© Zhmurko T., Kinzeryavyy V., Yubuzova Kh., Stojanovic A. Generalized classification of modern quantum cryptography and communication methods // Ukrainian Scientific Journal of Information Security, 2015, vol. 22, issue 3, p. 287-293.

УЗАГАЛЬНЕНА КЛАСИФІКАЦІЯ МЕТОДІВ КВАНТОВОЇ КРИПТОГРАФІЇ ТА ЗВ'ЯЗКУ

Тетяна Жмурко[1], Василь Кінзерявий[1], Халіча Юбузова[2], Алєксандар Стояновіч[3]

[1]Національний авіаційний університет, Україна
[2]Казахський національний дослідницький технічний університет ім. К.І. Сатпаєва, Республіка Казахстан
[3]Інститут досліджень квантових обчислень та квантової інформації, Бразилія

ЖМУРКО Тетяна Олександрівна

Рік і місце народження: 1990 рік, м. Вінниця, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: асистент кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, програмний захист інформації, квантова криптографія.
Публікації: більше 20 наукових публікацій, серед яких монографія, наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: taniazhm@gmail.com

КІНЗЕРЯВИЙ Василь Миколайович, к.т.н.

Рік і місце народження: 1985 рік, м. Кам'янець-Подільський, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2014 року.
Наукові інтереси: інформаційна безпека, криптографія та криптоаналіз блокових симетричних шифрів.
Публікації: більше 80 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, патенти та авторські свідоцтва.
E-mail: v.kinzeryavyy@gmail.com

ЮБУЗОВА Халіча Ібрагимівна

Рік і місце народження: 1967 рік, м. Алмати, Республіка Казахстан.
Освіта: Казахський університет шляхів сполучення.
Посада: старший викладач кафедри Інформаційної безпеки.
Наукові інтереси: експертні та інтелектуальні системи, мережеві застосунки, мікропроцесорні системи, передавання, шифрування та кодування інформації.
Публікації: більш ніж 20 наукових статей.
E-mail: hali4a@mail.ru

СТОЯНОВІЧ Алєксандар Деспотовіч

Рік і місце народження: 1982 рік, Ягодина, Сербія.
Освіта: Белградський університет, 2009 рік.
Посада: аспірант (PhD) в UFC Brazil, дослідник в Інституті досліджень квантових обчислень та квантової інформації.
Наукові інтереси: прикладна квантова криптографія, аутентифікація.
Публікації: 4 наукові статті в міжнародних рецензованих журналах.
E-mail: stojanovic.alex1@gmail.com

Анотація. *Розвиток сучасних потужних обчислювальних технологій ставить під загрозу конфіденційність інформації, що забезпечується, як правило, традиційними криптографічними засобами, і змушує дослідників шукати альтернативні методи захисту. З огляду на сучасні тенденції, такими альтернативами можуть стати методи квантової криптографії та зв'язку, що на відміну від традиційних (класичних) аналогів використовують специфічні унікальні властивості квантових частинок і ґрунтуються на непорушності законів квантової фізики. Існуючі класифікації у галузі квантової криптографії та зв'язку не враховують велику кількість сучасних методів – це ускладнює їх дослідження та*

використання при розробці квантових систем захисту інформації. У статті проведено аналіз сучасних методів квантової криптографії та зв'язку, визначено їх переваги і недоліки, оцінювання стійкості до різного роду кібератак, а також досліджено існуючі класифікації цих методів. На підставі часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії, розроблено узагальнену класифікацію методів квантової криптографії та зв'язку. Така класифікація дає можливість виявити низку проблем у цій галузі та дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації.

Ключові слова: *квантова криптографія, класифікація, квантовий прямий безпечний зв'язок, квантовий розподіл ключів, квантова телепортація, квантова теорія ігор, квантовий цифровий підпис.*

Вступ. Останні два десятиріччя бурхливо розвивається новий та неоднозначний у сприйнятті науковців мультидисциплінарний напрямок – квантова криптографія (КК). Як і всі напрямки науки, що змушують науковців сперечатись про їх доцільність, переваги та недоліки, КК досліджується багатьма науковими центрами та університетами, в наслідок чого з'являються нові та удосконалені протоколи, що забезпечують захист інформації, ґрунтуючись на непорушних постулатах квантової фізики, та у своїй більшості досягають теоретико-інформаційної стійкості. Однак, поява великої кількості нових протоколів та методів КК в деякій мірі значно ускладнює роботу науковців та дослідницьких центрів, оскільки їх класифікація проводиться частково та своєчасно не оновлюється, що ускладнює пошук і не дає змоги у повній мірі оцінити рівень існуючих досягнень для їх подальшого ефективного використання.

