УДК 003.26:004.056.55

Д.М. Грабінський, аспірант**, А.В. Вороніна,** студентка**,**
В.М. Кінзерявий, к.т.н.**, С.О. Гнатюк,** к.т.н.**,**
академічний радник Інженерної академії України

АНАЛІЗ МЕТОДІВ ТА ПРОТОКОЛІВ РОЗПОДІЛУ КРИПТОГРАФІЧНИХ КЛЮЧІВ

Національний авіаційний університет, E-mail: dimongrabinskyi@gmail.com

Проблема розподілу криптографічних ключів є дуже гострою та найбільш досліджуваною у сучасній криптографії. Вона полягає у необхідності доставки секретного ключа легітимним користувачам перед процедурою шифрування інформації в умовах суворої секретності. Зважаючи на швидкий ріст обчислювальних можливостей сучасної техніки та використання квантових технологій, деякі широко використовувані методи та протоколи розподілу криптографічних ключів уже не можуть забезпечити надійного обміну. З огляду на це, у статті здійснено пошук методів та протоколів розподілу криптографічних ключів, що дало можливість визначити їх переваги та недоліки, а також оцінити можливість використання у сучасних криптографічних системах різного призначення.

Ключові слова: *криптографія, розподіл криптографічних ключів, криптографічні методи та протоколи, квантовий розподіл ключів, центр розподілу ключів, метод довірених кур'єрів, симетричний і асиметричний криптографічний метод.*

Вступ. Найбільш ефективним напрямом захисту персональних конфіденційних даних користувачів завжди був криптографічний захист, який в головній мірі залежить від вибору алгоритму шифрування та методу управління криптографічними ключами (КК). При чому, розкриття КК зловмисником надає йому повний доступ до всієї інформації в незалежності від криптостійкості застосованого алгоритму. Під управлінням КК розуміється інформаційний процес, який включає в себе три елемента: генерацію, накопичення та розподіл ключів. Для зловмисників найбільш привабливим з цього переліку є розподіл ключів, адже у більшості випадків він відбувається через незахищені канали зв'язку. З огляду на це, дослідження існуючих методів та протоколів розподілу криптографічних ключів є **актуальною** задачею.

Метою роботи є пошук існуючих методів та протоколів розподілу криптографічних ключів для визначення можливості їх використання у криптографічних системах різного призначення.

Основна частина. Далі будуть розглянуті основні методи розподілу криптографічних ключів та протоколи, які практично їх реалізують.

1. Класичний асиметричний криптографічний метод. Для вирішення проблеми розподілу КК ще у 70-х роках XX століття почали використовувати асиметричні криптосистеми [1]. Головною особливістю таких систем являється використання пари ключів – відкритого та секретного. Відкритий ключ зазвичай розміщується у відкритих каталогах та використовується для шифрування повідомлень. Секретний ключ використовується для розшифрування повідомлень та зберігається у надійному місці. Знаючи відкритий ключ теоретично можливо відновити й секретний, але для цього потрібно виконати велику кількість математичних операцій. Асиметричні криптосистеми зазвичай використовуються для передачі інформації відкритими каналами зв'язку. Однак, у порівнянні із симетричними криптосистемами, асиметричні мають значно нижчу швидкодію, що із зростанням об'єму трафіку який передається, знижую актуальність їх використання вцілому. Тому, широкого розповсюдження набули гібридні криптосистеми, які для шифрування самого повідомлення використовують швидкодіючі симетричні алгоритми, а відповідні симетричні ключі засекречуються в асиметричній криптосистемі. Найбільш розповсюдженими протоколами розподілу КК, які належать до асиметричного криптографічного методу є:

а) Протокол обміну ключами Діффі-Хелмана. Вперше поняття криптографії з відкритим ключем було введено в 1976 році Уітфілдом Діффі і Мартіном Хеллманом [2]. Вони запропонували використовувати різні ключі для шифрування та дешифрування повідомлень. Розподіл ж таких ключів між легітимними користувачами (Абонентом 1 та Абонентом 2) мав відбуватися за описаним ними протоколом обміну ключами, який сьогодні відомий як протокол Діффі-Хеллмана (ДХ). Початкова версія протоколу ДХ для обміну ключами між двома користувачами має наступний вигляд:

1. Обираються просте велике число p та примітивний елемент g, який належить мультиплікативній функції $GF(p)$. Для протоколу p та g являються відкритими константами і зазвичай знаходяться у загальнодоступному місці.

