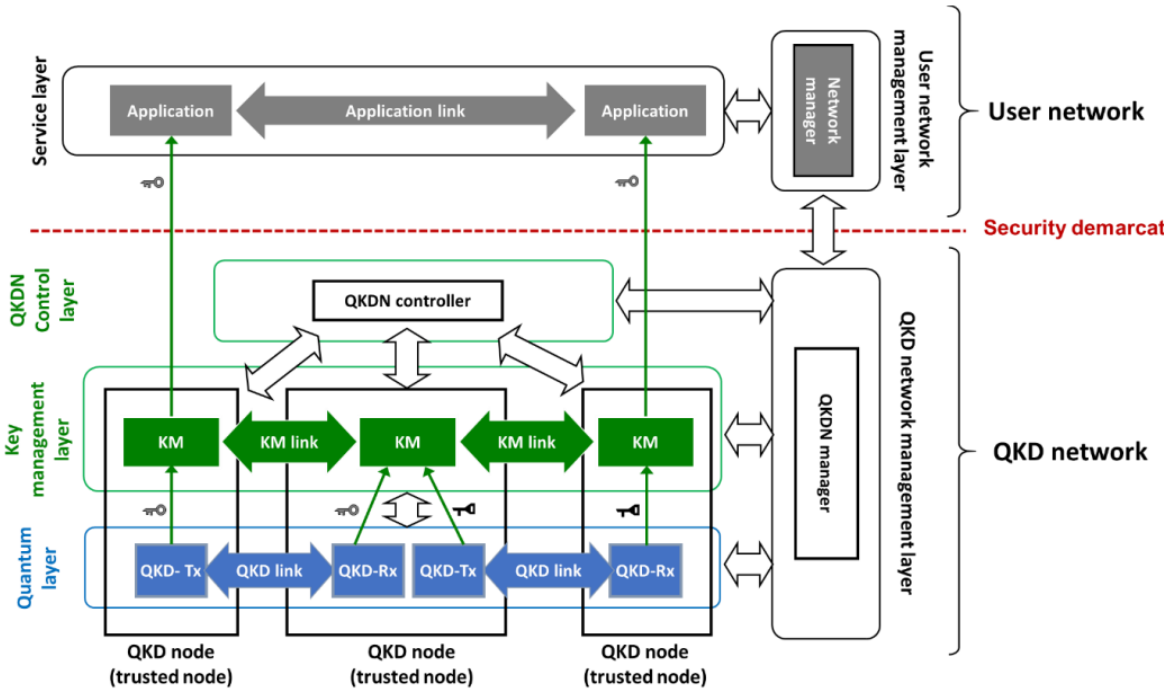

Рис. 5. Загальна структура мережі КРК ITU-T

Централізоване управління мережею КРК використано на вирішення проблеми розрахунку шляху передачі квантового ключа при розподілі загального секрету для двох ВКМ.

Роботи авторів стандартів ITU-T, що стосуються управління мережами КРК через концепцію SDN мереж, дозволяють припустити, що виділення рівня управління, пов'язаного з іншими рівнями мережі КРК, зроблено для подальшого спрощення інтеграції мереж КРК в існуючі мережі зв'язку загального користування з єдиним управлінням, тобто. об'єднання класичних та квантових SDN мереж. Як дані, що передаються на рівні даних SDN мережі, передбачаються однофотонні імпульси в квантовому каналі разом зі службовим трафіком протоколу КРК, а також ключова інформація при формуванні загального секрету. Звернемо увагу, що зовнішні СЗІ об'єднані у свою мережу, у якої також виділено централізовану сутність, що відповідає за управління мережею СЗІ.

Зауважимо, що існуючі документи, що описують структуру та сценарії роботи мереж КРК, не поділяють квантові ключі, згенеровані безпосередньо апаратурою КРК, та загальні секрети, що передаються в СЗІ, підключені до мережі. Це не зовсім коректний підхід, оскільки квантові ключі можливі лише між ВКМ, з'єднаними безпосередньо квантовим каналом.