Аналіз існуючих досліджень і постановка завдання. На сьогодні існує декілька класифікацій методів та протоколів КК, проте вони або орієнтовані на узагальнення протоколів одного виду, наприклад, у роботі [1] представлена класифікація протоколів квантового розділення секрету (КРС, *quantum secret sharing*). У роботі [2] проводиться класифікація квантових протоколів шифрування з відкритим ключем (*quantum public-key encryption protocol*) за шістьма елементами кортежу та виділяють з 64 видів три основні типи протоколів. За аналогічним методом класифікують квантові протоколи симетричного шифрування (*quantum symmetric-key encryption protocols*) [3]. У [4] наведена класифікація протоколів квантової телепортації (КТ), а також представлено двосторонню КТ та двосторонній квантовий прямий безпечний зв'язок (КПБЗ). Часткова класифікація протоколів квантового розподілу ключів (КРК), КРС та систематизація деяких атак на КК проводилась у [5]. Робота [6] представляє класифікацію протоколів одного з напрямків квантової теорії ігор (КТІ). Класифікація Корченка-Васіліу-Гнатюка [7] є однією з найбільш повних, однак вона є досить застарілою – не враховує протоколи КТ, КТІ тощо. Як правило науковці проводять окремо класифікацію різного роду атак на протоколи КК [8-10, 15], а найчастіше досліджують конкретний протокол і конкретну атаку на нього [9-16], тобто стійкість до певного класу атак не виділяють як окрему класифікаційну ознаку.

З огляду на це, **метою** статті є розробка узагальненої класифікацій сучасних методів квантової криптографії та зв'язку за рахунок розширення номенклатури методів та базових ознак.

Основна частина. До методів квантової криптографії та зв'язку відносяться: КРК, КПБЗ, КРС, квантовий потоковий шифр (КПШ), квантовий цифровий підпис (КЦП), квантова стеганографія (КС), КТ та КТІ.

Квантовий розподіл ключів (*quantum key distribution*) – найбільш розвинутий та досліджений напрямок КК, який у сучасних дослідженнях [17] прийнято розділяти на:

– *DV-QKD (discrete-variable)* – КРК з дискретними змінними – як носій інформації використовується фаза фотонів / поляризація, детектором є лічильники фотонів, діапазон передачі – 100 км, в обов'язкові компоненти має входити активне охолоджуюче обладнання. Головна перевага протоколів в тому, що за відсутності помилок, Аліса і Боб (легітимні користувачі) відразу розділяють ідеальний секретний ключ. Проте головними і суттєвими недоліками є відсутність джерел одиночних фотонів і низька ефективність їх детекторів, що спричиняє пошуки інших варіантів реалізації протоколів КРК. Протоколи DV-QKD можуть бути реалізовані з декількома джерелами, але вимагають використання методів обрахунку кідькості фотонів (*photon-counting*). До них відносять такі протоколи [18]: BB84, SARG04, The six-state protocol, Singapore protocol, B92, протоколи типу GV, модифікаціями якого є протоколи Koashi-Imoto та Guo-Shi, а також типу N09, до якого відносять оригінальний протокол N09 та Sun-Wen protocol.

– *CV-QKD (continuous-variable)* – КРК з безперервними змінними – як носій інформації використовуються амплітудно-фазове поле, детектор – когерентний, діапазон передачі – 25 км, компоненти використовуються стандартні. Лічильники фотонів замінені на стандартні p-i-n фотодіоди, які є більш швидкими та більш ефективними. Крім того вони використовують когерентні методи виявлення (*coherent detection techniques*), що широко використовуються в класичних оптичних комунікаціях. Згідно [19-20] вони поділяються на P&M (*Prepare-and-Measure*) та E-B (*Entanglement-base*).

– *DFS-QKD (differential phase shift).* На відміну від DV-QKD та CV-QKD протоколів замість того, щоб бути закодованими в кубіти, ключова інформація кодується в фазу послідовних імпульсів слабкого когерентного світла. У протоколі DPS, Аліса кодує логічні біти у фази імпульсів. Якщо фаза модулюється «0», то Аліса посилає логічний нуль, а якщо фаза між двома імпульсами π, то вона кодує логічну одиницю. Якщо відносна фаза між двома імпульсами дорівнює «0», то Боб виявить «0», і

аналогічно, якщо фаза між двома імпульсами π, то він отримає логічну «1».

Історично перший протокол КРК – *BB84* [21], запропонований у 1894 році Ч. Беннетом та Ж. Брассаром, основними задачами BB84 є генерація та розподіл ключів шифрування між двома абонентами, що з'єднані квантовим та класичним каналами зв'язку, У протоколі BB84 використовуються 4 поляризовані стани фотонів (0°, 45°, 90°, 135°), які передаються квантовим каналом зв'язку. Пошук та виправлення помилок виконується з використанням відкритого класичного каналу, який не повинен бути конфіденційним, тільки аутентифікованим. Для виявлення факту дій зловмисника використовується процедура контролю помилок, а для забезпечення безумовної стійкості використовується класична процедура підсилення секретності (*privacy amplification*).