2. Далі, Абонент 1 вибирає випадкове число x із множини $GF(p)$ та підраховує значення виразу $g^x \bmod p$. Отримане значення відсилається Абоненту 2.

3. У свою чергу, Абонент 2 також вибирає випадкове число y та знаходить значення виразу $g^y \bmod p$, яке і відсилає Абоненту 1.

4. В кінцевому вигляді секретним ключем буде вираз g^{xy}, який Абонент 1 та Абонент 2 з легкістю отримають шляхом піднесення отриманого повідомлення до степеня x та y відповідно. Відновлення секретних ключів x та y по відомим значенням g^x та g^y зводиться до задачі дискретного логарифма, розв'язання якої при правильному виборі p та g на сьогоднішній час неможливе.

Однак, протокол ДХ вразливий до атаки «людина посередині». Так, при обміні даними між Абонентом 1 та Абонентом 2 Зловмисник може видавати себе за легітимного користувача (адже Абонент 1 та Абонент 2 не знають точно з ким вони спілкуються). Таким чином, Зловмисник може перехоплювати, модифікувати та пересилати повідомлення без відома легітимних абонентів. Можливість такої атаки викликала необхідність до модифікації даного протоколу, яка була здійснена шляхом залучення контролюючого органу – центру реєстрації ключів (ЦРК). Відмінність останнього методу від описаного вище протоколу полягає у занесенні відкритих ключів g^x та g^y до електронної бази ЦРК. Відкриті ключі зберігаються разом з реєстраційною інформацією власника ключа, що в свою чергу дає можливість ідентифікації користувача з яким планується взаємодія. Така процедура нівелює можливість проведення атаки «людина посередині», але і в свою чергу сприяє виникненню нових загроз. По-перше, виникає можливість компрометації самого ЦРК – що цілком можливо, яка може бути здійснена шляхом підміни електронної бази ключів. По-друге, немає цілковитої упевненості у добросовісній роботі самого ЦРК, який володіючи великою базою відкритих ключів сам може здійснювати взаємодію з користувачами. Таким чином, використання вище описаного протоколу не дає цілковитої гарантії у надійному розподілі КК.

б) Триразовий протокол рукостискання [1]. Даний протокол використовується для визначення загального секретного ключа (K). Попередньо, Абоненту 1 та Абоненту 2 потрібно обмінятися своїми відкритими ключами. Алгоритм роботи протоколу має наступний вигляд:

1. Абонент 1 відсилає повідомлення $C = E_{A2}(R_{A1}, I_{A1})$, де E_{A2} - процедура шифрування з відкритим ключем Абонента 2, I_{A1} – ідентифікатор Абонента 1 та R_{A1} – випадкове число.

2. Своїм секретним ключем Абонент 2 розшифровує повідомлення та отримує значення I_{A1} та R_{A1}. На наступному кроці Абонент 2 вибирає випадкове число R_{A2} та відсилає $C' = E_{A1}(R_{A1}, R_{A2})$.

3. Після розшифрування C' Абонент 1 може в реальному часі визначити, що Абонент 2 отримав R_{A1}, бо тільки він може розшифрувати C.

4. Абонент 1 відсилає Абоненту 2 повідомлення $C'' = E_{A2}(R_{A2})$, та у реальному часі може визначити чи Абонент 1 отримав R_{A2}, бо тільки він може розшифрувати C'.