Частково такий підхід обґрунтований основним пропонованим способом розподілу загального секрету для пари СЗІ, що полягає у передачі квантового ключа деякого сегмента мережі до цільових ВКМ.

Архітектура мережі, пропонована ITU-T, розглядає питання, які раніше не висвітлені у відкритих наукових публікаціях.

Запропоновано рішення для синхронізації спільних секретів на несусідніх ВКМ, а також набір метаданих, якими необхідно супроводжувати квантові ключі.

Квантова апаратура виробляє ключі нефіксованої довжини. Вироблена квантова гамма передається до рівня управління ключами, де з переданої гами формуються квантові ключі заданої, єдиної для всієї мережі КРК довжини. До сформованих квантових ключів додаються метадані, що дозволяють контролювати життєвий цикл ключів у мережі, включаючи час створення ключа, довжину, ідентифікатори вузлів, на

яких згенеровано ключ, час переміщення ключів між сутностями (від квантової апаратури до рівня управління ключами, між пристроями управління ключами тощо).

Контроль за станом квантової апаратури, у тому числі за подіями в квантовому каналі та величиною помилки QBER, проводиться в єдиному центрі управління. Збір даних контролю проводиться рівнем управління ключами з наступною передачею в центр управління. Зазначимо, що пропонований у документах ITU-T підхід вимагає передачі даних, що дозволяють порушнику оцінити ефективність своїх впливів на мережу КРК між вузлами мережі. Потрібний докладний аналіз такого трафіку визначення необхідних заходів захисту, тобто. чи достатньо забезпечувати лише цілісність даних чи необхідне забезпечення конфіденційності.

Перенесення функцій контролю над станом квантової апаратури з самої апаратури у віддалений центр управління з одного боку дозволяє оптимізувати процеси формування квантових ключів, оскільки параметри вироблення квантових ключів прямо чи опосередковано (залежно від способу формування та передачі квантового ключа) впливають на його генерацію. З іншого боку, аналіз стану квантової апаратури щодо наявності тих чи інших атак порушника у віддаленому центрі збільшує час реакції всієї системи на дії порушника, що може негативно позначатися на стійкості системи загалом.

Єдиний центр контролю має функцію контролю життєвого циклу ключів, що генеруються у мережі КРК. Для цього в центр контролю передаються метадані, що прикріплюються до ключів при передачі з квантової апаратури, у разі зміни цих метаданих.

Процес розподілу загальних секретів для довільної пари ВКМ згідно [6,15] полягає в наступному:

1. Сервіс управління мережею СЗІ формує перелік пар СЗІ, для яких потрібні спільні секрети від мережі КРК. Цей перелік передається до центру керування мережею КРК. Причому в документах ITU-T ці спільні секрети називаються квантовими ключами поруч із істинно квантовими ключами, формованими в одному сегменті мережі КРК.

2. Центр управління мережею КРК визначає ланцюжки ВКМ, за якими можна передати квантові ключі на ВКМ, пов'язані з парами СЗІ, для яких мережа СЗІ запросила ключі. На визначення ланцюжків ВКМ впливає кількість готових квантових ключів на сегментах мережі, швидкість генерації нових квантових ключів (за результатами аналізу стану квантової апаратури), а також топологія мережі в цілому.

3. Набір певних ланцюжків передається до контролера мережі КРК, який формує інструкції для кожного ВКМ, що включають маршрут передачі ключів та вказівку, які саме ключі використовувати для передачі, а які для забезпечення конфіденційності передачі даних. Вводяться три види маршрутизації, що визначають шляхи передачі квантових ключів на цільові ВКМ:

1.Ручна маршрутизація - статично задані ланцюжки для пар ВКМ, до яких здійснюється підключення СЗІ.

Цей спосіб доцільно застосовувати лише до невеликих мереж КРК або до мереж з невеликою кількістю розгалужень, де такі ланцюжки легко розраховуються і не мають альтернативних варіантів.

2. Маршрутизація за фіксованою швидкістю.