«Six states» протокол [22] передбачає використання чотирьох станів, аналогічних протоколу BB84, і додатково вводяться ще два можливих напрямки поляризації – правоциркулярний та лівоциркулярний. Такі зміни з одного боку зменшують кількість інформації, що може бути отримана зловмисником, а з іншого боку ефективність протоколу також зменшується (до 33%). Також запропоновано узагальнення протоколу з шістьома станами на багаторівневі квантові системи. Даний протокол має дещо більшу інформаційну місткість та значно більшу стійкість до атаки «перехоплення – повторної посилки» кудитів.

Протокол 4+2 [23] є перехідним між BB84 та B92. У ньому використовуються чотири квантових стани для кодування: «0» та «1» у двох базисах. Стани в кожному базисі вибираються неортогональними, крім того, стани в різних базисах також мають бути попарно неортогональними. Для протоколу 4+2 характерна менша кількість помилок відносно протоколу BB84 для кубітів і менша кількість корисної інформації, що може отримати зловмисник, але одночасно відбувається й зменшення відносної ефективності протоколу.

У протоколі *GV* [24] кодування «0» та «1» виконується за допомогою двох ортогональних станів. Кожен з цих двох станів є суперпозицією двох локалізованих нормалізованих хвильових пакетів. Для захисту проти атаки «перехоплення – повторної посилки» використовується випадковий час відправлення пакетів. Модифікований варіант протоколу Гольденберга-Вайдмана – це протокол *Koashi-Imoto* [25], удосконалений тим, що замість випадкового часу відправлення пакетів використовується асиметризація інтерферометра, тобто світло розбивається у нерівних пропорціях між довгим і коротким плечами інтерферометра.

Протокол *B92* [26] з використанням потужних імпульсів, але зловмисник може одержати більше інформації про ключ для заданого рівня створюваних їм помилок, ніж у протоколі BB84, тобто стійкість протоколу B92 нижче стійкості протоколу BB84. Ефективність протоколу становить 25%.

Протокол E91 [27], відноситься до КРК з використанням переплутаних станів. Під час передавання інформації за протоколом E91 перехоплення одного із фотонів пари не дає зловмиснику ніякої корисної інформації. Крім того, запропоновано узагальнення схеми Екерта на тривимірні та багатовимірні квантові системи, що значно збільшує інформаційну місткість протоколу.

Протоколи зі станами «приманки» (decoy states protocols) є удосконаленим варіантом протоколу BB84, у якому відправник, шляхом заміни підмножини імпульсів, вводить так звані приманки [28]. Даному типу протоколів характерний більш високий рівень безпеки, ніж у BB84. Крім того, такі протоколи відзначаються стійкістю проти PNS атаки. До явних переваг протоколів зі станами «приманки» також можна віднести і збільшення довжини каналу за рахунок лінійної залежності від втрат у каналі. Проте, без попередньої аутентифікації користувачів на таких протоколах не можливо побудувати завершене повноцінне рішення проблеми розподілення криптографічних ключів.

SARG04 protocol [29] на рівні квантової частини протокол еквівалентний BB84, проте замість джерел одиночних фотонів використовуються послаблені лазерні імпульси. Стійкий до PNS атаки.

COW (coherent one-way) protocol [30] – це новий протокол для практичної квантової криптографії, розроблений Н. Жізаном (N. Gisin) та ін. в 2004 р. У протоколі Аліса (передавач) посилає пару імпульсів, один порожній і один непорожній (містить середнє число фотонів 0,5). Біти кодуються в парі імпульсів, з значенням біту визначають по положенню непорожнього імпульсу: перше положення «0» і друге положення «1». Боб, приймач, використовує детектор, щоб розрізняти імпульси. Аліса і Боб також перевіряють узгодженість імпульсів. Боб випадковим чином вибирає невелику частину імпульсів, що не використовується як дані, щоб відправити на інтерферометр, який вимірює когерентність між суміжними кубітами. У зв'язку з цим заходом безпеки, зловмисник не може виконати PNS-атаку, так як видалення або блокування фотонів, неможливе без порушення системи. На відміну від інших протоколів інтерферометр використовується тільки для оцінки інформації на когерентність і не може призвести до помилок на ключі. Протокол не використовує посимвольний тип кодування (як BB84, B92, SARG04).

KMB09 [31] (розроблений Khan M.M., Murphy M., Beige A. у 2009 р.) – протокол у якому Аліса і Боб використовують два взаємно неупереджені базиси – один із них кодує «0», а інший кодує «1». Безпека схеми обумовлено швидкістю передачі мінімального індексу помилки (ITER) і квантового рівня помилок, що вноситься зловмисником. ITER значно збільшується для більш високих розмірностей фотонних станів. Це дозволяє мати більше шуму в лінії передачі, тим самим збільшуючи можливу відстань між Алісою та Бобом без необхідності проміжних вузлів.