5. Описаними вище діями Абонент 1 та Абонент 2 аутентифікували один одного та можуть приступати до передачі секретного ключа (K). Абонент 1 відсилає Абоненту 2 повідомлення $E_{A2}(D_{A1}(K))$,. Розшифрувавши повідомлення, Абонент 2 отримує секретний ключ K який відповідає секретному ключу Абонента 1.

Таким чином, описаний вище протокол забезпечує як секретність, так і автентичність при обміні ключем K. Однак, для такого протоколу залишається актуальним питання розподілу відкритих ключів Абонента 1 та Абонента 2, адже Зловмисник може видавати себе за

легітимного користувача та підмінити відкриті ключі користувачів своїми відкритими ключами. Також, у деяких випадках, значення R_{A1}, R_{A2} мають між собою закономірність, виявивши яку – Зловмисник також може видавати себе за легітимного користувача.

в) протокол MQV (Менезес-Кью-Ванстоун). Протокол MQV представляє собою протокол розподілу ключів з аутентифікацією сторін, який запропонований в 1995 році Альфредом Менезисом, Кью та Скотом Ванстоуном [3]. Даний протокол базується на алгоритмі розподілу ключів Діффі-Хеллмана. Для аутентифікації легітимних користувачів не використовується ніяка додаткова інформація (наподобі ЕЦП), що дозволяє суттєво скоротити розмір інформації яка передається. Алгоритм роботи протоколу має наступний вигляд:

1. Абонент 1 та Абонент 2 мають свою ключову пару відкритих та секретних ключів: $(A1: G^a, a), (A2: G^b, b)$ та попередньо обмінялися своїми відкритими ключами.
2. Кожен із них генерує сеансову пару ключів $(A1: G^c, c)$ та $(A2: G^d, d)$.
3. Відбувається обмін ключами як в класичному протоколі Діффі-Хеллмана: Абонент 1 посилає Абоненту 2 G^c, а Абонент 2 посилає Абоненту 1 G^d. Тепер, Абонент 1 та Абонент 2 знаючи наступні значення: $A1, A2, C, D, a, c$ та $A1, A2, C, D, b, d$ відповідно виконують:

Абонент 1:

1. Вибирає число l, яке дорівнює половині розміру повідомлення (Для ЕС-MQV l=80).
2. Задає $i = C$ та знаходить $S_{A1} = (i(\mathrm{mod} 2^l)) + 2^l$.
3. Задає $j = D$ та знаходить $T_{A1} = (j(\mathrm{mod} 2^l)) + 2^l, h_{A1} = C + S_{A1} \times a$.
4. Підраховує $p_{A1} = \left(DB^{T_{A1}}\right)^{h_{A1}}$.

Абонент 2:

1. Задає значення $i = D$ та знаходить $S_{A2} = (i(\mathrm{mod} 2^l)) + 2^l$.
2. Задає $j = C$ та знаходить $T_{A2} = (j(\mathrm{mod} 2^l)) + 2^l, h_{A2} = D + S_{A2} \times b$
3. Підраховує $p_{A2} = \left(CA^{T_{A2}}\right)^{h_{A2}}$.

Отримані результати $p_{A1} = p_{A2}$ і є загальним секретних ключем для цих користувачів. Така реалізація роботи протоколу , по-перше, забезпечує стійкість до атаки "людина посередині" (на відмінно від протоколу Діффі-Хеллмана), по-друге, позбавляє користувача необхідності підписання кожного відправленого повідомлення (у порівнянні з ЕЦП), по-третє, забезпечує невеликий розмір передаваємого повідомлення. Він є стандартизований такими міжнародними організаціями як ANSI, NIST, ISO, IEEE. Однак, у статті [4] представлені вразливості даного протоколу та запропоновані можливі варіанти їх вирішення. Таким чином, з огляду на існуючі вразливості протоколу, неможливо говорити про гарантовану надійність його використання.