Цей вид маршрутизації орієнтований на оптимальне навантаження мережі виходячи з продуктивності квантової апаратури. Центр управління мережею аналізує поточну швидкість роботи кожної пари квантової апаратури, а також визначає цільові пари ВКМ, на які необхідно доставити ключі для передачі СЗІ. Ланцюжки вузлів підбираються так, щоб швидкість формування квантових ключів по всіх ланцюжках у сукупності виявилася мінімальною. Потім розраховані ланцюжки передаються до контролера мережі, де формуються конкретні інструкції для вузлів квантової мережі.

3.Адаптивна маршрутизація. Цей вид маршрутизації описаний як додатковий до попередніх. Кожен ВКМ запам'ятовує розраховані маршрути. При отриманні

мережею КРК запиту загального секрету, що повторює один із раніше отриманих, маршрут не перераховується, а ВКМ видається команда повторити формування загального секрету на основі раніше отриманих інструкцій. Цей вид маршрутизації може бути доцільний при стабільній роботі мережі КРК та регулярних запитах ключів від постійних пар СЗІ.

Жоден із запропонованих способів маршрутизації не враховує стійкість застосовуваних методів захисту під час передачі ключової інформації по ланцюжках ВКМ і, відповідно, підсумкову стійкість розподіленого загального секрету.

Для моніторингу роботи мережі КРК загалом крім зазначених вище функцій центр управління додатково оснащується наступним функціоналом: модуль управління, що відповідає, крім розрахунків маршрутів передачі квантових ключів, за забезпечення якості послуг, що надаються мережею (Quality of Service); модуль аутентифікації, який відповідає за аутентифікацію та ідентифікацію вузлів мережі; модуль політик, який відповідає за управління політиками безпеки мережі КРК, до цього модуля може підключатися оператор моніторингу роботи мережі.

Для побудови мережі КРК необхідно виробити рішення супутніх завдань, що стосуються взаємної ідентифікації пристроїв, що становлять мережу КРК; єдиного налаштування та моніторингу параметрів мережі КРК, що відповідають за безпечне функціонування, а також забезпечення необхідних експлуатаційних властивостей. У розглянутих джерелах зустрічається різний поділ ВКМ.

Документи ITU-T вводять наступну класифікацію:

1. Користувальницькі ВКМ. Дані ВКМ повинні мати можливість підключення СЗІ. Зазвичай користувальницькі ВКМ містять один екземпляр квантової апаратури. З економічної доцільності це Клієнт КРК.

2. Проміжні ВКМ. Дані ВКМ мають становити основу мережі КРК, вирішуючи основне питання: збільшення дальності розподілу загального секрету СЗІ. Проміжні ВКМ містять як мінімум пару екземплярів квантової апаратури, Сервер КРК та Клієнт КРК, кожен з яких з'єднаний з квантовою апаратурою інших ВКМ, проміжних або доступу. Фактично проміжні ВКМ становлять основні магістральні гілки мережі КРК.

3. ВКМ доступу. Такі ВКМ необхідні для з’єднання проміжних ВКМ з кінцевими, тобто, користувальницькими ВКМ. Містить Сервер КРК для зв'язку з користувальницьким ВКМ та один або більше відповідних екземплярів квантової апаратури для зв'язку з проміжними ВКМ.

Окремо зазначається, що користувачем загальних секретів (маються на увазі загальні секрети, що розподіляються по мережі) можуть виступати як незалежні зовнішні пристрої, так і вбудовані безпосередньо в ВКМ.

Отже, мережі КРК, що описуються в європейських рекомендаціях, мають багаторівневу структуру із централізованим управлінням. При цьому взаємодія із СЗІ, зовнішніми по відношенню до мережі КРК, та розподіл загального секрету для пари ВКМ відносяться до одного рівня мережі КРК. Всі ключі, що з'являються в мережі КРК, називаються квантовими ключами, що вводить додаткову плутанину і невідмінність квантових ключів, створюваних внаслідок протоколу КРК, від загальних секретів, отриманих у результаті подальшого функціонування мережі КРК. Централізоване управління мережею КРК веде до виникнення точки відмови у зв'язку з підвищенням навантаження на єдиний центр управління.