Квантовий прямий безпечний зв'язок [32-34, 51-53] характерною особливістю даного методу є відсутність криптографічних перетворень, відповідно відсутня і проблема розподілу ключів

шифрування. Протоколи КПБЗ можна поділити на такі типи: пінг-понг (PP) протокол (різні його варіанти) [33, 35, 51-53], протоколи з передаванням переплутаних кубітів блоками [36], протоколи з одиничними кубітами та протоколи з групами переплутаних кудитів.

Більшість запропонованих до теперішнього часу протоколів КПБЗ потребують передачі кубітів блоками. Це дозволяє виявити прослуховування квантового каналу до початку передачі самого повідомлення й таким способом гарантувати безпеку передачі – якщо прослуховування виявлене до передачі повідомлення, то легітимні сторони переривають сеанс і ніяка інформація не витікає до зловмисника. Але для зберігання таких блоків кубітів необхідна квантова пам'ять великого об'єму. Технологія квантової пам'яті активно розробляється, але поки ще далека від масового застосування в стандартному телекомунікаційному устаткуванні. Тому з погляду технічної реалізації перевагу мають протоколи, у яких передача здійснюється одиничними кубітами або невеликими їхніми групами (за один цикл протоколу). Таких протоколів запропоновано небагато, і вони мають тільки асимптотичну безпеку, тобто атака буде виявлена з високою ймовірністю, але до цього зловмисник зможе одержати деяку частину повідомлення. Отже, виникає проблема підсилення безпеки таких протоколів, тобто створення таких методів попередньої обробки передаваної інформації, які зроблять перехоплену зловмисником інформацію для нього некорисною.

Квантове розділення секрету. Переважна частина квантових протоколів розділення секрету (КПРС) використовує властивості переплутаних квантових станів [37-38]. У роботах [1, 51-53] наведено детальний огляд сучасного стану протоколів КРС та проведено їх класифікацію.

Квантовий потоковий шифр передбачає шифрування даних подібно до класичних потокових шифрів, але із застосуванням квантового шумового ефекту [39] і може використовуватись в оптичних комунікаційних мережах. КПШ базується на протоколі *Yuen 2000 (Y-00)* [40-41, 51-53]. Вихідними даними передавача у даній схемі є послідовність когерентних станів, що переносить інформацію про дані чи ключ. Теоретико-інформаційна стійкість протоколу Y-00 забезпечується рандомізацією, що базується на квантовому шумі, а також на додаткових математичних (обчислювальних) схемах. Ще однією перевагою КПШ є більша захищеність порівняно із звичайними потоковими шифрами завдяки квантовому шумовому ефекту і неможливості клонування квантових станів. Що стосується недоліків КПШ, то варто відмітити, перш за все, складність практичної реалізації системи [42].

Квантовою телепортацією називається передача квантового стану на відстань за допомогою роз'єднаної в просторі заплутаної пари і класичного каналу зв'язку, при якій стан руйнується в точці відправлення при проведенні вимірювання, після чого відтворюється в точці прийому**.** При цьому обов'язковою є передача інформації між джерелом і приймачем класичним, неквантовим каналом, яка може здійснюватися не швидше, ніж зі швидкістю світла. Протоколи КТ розділяють на два класи: *імовірнісні* та *детерміновані*. Експерименти та протоколи групи науковців під керівництвом Цайлінгера та Де-Мартіні – відносять до імовірнісних (для таких протоколів не важливо скільки фотонів загубиться при пересиланні, вони більш придатні для передачі на великі відстані). Детальне дослідження протоколів проведено у [43].

Квантова теорія ігор. Одним з напрямків у дослідженнях КК є вивчення різних стратегій передачі повідомлення одержувачу, для цього використовуються основи теорії ігор з елементами квантової фізики. У деяких випадках дії відправника і зловмисника розглядаються як асиметрична квантова гра двох гравців [44]. У КТІ суперпозиція використовується для моделювання невизначеності, коли неможливо знати, якою стратегією в цей момент часу скористається гравець. У класичному математичному апараті теорії ймовірності такої можливості немає, там враховується лише ймовірність, з якою гравець може вибрати ту чи іншу стратегію. А використання суперпозиції для моделювання цієї невизначеності дозволить вирішувати завдання, які стандартна імовірнісна концепція описати не може. Загальна схема квантової гри наведена у [45] та полягає у наступному: побудова квантової гри починається з вибору початкового стану і визначення можливої заплутаності системи двох гравців. Далі шукають можливі квантові рішення (стратегії) гравців різних типів. Після того, як обидва гравці вибрали свою індивідуальну квантову стратегію, вводиться оператор розчеплення (розплутування) для підготовки вимірювання стану гравців. Оператори заплутування і розплутування залежать від додаткового параметра, який вимірює ступінь заплутаності системи. Очікуваний виграш у квантовій версії загальної гри двох гравців залежить від матриці виграшів і спільної ймовірності спостерігати чотири вимірюваних величини, які і є результатами гри. Квантовий стан заплутаності двох гравців зовсім не означає, що заплуталися самі гравці (або їх думки). Процес квантової декогеренції забороняє такі макроскопічні заплутані системи, створені з мікроскопічних квантових частинок.