2. Класичний симетричний криптографічний метод. На відмінно від асиметричних криптографічних систем з відкритим та секретним ключами, симетрична криптосистема для шифрування та розшифрування даних використовує один і той же ключ, який повинен зберігатися у надійному місці [1, 3]. До відомих симетричних алгоритмів шифрування належать AES, DES, 3DES, Twofish, ГОСТ 28147-89 та інші. Для усіх цих алгоритмів найбільш актуальним питанням є розподіл ключів, адже перехопивши його, зловмисник зможе шифрувати та розшифровувати повідомлення видаючи себе за легітимного користувача.

а) Протокол Барроуза. Для розподілу ключів за даним протоколом залучається довірена третя сторона ЦРК. Так, користувачі, які прагнуть взаємодіяти між собою попередньо реєструються в ЦРК та отримують секретний ключ, за допомогою якого відбуватиметься взаємодія з ЦРК. Маючи даний секретний ключ, кожен із зареєстрованих користувачів може ініціалізувати взаємодію з іншим користувачем наступним чином:

1. Абонент 1 на своїй стороні генерує сеансовий ключ K_{A1A2}, знімає мітку часу t_{A1} та представляє інформацію про Абонента 2. Всі ці дані шифруються секретним ключем взаємодії з ЦРК та відправляються останньому.

2. На своїй стороні ЦРК отримує повідомлення виду $\{t_{A1}, b, K_{A1A2}\}_{K_{A1}}$, розшифровує його та аналізує отримані дані. Якщо отримана мітка часу близька до поточного моменту часу, ЦРК додає до повідомлення свою мітку часу та шифрує його спільним ключем з Абонентом 2.

3. Абонент 2 отримує повідомлення типу $\{t_{ЦРК}, a, K_{A1A2}\}_{K_{ЦРКA2}}$, розшифровує його, звіряє мітку часу та реквізити Абонента 1. Коректна часова мітка та дані Абонента 1 підтверджують достовірність отриманого ключа. На даному етапі розподіл ключів завершений і у обох користувачів є однаковий секретний ключ K_{A1A2}. Описаний вище протокол на сьогоднішній день майже не використовується, адже має ряд суттєвих недоліків:

1. Відповідальність за генерацію та зберігання стійкого ключа повністю лежить на користувачу, який ініціалізує взаємодію.
2. Коректність роботи протоколу залежить від синхронізації годинників.
3. Можливе зловживання повноваженнями збоку ЦРК.

б) Протокол Нідхема-Шредера. Даний протокол запропонований в 1978 році Майклом Шредером і Роджером Нідхемом [2]. Для взаємодії, так само як і за попереднім протоколом, необхідне залучення ЦРК:

1. Абонент 1 повідомляє ЦРК про намір взаємодії з Абонентом 2. Для цього він генерує унікальну числову вставку N_{A1} та відправляє повідомлення виду $\{A1, A2, N_{A1}\}$.

2. ЦРК генерує ключ K_{A1A2} та разом з числовою вставкою N_{A1} відправляє листа Абоненту 1. У цьому ж повідомленні відправляється сеансовий ключ зашифрований ключем $K_{A2ЦРК}$. Загальний вид повідомлення має вигляд $\{N_{A1}, b, K_{A1A2}, \{K_{A1A2}, a\}_{K_{A2ЦРК}}\}_{K_{A1ЦРК}}$.

3. Абонент 1 розшифровує повідомлення своїм ключем та перевіряє на коректність значення N_{A1}. Упевнившись в достовірності даних, він пересилає сеансовий ключ Абоненту 2.

4. Отримавши повідомлення виду $\{K_{A1A2}, a\}_{K_{A2ЦРК}}$ Абонент 2 розшифровує його своїм секретним ключем та отримує значення сеансового ключа. Для аутентифікації Абонента 1, у четвертому листі відправляється числова вставка Абоненту 2.

5. Абонент 1, отримавши повідомлення виду $\{N_{A2}\}_{K_{A1A2}}$ розшифровує його та останнім листом відсилає Абоненту 2 простий вираз який залежить від N_{A2}: $\{N_{A2} - 1\}_{K_{A1A2}}$. Таким чином відбулася передача сеансового ключа та аутентифікація взаємодіючих сторін.