Отже, є проблема дослідження можливості побудови децентралізованої мережі квантового розподілу ключів, а також необхідність вирішення проблеми розподілу квантових ключів (загального секрету) на довільні пари вузлів квантової мережі із забезпеченням не тільки цілісності ключової інформації, а також конфіденційності, уточнення поняття довіри до проміжних вузлів квантової мережі.

ВИСНОВКИ

У результаті проведеного дослідження виявлено наступні проблеми, пов'язані з недоліками технології квантового розподілу ключів:

1. Системи квантового розподілу ключів мають граничну довжину квантового каналу, визначається протоколом квантового розподілу ключів. Пристрої користувача, для яких генеруються квантові ключі, можуть довільно розташовуватися, на відстанях, що перевищують допустиму довжину квантового каналу. Необхідно розглянути задачу розподілу квантових ключів для довільних пар пристроїв квантової мережі, що розташовані поза граничної довжини квантового каналу.

2. Системи квантового розподілу ключів повинні мати автентифікований класичний канал, при цьому необхідно забезпечити цілісність інформації у квантовому каналі.

3. Забезпечити синхронізації квантових ключів, що передаються в вузли квантової мережі, пристрої користувача. Відомі підходи, не враховують квантової специфіки апаратури.

4. Необхідно розглянути задачу забезпечення конфіденційності ключової інформації та її цілісності на довірених проміжних вузлах квантової мережі.

5. Структура мережі квантового розподілу ключів та спосіб її функціонування містять не вирішені задачі, що перешкоджають ефективному розповсюдженню та створенню квантових ключів на довільні пари вузлів квантової мережі.

З урахуванням розглянутих задач у рамках проведеного дослідження для підвищення захищеності мереж квантового розподілу ключів необхідно вирішити наступні задачі: розробити підхід до побудови автентифікованого класичного каналу квантової апаратури; розробити спосіб взаємодії користувальницьких систем захисту інформації з квантовою апаратури, що уточнює процеси забезпечення цілісності загальних секретів та синхронізації при їх передачі до систем захисту; розробити метод розподілу квантових ключів для декількох вузлів квантової мережі магістральної топології.

ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.
2. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836.
3. Квантова криптографія. Пояснення [Електронний ресурс] // Quantum Xchange. – 2019. – Режим доступу: https://quantumxc.com/blog/quantum-cryptography-explained/ (дата звернення 02.03.2024).
4. **Satish Kumar**. Quantum Cryptography [Електронний ресурс] // Tutorialspoint. – 2023. – Режим доступу: http://surl.li/fjebs (дата звернення 05.03.2024).
5. **Грамблінг Е**. Квантові обчислення. Прогрес і перспективи / Е. Грамблінг, М. Горовіц. – Вашингтон: Національні академії наук, техніки та медицини, 2019. – 272 с.
6. **Керті М., Ло Х.-К., Тамакі К**. Безпечний квантовий розподіл ключів. Фотоніка природи. 2018. Т. 8. С. 595–604.
7. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403, зі змінами від 28.07.2022 року. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163
8. **Бем, М.В**. Стандарти захисту персональних даних в соціальній сфері. / М. В.Бем, І. М. Городиський -Львів:, 2018р. - 110 с.
9. **Богуш, В.М**. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2015. – 432 с.
10. **Голубєв О.В**. Програмно-технічні засоби захисту даних від комп'ютерних злочинів / О. В. Голубєв– Запоріжжя: «Павел», 2018. – 145 с.
11. **Горбулін В.П.** Проблеми захисту інформаційного простору України / М.М. Баченок, П.В. Горбулін – К.: Інтертехнологія, 2019. – 138 с.
12. **Біленчук П.Д.** Правові засади інформаційної безпеки України: монографія /Л.В. Борисова, І.М. Неклонський.– Харків: 2018. – 289 с.