До КТІ [46] входять такі протоколи як квантове вручення біту (*quantum bit commitment*), квантове підкидання монети (*quantum coin tossing*) та квантова рулетка (*quantum gambling*). Поняття класичного вручення біту (математична версія відправки заклеєного конверту) є загальним примітивом для розробки секретних криптографічних протоколів. Дані, що відправляються від Аліси до Боба перебувають у стані замкнутості (локінгу) і можуть бути розшифровані тільки при вручені Бобу ключа від Аліси. *Квантове вручення біту* [47], як і квантові протоколи розподілу ключів, забезпечує теоретико-інформаційну (безумовну) стійкість. Проте, спираючись лише на властивості квантового каналу, експериментальне квантове вручення бітів неможливе. Ця проблема була вирішена науковцями

у 2013 р. шляхом поєднання квантової фізики і теорії відносності, при цьому відбулася передача безумовно стійкого повідомлення (між Женевою та Сінгапуром за 50 мс).

Квантове підкидання монети [47] використовує квантові монети, які, на відміну від звичайних, можуть перебувати у нескінченній кількості станів. Також, можливі деякі змішані стани, які пояснюються явищем суперпозиції у квантовій механіці. Використання змішаної позиції гарантує одній зі сторін постійний виграш. Якщо Аліса використовує змішаний стан, то у будь-якому випадку, не залежно від дій Боба з монетою, і за умови попередньої домовленості про кінцеве число ходів, вона буде вигравати, оскільки у кінці гри зможе перевести свою монету зі змішаного стану в чистий (абсолютний).

Квантова рулетка [46], завдяки використанню непорушних постулатів квантової механіки, унеможливлює шахрайство, яке можливе у класичній версії гри «вибір виграшної коробки». Наприклад, Аліса приховує м'яч у будь-якій коробці, а Боб відгадує його місцезнаходження. Якщо грали віддалено, Аліса може легко збрехати про виграш. Або, якщо коробки були з Бобом, він міг обдурити, стверджуючи, що він знайшов м'яч. Використовуючи квантову рулетку шахрайство неможливе з огляду на те, що опоненти можуть завжди з'ясувати, який вибір зробив інший, коли гра закінчена (завдяки суперпозиції своїх дій). Хоча зазначені протоколи є лише примітивами безпеки, проте на їх основі можуть бути побудовані більш складні протоколи, здатні повністю змінити уявлення про безпеку в інформаційно-комунікаційних системах. Окрім того, також проведено багато досліджень та багато класичних ігор переведено у квантовий простір, наприклад, «prisoners' dilemma», «the battle of the sexes», «the Monty Hall problem», «rock-scissors-paper», «quantum tic-tac-toe» [48, 50].

З урахуванням зазначених методів квантової криптографії та зв'язку, а також нової базової ознаки (стійкість до певного типу кібератак), узагальнена класифікація матиме такий вигляд (рис. 1):