Головним недоліком роботи протоколу Нідхема-Шредера є той факт, що Абонент 2 не може точно визначити стан новизни отриманого ключа. Зловмисник, отримавши повідомлення та ключ минулих сеансів, може використовувати старі листи та видавати себе за Абонента 1.

в) **Протокол Kerberos.** Kerberos (укр. Цербер) розроблений в 1987 році працівниками MIT інституту. Він базується на протоколі Нідхема-Шредера та усуває вразливість останнього до атаки з використанням ключів минулих сеансів. Основна відмінність протоколу Kerberos від протоколу Нідхема-Шредера полягає у введенні часової мітки створення сансового ключа $t_{ЦРК}$, часової мітки Абонента 1 – t_{A1} та періоду дії сеансового ключа l. Тепер, Абонент 2, отримавши повідомлення від Абонента 1 зможе з точністю ідентифікувати час створення ключа в ЦРК, час отримання ключа Абонентом 1 та порівняти їх значення з поточним часом. Якщо виконується наступне співвідношення $t_{пот} - t_{A1} \prec l$, то Абонент 2 з впевненістю може сказати що він взаємодіє з Абонентом 1 та створений ключ є сеансовим тільки для поточного сеансу. Остання версія даного протоколу використовуються у ОС AppleMac OS X, Red Hat EnterpriseLinux4, FreeBSD, Solaris, Windows 2000 та наступних версіях. Однак, знайдені вразливості у реалізаціях протоколу [5] не дають підстав гарантувати достовірну надійність його використання. Також, можливість атаки на протокол виникає внаслідок асинхронізації годинників між ЦРК та користувачами системи.

д) Протокол розподілу ключів по паралельним каналам. Вирішення проблеми розподілу ключів часто здійснюється шляхом розбиття ключа на декілька частин та їх передача різними каналами зв'язку. Таким підхід дозволяє зменшити ймовірність відтворення зловмисником усієї

ключової інформації, оскільки для цього потрібно перехопити усі частини ключа. Сама реалізація протоколу у чистому вигляді майже не використовується, адже передача ключа відбувається у незашифрованому вигляді. Натомість, комбінація із тими протоколами які описані в даній статті є досить надійною та має своє застосування у сучасній банківській сфері та галузі державного управління. Недоліками даного протоколу являється висока вартість підтримки надійного функціонування усіх каналів зв'язку. Оскільки при недостатній захищеності хоча б одного із каналів, зловмисник зможе внести зміни у одну із частин ключа, що в свою чергу вплине на достовірність відновлення усього ключа вцілому.

3. Квантовий розподілу ключів. На відмінно від традиційної криптографії, яка для забезпечення секретності даних використовує математичні методи, квантова криптографія заснована на законах фізики (а саме на непорушності постулатів квантової механіки) [6]. Використовуючи квантові явища, цілком можливо створити таку інформаційно-комунікаційну систему, в якій завжди можливо виявляти прослуховування каналу. Це забезпечується тим, що спроба вимірювання взаємозалежних параметрів квантової системи вносить в неї порушення та змінює вихідні сигнали. Таким чином, легітимні користувачі за рівнем шуму в каналі можуть виявляти рівень активності зловмисника.

а) Протокол BB84. Даний протокол квантового розподілу ключів (КРК) запропонований в 1984 році Беннетом Ч. Та Брассардом Ж. До складу системи розподілу ключів за даним протоколом входять передавач та приймач. Передавач складається з генератора, який може посилати фотони в чотирьох поляризаціях (0, 45, 90 чи 135 градусів). Ступінь поляризації залежить від передаваємої в бітах інформації (90 та 135 градусів для “1”, 0 та 45 градусів для “0”). На стороні приймача використовується фіксатор, який визначає вид та ступінь поляризації фотонів. КРК за таким протоколом здійснюється за наступними кроками:

