УДК 004.056.53

***Сарапук О.І., Рибінський В.О., Сапіташ В.І.***

*Західноукраїнський національний університет*

# АРХІТЕКТУРА СИСТЕМИ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ

**Вступ**. Традиційні криптографічні методи, засновані на складності математичних задач, поступово втрачають надійність у зв'язку з появою потужних обчислювальних засобів і перспективних квантових обчислювачів, здатних ефективно зламувати класичні шифри. У цьому контексті особливої актуальності набувають квантові методи захисту інформації [1], зокрема квантовий розподіл ключів (КРК) (Quantum Key Distribution, QKD), який забезпечує безумовну стійкість криптографічного обміну завдяки використанню фундаментальних принципів квантової механіки [2].

Розробка ефективної архітектури системи квантового розподілу ключів є актуальним науково-технічним завданням і важливим кроком до впровадження квантової безпеки в практичні телекомунікаційні мережі, який визначає перспективи формування безпечних інформаційних середовищ у майбутніх квантових комунікаційних мережах.

**Мета:** розробити архітектуру системи квантового розподілу ключів.

## 1. Розробка архітектури системи квантового розподілу ключів

Квантова апаратура, що реалізує протокол КРК, являє собою комплекс із двох пристроїв, з'єднаних квантовим каналом. Спрощена архітектура комплексу наведена на рисунку 1.

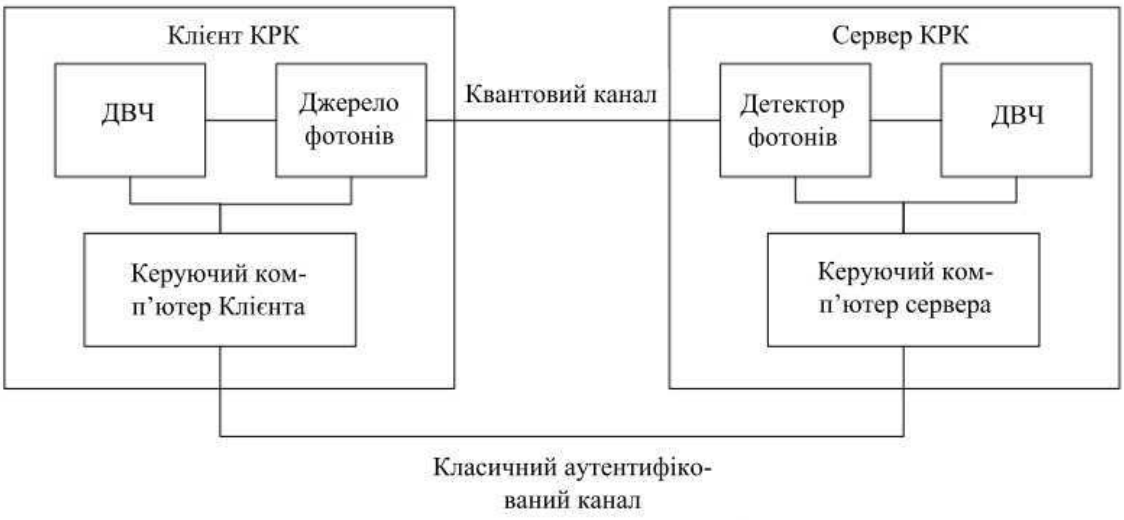


Рисунок 1 – Схема комплексу квантової апаратури

Один з пристроїв комплексу, що містить генератор (джерело) поодиноких фотонів, прийнято називати Клієнтом КРК. Суміжний пристрій, що містить детектор (приймач) поодиноких фотонів, називають Сервером КРК. Кожен з пристроїв має датчик випадкових чисел (ДВЧ). При цьому рекомендується використовувати датчики, в основі випадкових процесів яких лежать квантові ефекти, що дозволяє отримати істинно випадкову послідовність, з якої надалі формується квантовий ключ.

Сервер КРК і Клієнт КРК з'єднані двома логічними каналами: квантовим і класичним. Квантовий канал призначений для передачі квантових інформаційних станів, тобто фотонів і, як правило, реалізується за допомогою звичайного оптоволокна. Існують системи КРК, у яких як квантовий канал застосовується повітряне середовище, але вони поки що перебувають на стадії лабораторних установок.

Важливою особливістю технології КРК є повна доступність квантового каналу для зловмисника, тобто цей канал не контролюється і не захищається від втручання. Крім квантового каналу, Сервер і Клієнт КРК повинні бути з'єднані класичною лінією зв'язку, де реалізується класичний автентифікований канал. До цього каналу висуваються вимоги щодо забезпечення цілісності переданих даних та автентифікації відправника.

Реальна система КРК додатково має ще логічний службовий канал для передачі даних, який передає команди управління й моніторингу апаратури, не пов'язані безпосередньо з протоколом КРК. У деяких реалізаціях може знадобитися забезпечення не лише цілісності, а й конфіденційності цих даних. Для роботи системи КРК в апаратуру необхідно завантажити попередньо розподілені ключі, які потрібні щонайменше для побудови класичного автентифікованого каналу до першого успішного отримання достатньої кількості квантових ключів. Одну ітерацію реалізації протоколу КРК називають сеансом КРК.

Зазвичай кожен сеанс КРК складається з таких етапів:

– підготовка квантового каналу;
– передача поодиноких фотонів квантовим каналом;
– постобробка переданої послідовності.