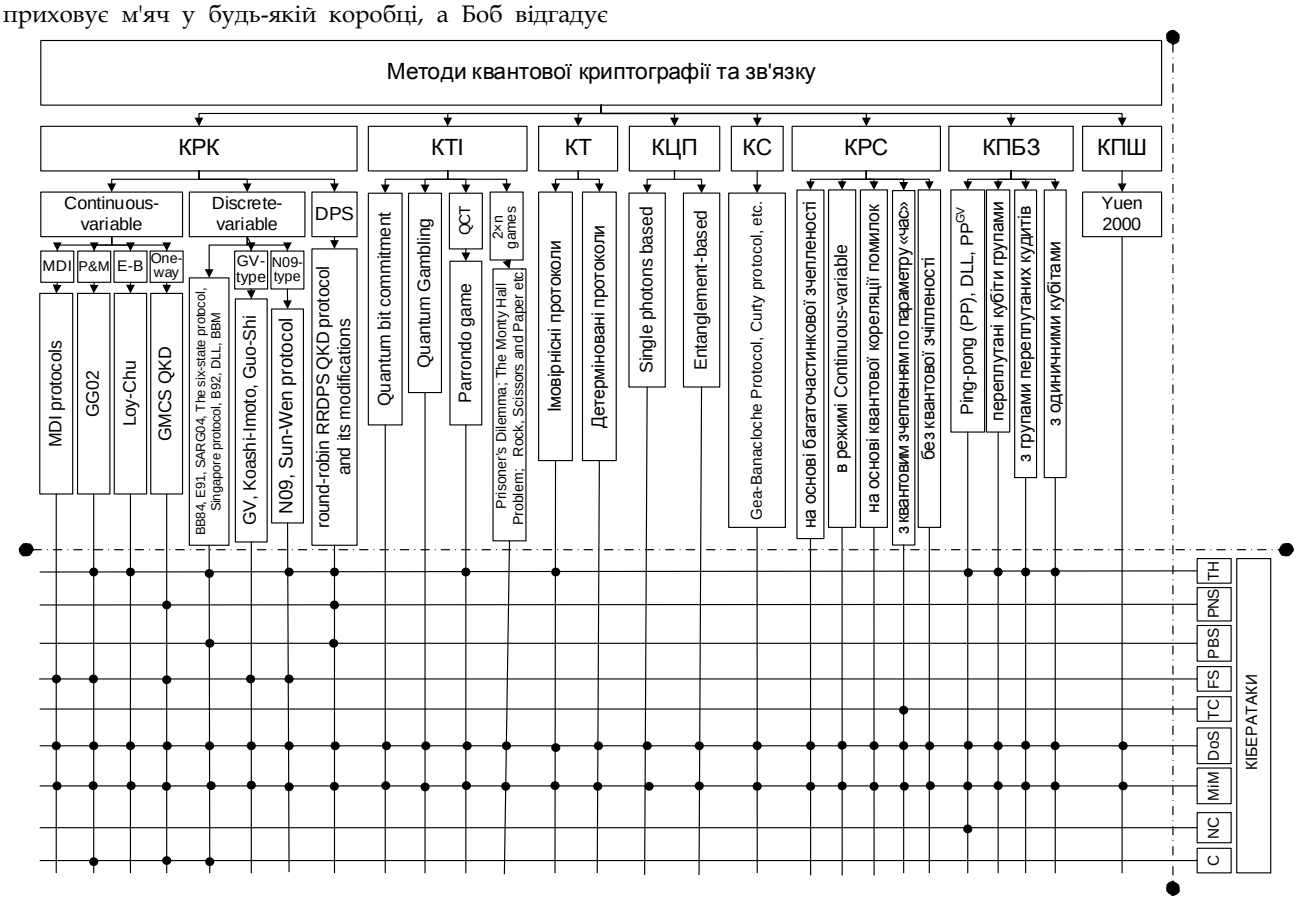

Рис. 1. Узагальнена класифікація методів квантової криптографії та зв'язку

Висновки. Таким чином, у цій роботі проведено аналіз сучасних методів та протоколів квантової криптографії і зв'язку (визначено їх переваги і недоліки), їх існуючі класифікації. На підставі часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії, розроблено узагальнену класифікацію. За рахунок розширення номенклатури методів та базових ознак, ця класифікація, дає можливість виявити низку проблем у цій галузі та дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації.

Література

[1] Лимарь И.В., Василиу Е.В. Классификация квантовых технологий разделения секрета / Захист інформації. – Том 16. – №3. – 2014 – С. 201-214.

[2] Chenmiao W., Li Ya. A complete Classification of Quantum Public-key Encryption Protocols Available from: http://arxiv.org/pdf/ 1507.03765v2.pdf

[3] Chong X., Li Y., Yong P. Dongqing Chen The Classification of Quantum Symmetric-Key Encryption Protocols. Available from: http://arxiv.org/pdf/1006.4216.pdf

[4] Hassanpour S., Houshmand M. Bidirectional quantum teleportation and secure direct communication via entanglement swapping. Available from http://arxiv.org/ftp/arxiv/papers/1411/1411.0206.pdf

[5] Xiaoqing T. Introduction to Quantum Cryptography (part of Theory and Practice of Cryptography and Network Security Protocols and Technol.) Available from http://cdn.intechopen.com/pdfs-wm/43793.pdf

[6] D'ariano G.M. Quantum bit commitment: a complete classification of protocols. Available from http://www.qubit.it/research/publications/0209150.pdf

[7] Korchenko O., Vasiliu E., Gnatyuk S. Modern quantum technologies of information security, Aviation. Vilnius: Technika, Vol. 14, No. 2, 2010, p. 58-69.

[8] Кузнецова А.В. Стратегии атак на квантовые протоколы защиты информации. – Цифрові технології. – № 14. – 2013. – С. 134-137.

[9] Scarani V., Ribordy G., Gisin N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. Available from: http://www.unige.ch/gap/quantum/ _media/publications:bib: prl57901.pdf

[10] Корченко А.Г. Методы перехвата информации в информационно-коммуникационных системах на основе квантових технологий / А.Г. Корченко, Е.В. Василиу, Т.А. Жмурко, С.А. Гнатюк // Монография. – Х. : Цифрова друкарня. – № 1, 2013. – С. 98-110.

[11] Waks E. Security of Quantum Key Distribution with Entangled Photons Against Individual Attacks / E. Waks, A. Zeevi, Y. Yamamoto // Physical Review A. – 2002. – V. 65, issue 5. – 052310.

[12] Василиу Е.В. Анализ атаки на пинг – понг протокол с триплетами Гринбергера-Хорна-Цайлингера / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 15-24.