1. Абонент 1 посилає фотони у вибраній довільним чином одній із чотирьох поляризацій.
2. Для кожного отриманого фотону на приймаючій стороні вибирається тип вимірювання (прямолінійне чи діагональне). Результати вимірювання записуються та зберігаються в секреті.
3. Абонент 2 по відкритому каналу передає обраний тип вимірювання кожного фотону.
4. Отримавши повідомлення, Абонент 1 звіряє дані із початковою послідовністю та по відкритому каналу повідомляє про співпадання вибраного типу вимірювання.
5. Абонент 1 та Абонент 2 вибирають всі випадки, в яких відбулося співпадання типу вимірювання поляризації. Ключова інформації отримується шляхом перетворення співпадаючих випадків в біти (0 та 1). Тепер у обох користувачів є однаковий секретний ключ яким і будуть шифруватися повідомлення. Якщо зловмисник буде намагатися перехопити повідомлення під час КРК, то він обов'язково внесе помилки в це повідомлення, так як за законами квантової механіки неможливо виміряти тип поляризації для незв'язаних між собою видів. Тому, легітимні користувачі з легкістю можуть виявити факт прослуховування каналу. Для цього проводиться процедура контролю помилок повідомлення-ключа шляхом співставлення випадково вибраних бітів ключа. При неспівпаданні хоча б одного біту припускається перехоплення повідомлення і процедура передачі ключа повторюється. Якщо всі перевірені біти співпали, ключ вважається достовірним та приймається в експлуатацію.

В роботі [6] виявлена вразливість протоколу BB84 до атаки розподілення числа фотонів. Однак, при використанні слабких когерентних імпульсів з середньою кількістю фотонів в імпульсі 0,1 та квантових каналів з малим коефіцієнтом втрат можливе встановлення секретного ключа та забезпечення стійкості протоколу до цієї атаки. Проте, використовуючи зазначені параметри значно знижується швидкість та відстань передачі ключа. Також, створення систем із можливістю випромінювання однофотонних імпульсів є досить трудоємкою та високовартісною задачею, що у поєднанні з зазначеними вище недоліками передачі ключа ставить під сумнів ефективність використання протоколу вцілому.

б) Протокол B92. Для КРК за даним протоколом використовуються поляризовані в двох різних напрямках фотони. Абонент 1 для кодування бітів використовує два поляризаційні фільтри з кутом між напрямами поляризації в 45 градусів (напрями неортогональні). На приймаючій стороні Абонент 2 використовує фільтри з кутом 90 та 135 градусів поляризації. Таким чином, якщо кут між напрямом поляризації фотона та фільтра становить 90 градусів, то такий фотон не проходить через фільтр. При відмінності в напрямі поляризації в 45 градусів ймовірність проходження фотону через фільтр становить 0,5. Послідовність дій КРК за

протоколом B92 має наступний вигляд:

1. Абонент 1 передає інформацію через два фільтра з орієнтацією в 0 та +45 градусів.
2. Фільтри Абонента 2 зорієнтовані на 90 та 135 градусів відповідно. Отримані поляризовані фотони від Абонента 1 пропускаються через перший чи другий фільтри. Так, наприклад, через один із фільтрів фотон не проходить (наприклад, фільтр в 135 градусів). Оскільки, Абонент 2 не знає що конкретно йому відправлено (0 чи 1), то він і не може з впевненістю сказати який біт він отримав: 1, який відповідає фотону, що не проходить, чи 0, який не проходить через фільтр з ймовірністю 0,5. В той же час, якщо фотон проходить через фільтр, то Абонент 2 впевнений, що отриманий фотон відповідає 0. Таким чином, через один із обраних фільтрів пройде близько 1/4 частина із всієї отриманої послідовності фотонів.
3. Здійснивши попередній крок, Абонент 2 відкритим каналом повідомляє Абоненту 1 інформацію про успішно пройдені 25 фотонів із 100. Вони і стануть ключем для наступного повідомлення. Інформація про застосовані фільтри та отримані значення поляризації повинна зберігатися в таємниці. Тому, навіть, якщо зловмисник перехопить дані у відкритому каналі, він не зможе відтворити ключ без цієї інформації.