13. **Буров Є.В.** Комп'ютерні мережі. Том 1. / Є.В.Буров, М.М.Митник //Навчальний посібник – Львів, «Магнолія 2006», 2019р.- 256 с.
14. **Буров Є.В.** Комп'ютерні мережі. Том 2. / Є.В.Буров, М.М.Митник//Навчальний посібник – Львів, «Магнолія 2006», 2019р. - 334 с.
15. **Shor P.W.** Algorithms for quantum computation: discrete logarithms and factoring. 35th annual symposium on foundations of computer science, Santa Fe, NM, USA. URL: https://doi.org/10.1109/sfcs.1994.365700 (date of access: 16.11.2023).
16. **Вербіцький О.В.** Вступ до криптології / О.В. Вербіцький. – Львів : ВНТЛ, 2017р. – 248 с.
17. **Остапов С.Е.** Квантова інформатика та квантові обчислення / С.Е.Остапов, Ю.Г.Доб-ровольський - Чернівці: ЧНУ, 2021. – 69-73 с
18. **Ленков С.В.** Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.
19. **Вишня В.Б.** Основи інформаційної безпеки: навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.
20. **Остапов С.Е.** Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків: Вид-во ХНЕУ, 2016. – 476 с.
21. **Бурячок В.Л.** Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К.: ДУТ-КНУ, 2016. – 178 с.
22. **Лавров Є.А.** Математичні методи дослідження операцій: підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми: Сумський державний університет, 2017. – 212 с.

REFERENCES

1. Doktryna informatsiinoi bezpeky Ukrainy, zatverdzhenoi Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku № №47/2017, 15s.
2. Derzhavnyi standart Ukrainy Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia. DSTU 3396.0-96 [Elektronnyi resurs]. – Rezhym dostupu: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836
3. Kvantova kryptohrafiia. Poiasnennia [Elektronnyi resurs] // Quantum Xchange. – 2019. – Rezhym dostupu: https://quantumxc.com/blog/quantum-cryptography-explained/ (data zvernennia 02.03.2024).
4. **Satish Kumar**. (2023) Quantum Cryptography [Elektronnyi resurs] // Tutorialspoint. –Rezhym dostupu: http://surl.li/fjebs (data zvernennia 05.03.2024).
5. **Hramblinh E.** (2019) Kvantovi obchyslennia. Prohres i perspektyvy / E. Hramblinh, M. Horovits. – Vashynhton: Natsionalni akademii nauk, tekhniky ta medytsyny, – 272 s.
6. **Kerti M., Lo Kh.-K., Tamaki K.** (2018) Bezpechnyi kvantovyi rozpodil kliuchiv. Fotonika pryrody. T. 8. S. 595–604.
7. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» zi zminamy. Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403, zi zminamy vid 28.07.2022 roku. Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2163
8. **Bem, M. V.** (2018) Standarty zakhystu personalnykh danykh v sotsialnii sferi. / M. V.Bem, I. M. Horodyskyi -Lviv: - 110 s.
9. Bohush, V.M. (2015) Informatsiina bezpeka derzhavy / V.M. Bohush, O.K. Yudin. – K.: MK-Pres. – 432 s.
10. **Holubiev, O.V.** (2018) Prohramno-tekhnichni zasoby zakhystu danykh vid kompiuternykh zlochyniv / O. V. Holubiev– Zaporizhzhia : «Pavel». – 145 s.
11. **Horbulin, V.P.** (2019) Problemy zakhystu informatsiinoho prostoru Ukrainy / M.M. Bachenok, V.P. Horbulin – K.: Intertekhnolohiia. – 138 s.
12. **Bilenchuk, P.D.** (2018) Pravovi zasady informatsiinoi bezpeky Ukrainy: monohrafiia /L.V. Borysova, I.M. Neklonskyi.– Kharkiv: – 289 s.
13. **Burov, Ye.V.** (2019) Kompiuterni merezhi. Tom 1. / Ye.V. Burov, M.M. Mytnyk // Navchalnyi posibnyk – Lviv, «Mahnoliia 2006» - 256 s.
14. **Burov, Ye.V.** (2019) Kompiuterni merezhi. Tom 2. / Ye.V. Burov, M.M. Mytnyk // Navchalnyi posibnyk – Lviv, «Mahnoliia 2006» - 334 s.
15. **Shor P.W.** (2023). Algorithms for quantum computation: discrete logarithms and factoring. 35th annual symposium on foundations of computer science, Santa Fe, NM, USA. URL: https://doi.org/10.1109/sfcs.1994.365700 (date of access: 16.11.2023).
16. **Verbitskyi O.V.** (2017). Vstup do kryptolohii / O.V. Verbitskyi. – Lviv : VNTL. – 248 s.