У результаті передачі квантовим каналом обидва пристрої отримують так званий сирий ключ. Далі постобробка відбувається через класичний автентифікований канал і включає три підетапи:

– узгодження базисів вимірювання на стороні приймача з базисами кодування на стороні джерела. Неспівпадіння відкидаються, а сирий ключ перетворюється на просіяний ключ;

– виправлення помилок у просіяних ключах для отримання ідентичних послідовностей у Сервері та Клієнті КРК. Результат – очищений ключ;

– посилення секретності – стиснення очищеного ключа для зменшення інформації, доступної зловмиснику. Результат – секретний квантовий ключ.

На рисунку 2 представлена узагальнена послідовність виконання протоколу КРК.

Потрібно відзначити, що результат роботи квантового протоколу не зовсім коректно називати квантовим ключем. Правильніше говорити, що результатом сеансу КРК є випадкова квантова ґамма, ідентична у двох абонентів, оскільки цей результат має змінну довжину, яка не завжди збігається з довжиною ключів, що застосовуються в алгоритмах кодування. Більше того, результат виконання одного й того ж протоколу КРК суттєво відрізняється для квантових каналів із низькими та високими втратами, що безпосередньо впливають на величину помилок під час передачі в квантовому каналі (QBER). Це, своєю чергою, впливає на обсяг

інформації про квантову ґамму, доступної порушнику, і яка зменшується на етапі посилення секретності.

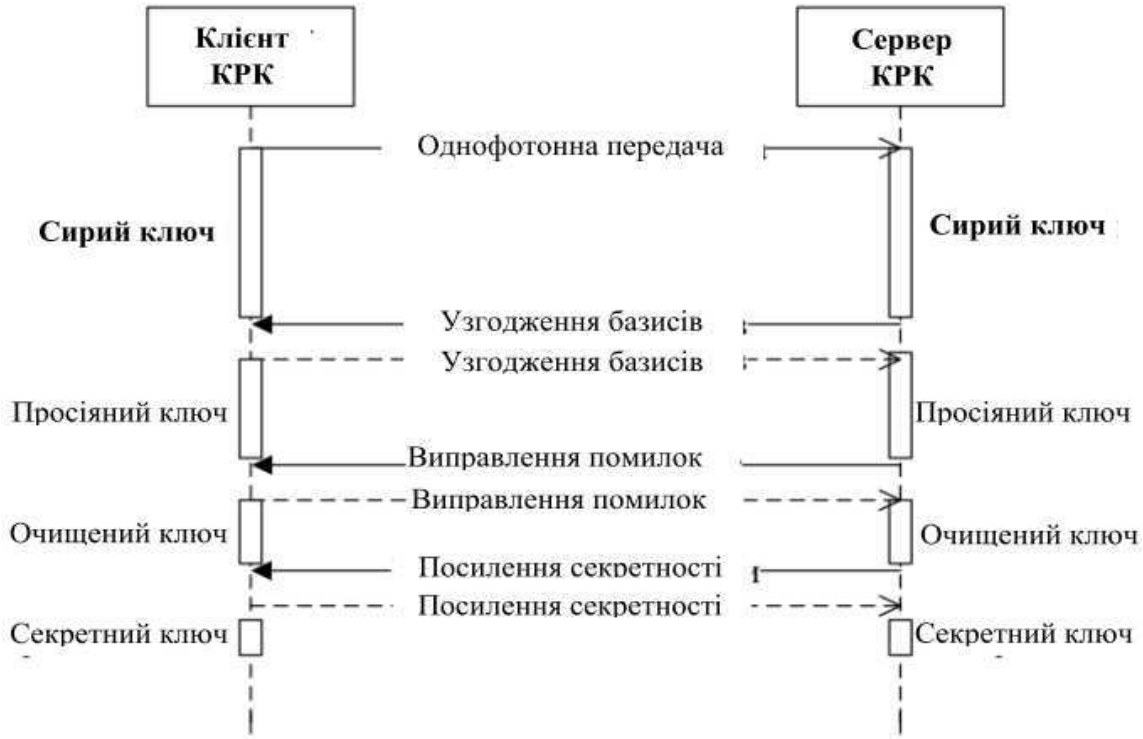


Рисунок 2 – Послідовність виконання протоколу КРК

Згідно з експериментальними даними, наведеними у [1], при довжині лінії у 50 км (що відповідає втратам 10 дБ при типовому затуханні у ВОЛЗ 0,2 дБ/км [2]) ефективність вироблення квантових ключів, тобто відношення числа зареєстрованих імпульсів на сервері КРК до загальної кількості імпульсів, відправлених клієнтом КРК, становить $2\times10^{-5}$. Таким чином, щоб отримати 256-бітний квантовий ключ при довжині лінії 50 км за один сеанс КРК, потрібна послідовність у $2\times10^{7}$ імпульсів. Втрати при довжині квантового каналу у 100 км складають 20 дБ, тобто у 10 разів більше, ніж при 50 км. Тому для вироблення 256-бітного квантового ключа за один сеанс КРК послідовність імпульсів, що передається квантовим каналом, має бути в 10 разів більшою, тобто не менше, ніж $2\times10^{8}$ імпульсів.

**Висновок.** Розроблено архітектуру системи квантового розподілу ключів, що дало можливість регулярної генерації спільних квантових ключів у користувацькі пристрої.

**Перелік використаних джерел.**

1. Quantum Safe Cryptography and Security [Електронний ресурс]. ETSI. Режим доступу: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

2. Quantum Key Distribution Products [Електронний ресурс]. TOSHIBA CORPORATION. Режим доступу: https://www.toshiba.co.jp/qkd/en/products.htm.