[13] Василиу Е.В. Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов / Е.В. Василиу, Р.С. Мамедов // Восточноевропейский журнал передовых технологий. – 2009. – № 4/2 (40). – С. 4-11.

[14] Василиу Е.В. Анализ атаки двух злоумышленников на протокол квантовой прямой безопасной связи / Е.В. Василиу, С.В. Николаенко // Труды Северо-Кавказ. фил. МТУСИ. – 2013. – С. 324-330.

[15] Suzuki S., Rodney V. Classification of Quantum Repeater Attacks. Available from: www.internetsociety.org/sites/default/files/01_2_3.pdf

[16] Jain N., Anisimova E., Khan I. et al. Trojan-horse attacks threaten the security of practical quantum cryptography. Available from http://iopscience.iop.org/1367-2630/16/12 /123 030

[17] Scarani V. et al. The security of practical quantum key distribution, Avail. from: http://quic.ulb.ac.be/ media/publications/2009-rmp-81-001301.pdf

[18] Shukla C., Banerjee A., Pathak A. Secure Quantum Communication with Orthogonal States Available from: http://arxiv.org/pdf/1407.3412.pdf

[19] Cutolo A., Mignani A.G., Tajani A. Photonics for safety and security, World Scientific Publishing Co. Pte. Ltd. – Singapore. – 2014. – 422 p.

[20] Cerf N.J., Leuchs G., Polzik E.S. Quantum information with CV of atoms and Light, Imperial College Press, 2007. – 604 p.

[21] Bennett C.H., Brassard G. Quantum cryptography: public key distribution and coin tossing // Proceedings of the IEEE Intern. Conf. on Comp., Syst. and Signal Proces. – Bangalore, India. – 1984. – P. 175-179.

[22] Bruss D. Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters. – 1998. – V. 81, № 14. – P. 3018-3021.

[23] Huttner B., Imoto N., Gisin N., Mor T. Quantum Cryptography with Coherent States // Physical Review A. – 1995. – V. 51, № 3. – P. 1863-1869.

[24] Goldenberg L., Vaidman L. Quantum Cryptography Based On Orthogonal States // Physical Review Letters. – 1995. – V. 75, № 7. – P. 1239-1243.

[25] Koashi M., Imoto N. Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps, Phys. Rev.Let., 1997, V. 79, № 12, P. 2383-2386.

[26] Bennett C.H. Quantum cryptography using any two non-orthogonal states // Physical Review Letters. – 1992. – V. 68, № 21. – P. 3121–3124.

[27] Ekert A. Quantum cryptography based on Bell's theorem, Phys. Rev. Let., 1991, V. 67, № 6, P.661-663.

[28] Wang X.-B. Comment on Decoy State Quantum Key Distribution // arXiv:quant-ph/0501143

[29] Scarani V., Acin A., Ribordy G., Gisin N., Phys. Rev. Lett. 92, 2004, 057901.

[30] Gisin N. et al., Rev. Mod. Phys., 74, 2002, P.145-195.

[31] Khan M.M., Murphy M., Beige A. High error-rate quantum key distribution for long-distance communication Available from: http://iopscience.iop.org/ article/10.1088/1367-2630/11/6/063043/pdf

[32] Chuan W., Fu Guo D., Gui Lu L. Multi-step quantum secure direct communication using multi-particle Greenberg-Horne-Zeilinger state. – Optics Communications. – 2005. – V. 253. – P. 15-19.

[33] Bostrom K., Felbinger T. Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.

[34] Cai Q.-Y., Li B.-W. Improving the capacity of the Bostrom – Felbinger protocol // Physical Review A. – 2004. – V. 69, № 5. – 054301.

[35] Василиу Е.В., Василиу Л.Н. Пинг-понг протокол с трех– и четырехкубитными состояниями Гринбергера-Хорна-Цайлингера // Труды Одесского политех. ун-та. – 2008. – Вып. 1(29). – С. 171-176.

[36] Wang Ch., Deng F.-G., Li Y.-S. et al. Quantum secure direct communication with high dimension quantum superdense coding // Physical Review A. – 2005. – V. 71, № 4. – 044305.

[37] Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. – М.: Мир, 2006. – 824 с.

[38] Стин Э. Квантовые вычисления. Перевод с английского И.Д. Пасынкова: НИЦ «Регулярная и хаотическая динамика», М. – Ижевск, 2000. – 111 с.