17. **Ostapov S.E.** (2021). Kvantova informatyka ta kvantovi obchyslennia. / S.E. Ostapov, Yu.H Dobrovolskyi - Chernivtsi: ChNU. – 69-73 s
18. **Lenkov S.V.** (2023). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv / S.V. Lienkov, V.M. Dzhulii, A.M. Bernaz, I.V. Muliar, I.V. Pampukha // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU -. №78. – C. 123-134.
19. **Vyshnia, V. B.** (2020) Osnovy informatsiinoi bezpeky : navch. posibnyk / V. B. Vyshnia, O. S. Havrysh, E. V. Ryzhkov. Dnipro : Dniprop. derzh. un-t vnutrish. sprav. – 128 s.
20. **Ostapov S. E.** (2016). Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv: Vyd-vo KhNEU. – 476 s.
21. **Buriachok V.L., Toliupa S.V., Semko V.V.** (2016). Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby: posibnyk. Kyiv, DUT-KNU, 178.
22. **Dzhulii V.M.**, **Miroshnichenko O.V., Solodieieva L.V.** (2022). Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, Vol.74, 73-82.
23. **Lavrov Ye.A., Perkhun L.P., Shendryk V.V.** (2017). Matematychni metody doslidzhennia operatsii: pidruchnyk. Sumy, Sumskyi derzhavnyi universytet, 212.

Research into the current state of quantum secret key distribution technologies

Serhiy Lenkov[1], Volodymyr Dzhuly[2], Ihor Mulyar[3], Yevhen Lenkov[4]

Abstract. The work is devoted to the study of the problems of using the technology of quantum distribution of secret keys, namely the problems of using and forming new secret keys, based on the generation of quantum keys and the distribution of new keys in networks of complex topologies.

In secure communication systems, information is transmitted over public networks, and thus is available to a potential attacker for carrying out various types of attacks. A potential attacker is able to store encrypted data transmitted over network channels, and attempt to decrypt it later, when technical means and attacks on information protection algorithms will allow, in an acceptable time, to carry out decryption. This is the basic principle of "Store now, decrypt later", which is one of the problems of information protection systems.

For block ciphers, there is a parameter - the key load, which limits the amount of information that one key can process using the data protection algorithm. NIST recommends a time frame for using secret keys, calculated in years. In the field of information security, there are more significant restrictions on the key load, related to the number of blocks that can be processed by one key, caused by attacks on block ciphers. With these restrictions, there is a need to regularly change the secret key used, and search for options for generating and delivering keys between two network nodes that organize a secure information transmission channel. Changing the secret key to a new key, independent of the previous one, allows you to protect the transfer of confidential information when the key used is compromised.

The technology of creating a quantum computer allows you to effectively attack known algorithms for generating secret keys based on the factorization of large numbers or the complexity of calculating a discrete logarithm. The quantum Shor algorithm [5, 6] allows you to solve these problems in polynomial time, so it is necessary to look for alternative solutions to the problem of regular changes in the network channel of the secret key in a pair of nodes.

It is important to take into account the need to ensure the quality of Perfect forward secrecy, when the master key is compromised, all subsequent secret keys must not be compromised. To achieve this property of modern encryption algorithms, there is a periodic update of master keys.

To prevent the accumulation of information, to successfully carry out attacks by the attacker and to comply with the load requirement on the secret key, it is necessary to solve the problem of regular changes of the secret, and regular generation/delivery of keys to network nodes.

Given the urgent needs that are intensively developing today in the secure and high-speed transmission of information, and no less, the rapid growth of technical capabilities, there is a need to develop options in advance that will ensure the security of information during transmission. Regular change, in geographically dispersed data protection systems, of common secret keys, in the case of ensuring the independence of secret keys, allows successfully solving the task.

Keywords: information security, vulnerabilities, attacks, quantum secret key, quantum distribution protocol.