Перевагами протоколу B92 являється зменшена кількість поляризованих станів фотонів (два стани B92 у порівнянні з чотирма в BB84), що спрощує апаратну реалізацію такої системи КРК.

Що ж до варіанту перехоплення інформації Зловмисником, то середня кількість помилок внесена нею під час вимірювання базису фотона складатиме 12,5% (що значно менше у порівнянні з 25% протоколу BB84) [6]. Також, ймовірність виявлення прослуховування каналу знижується за рахунок зменшення розміру корисної ключової інформації до 25% (у BB84 вона становить 50%). Загалом, у протоколі B92 значно важче визначити факт прослуховування каналу, що у поєднанні з проблемою передачі інформації на далекі відстані не дає підстав говорити про надійність його використання.

в) Протокол E91 (EPR). Даний протокол запропонований А. Екертом в 1991 році. В його основі лежить парадокс Енштейна-Подольскі-Розенберга (EPR). Так, запропоновано для КРК використовувати пари фотонів, які знаходяться в антисиметричних поляризаційних станах. Це стає можливим внаслідок випромінювання сферичного симетричного атома пари фотонів з протилежним напрямом поляризації [6]. При чому, напрям поляризаціє стає відомим тільки після його вимірювання. Для розподілу ключів за даним протоколом необхідний пристрій для генерації ERP пар фотонів та обладнання, яке дозволяє виміряти стан кожної отриманої частинки на приймаючій стороні. Послідовність дій КРК за протоколом E91 має вигляд:

1. На генераторі створюється M максимально заплутаних пар фотонів. Із кожної пари один фотон відправляється Абоненту 1, а інший — Абоненту 2.
2. Абонент 1 та Абонент 2 здійснюють вимірювання отриманих фотонів використовуючи відповідні проектори. Отримані результати узгоджуються з нерівністю Белла (тест на присутність Зловмисника) та парадоксом ERP.
3. Деяку частину отриманих біт перевіряють відкритим каналом. Не виявивши порушень у квантовій кореляції, не розголошена частина бітової послідовності стає секретним ключем (Абонент 1 чи Абонент 2 попередньо повинні інвертувати отриману послідовність).

Якщо Зловмисник навіть зможе підключитися до каналу, то все-одно вона не знає в якому з базисів необхідно здійснити перевірку фотонів, Тому, мінімум в 50% випадків буде порушена ERP кореляція. Прослуховування каналу виявляється легітимними користувачами шляхом проведення процедури контролю помилок (так само як в протоколах BB84 та B92).

г) Протокол розподілу ключів оснований на кодуванні через часові зсуви. Протокол запропонований в 2003 році Дебушертом Т. та Буше Б., а потім модифікований в 2009 році [6]. Для КРК використовуються когерентні лазерні імпульси, потужність яких послаблена до рівня одиничних фотонів. Алгоритм КРК за даним протоколом має наступний вигляд:

1. Абонент 1 посилає вибрану випадковим чином та однаковою ймовірністю послідовність імпульсів, які кодують біти “0” та “1”. Біт “0” охоплює часові інтервал (0 нс, 100 нс), біт “1” охоплює інтервал (50 нс, 150 нс) від початку такту ЛС.
2. Абонент 2 за допомогою детектору одиночних фотонів фіксує інтервали між отриманими однофотонними імпульсами. Для кожного одержаного імпульсу підраховується

значення зсуву $T_{зс}$ відносно початку такту ЛС. За отриманими даними зсуву відбувається декодування імпульсів в біти:

а) $T_{зс} \in$ (0 нс, 50 нс) — імпульс трактується як біт “0”.

б) $T_{зс} \in$ (100 нс, 150 нс) — імпульс трактується як біт “1”.

в) $T_{зс} \in$ [50 нс, 100 нс] — однозначно декодувати імпульс неможливо і він відкидається.