[39] Yan F.-L., Gao T., Li Yu.-Ch. Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations // Chinese Phys.Let. – 2008. – V. 25, № 4. – P. 1187 – 1190

[40] Yuen H. P. KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation // arXiv:quant-ph/0311061

[41] Nair R., Yuen H.P. On the Security of the Y-00 Direct Encryption Protocol // arXiv:quant-ph/0702093v2

[42] Hirota O., Kurosawa K. An immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol // arXiv:quant-ph/0604036v1

[43] Hassanpour S., Houshmand M. Bidirectional quantum teleportation and secure direct communication via entanglement swapping http://arxiv.org/ abs/1411.0206

[44] Eisert J., Wilkens M., Lewenstein M. Quantum games and quantum strategies, http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.83.3077

[45] Старобогатов Р. Квантовые стратегии предотвращения финансово-экономических кризисов http://econf.rae.ru/pdf/2012/05/1282.pdf

[46] Жмурко Т.О. Протоколи квантової теорії ігор / Т.О. Жмурко // Політ. Сучасні проблеми науки: міжнар. наук.-практ. конф. молодих учених і студентів, м. Київ, 2-3 квітня 2014 р., НАУ. – С. 6.

[47] Nayak A., Sikora J., Tunzel L. Quantum and classical coin-flipping protocols based on bit-commitment and their point games http://arxiv.org/abs/1504.04217

[48] Flitney A.P., Abbott D. An introduction to quantum game theory http://arxiv.org/pdf/quant-ph/0208069.pdf

[49] Gnatyuk S., Zhmurko T., Falat P. Efficiency increasing method for quantum secure direct communication protocols // Proc. of the EEE 8th Intern. Conf. on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – p. 468-472.

[50] Leaw J.N., Cheong S.A. Strategic Insights From Playing the Quantum Tic-Tac-Toe http://arxiv.org/abs/1007.3601v1

[51] Корченко О.Г., Васіліу Є.В., Гнатюк С.О. Сучасні квантові технології захисту інформації // Захист інформації. – 2010, № 1. – С. 77-89.

[52] Korchenko O.G., Vasiliu Ye.V., Gnatyuk S.O. Modern directions of quantum cryptography // Proc. of the fourth world congress «Aviation in the XXI-st century» – «Safety in Aviation and Space Technologies». – Kyiv, 2010. – V. 1. – P. 17.1-17.4.

[53] Korchenko O., Vasiliu Ye., Gnatyuk S. et al. Quantum Secure Telecommunication Systems, Telecommunications Networks – Current Status and Future Trends (ed. by J.H. Ortiz), InTech, 2012, p. 211-236.

УДК 003.26:004.056.55:621.39 (045)

Жмурко Т.А., Кинзерявый В.Н., Юбузова Х.И., Стоянович А.Д. Обобщенная классификация методов квантовой криптографии и связи

Аннотация. *Развитие современных мощных вычислительных технологий ставит под угрозу конфиденциальность, которая обеспечивается, как правило, традиционными криптографическими средствами, и заставляет исследователей искать альтернативные методы защиты. Учитывая современные тенденции, такими альтернативами могут стать методы квантовой криптографии и связи, которые в отличии от традиционных (классических) аналогов используют специфические уникальные свойства квантовых частиц и основываются на незыблемости законов квантовой физики. Существующие классификации в области квантовой криптографии и связи не учитывают большое количество современных методов – это затрудняет их исследование и использование при разработке квантовых систем защиты информации. В статье проведен анализ современных методов квантовой криптографии и связи, определены их преимущества и недостатки, проведена оценка их устойчивости к различного рода кибератакам, а также исследованы существующие классификации этих методов. На основе частичных обобщений теоретических положений и практических достижений в области квантовой криптографии, разработана обобщенная классификация методов квантовой криптографии и связи. Такая классификация дает возможность определить ряд проблем в этой области и позволяет расширить возможности выбора соответствующих методов для построения современных квантовых систем защиты информации.*

Ключевые слова: *квантовая криптография, классификация, квантовая прямая безопасная связь, квантовое распределение ключей, квантовая телепортация, квантовая теория игр, квантовая цифровая подпись.*

Zhmurko T., Kinzeryavyy V., Yubuzova Kh., Stojanovic A. Generalized classification of modern quantum cryptography and communication methods

Abstract. *Modern powerful computing technology development threatens the confidentiality of information that usually provided by traditional cryptographic means and forces researchers to look for alternative security methods. Given the current trends, these alternatives may be quantum cryptography and communication methods. These methods unlike traditional (classical) analogues use specific unique properties of quantum particles and are based on the inviolability of the quantum physics laws. Existing classifications in quantum cryptography and communications do not include the large number of modern methods. It complicates its study and use in the quantum information security systems development. In the paper modern methods of quantum cryptography and communication were analyzed, their advantages and disadvantages, security assessment to various kinds of cyberattacks were defined, and also the existing classifications of these methods were studied. On the basis of partial generalizations of theoretical positions and practical advances in quantum cryptography, the generalized classification of quantum cryptography and communication methods was constructed. This classification reveals a problem in this area and can extend the possibilities for choosing the appropriate methods for modern quantum information security systems development.*

Key words: *quantum cryptography, classification, quantum secure direct communication, quantum key distribution, quantum teleportation, quantum game theory, quantum digital signature.*

Отримано *08 жовтня 2015 року*, затверджено редколегією *27 листопада 2015 року*