3. На наступному етапі здійснюється вторинна обробка інформації, шляхом перевірки частини відправленої та отриманої послідовностей на однаковість. Секретна інформація приймається як сирий ключ. Також, відбувається процедура підсилення секретності, при які довжина ключа зменшується на деяке число біт, що залежить від рівня помилок при передачі. Тому, дані Зловмисника про ключ після таких дій стають дуже обмеженими.

д) Для передачі інформації квантовим каналом може використовуватися так званий квантовий прямий безпечний зв'язок (КПБЗ) [7]. Головною особливістю якого є обмін інформацією без будь-яких криптографічних перетворень, що в свою чергу вирішує проблему розподілу криптографічних ключів. Усі існуючі протоколи КПБЗ можна поділити на групи: а) класичний пінг понг протокол та різні його варіанти; б) протоколи з передаванням одиничних кубітів; в) протоколи з передаванням одиничних кубітів блоками.

На теперішній час запропоновано кілька десятків різних за призначенням протоколів КПБЗ [7]. Серед них протоколи для безпосередньої передачі повідомлень між двома користувачами, протоколи для передачі повідомлень від одного користувача до іншого під контролем третьої довіреної сторони, протоколи для передачі повідомлень від одного користувача до багатьох (бродкастінг) і від багатьох до одного, а також протоколи квантових конференцій. Більшість із цих протоколів ґрунтується на створенні і подальшому розподілі між користувачами переплутаних (корельованих) [6, 7] станів двох або більшої кількості кубітів, що дозволяє передавати інформацію у двійковому вигляді. Такі протоколи для практичної реалізації потребують квантової пам’яті великого розміру, яка із сучасним розвитком технологій поки не може широко використовуватися для таких цілей.

1. **Метод довірених кур’єрів.** Здійснення розподілу ключів заданим методом характеризується високою вартістю та значною залежністю від людського фактору. Незважаючи на високі ризики перехоплення інформації зловмисниками – метод активно використовується урядовими структурами. Зазвичай, здійснюється сертифікованими кур’єрами, які передають ключову інформацію від одного легітимного користувача до іншого протидіючи зовнішнім впливам. Розподіл ключів за цим методом, навідмінно від попередньо описаних протоколів, неможливо описати за рахунок математичних чи інших властивостей. Що, разом зі збільшенням відстані між користувачами та їх кількості, використання такого методу в найближчому майбутньому втратить свою актуальність.

Висновки. У цій роботі проведено порівняльний аналіз сучасних методів та протоколів розподілу криптографічних ключів, визначені їх преваги та недоліки. В результаті чого можна зробити висновок, що найбільш перспективним методом розподілу ключів являється квантовий метод, однак на сьогоднішній день, використання протоколів даного методу поки що неможливе. Подальші дослідження будуть направлені на удосконалення існуючих та розробкою більш ефективних методів розподілу ключів.

Список літературних джерел

1. Барычев С. Г. Основы современной криптографии / С. Г. Барычев, В. В. Гончаров, Р. Е. Серов – М.: Горячая линия – Телеком, 2002.

2. Брассар Ж. Современная криптология. - М.: ПОЛИМЕД, 1999.

3. Шнаер Б. Практическая криптография / Н. Фергюсон, Б. Шнаер. – М.: Вильямс, 2005. – 425 с.

4. Krawczyk H. HMQV: A High-Performance Secure Diffie-Hellman Protocol – Crypto, 2005.

5. Множественные уязвимости в Kerberos [Електронний ресурс]: – Режим доступу: - http://www.securitylab.ru/vulnerability/427896.php - Назва з екрану.

6. Румянцев К.Е. Квантовая криптография: принципы, протоколы, системы / К.Е. Румянцев, Д.М. Голубчиков // Всероссийский конкурсный отбор обзорно-аналитических статей по направлению "Информационно-телекоммуникационные системы" – 2008. – 37 с.

7. Василіу Є.В. Синтез структури квантових систем прямого безпечного зв’язку / Є.В. Василіу // Цифрові технології. – 2011, № 9. – С.10 – 21.