НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ЖМУРКО Тетяна Олександрівна

УДК 003.26:621.39:530.145

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ КВАНТОВОЇ КРИПТОГРАФІЇ

Спеціальність 05.13.21 – «Системи захисту інформації»

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Київ – 2016

Дисертацією є рукопис.

Робота виконана в Національному авіаційному університеті Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент **Гнатюк Сергій Олександрович,** Національний авіаційний університет, доцент кафедри безпеки інформаційних технологій.

Офіційні опоненти: доктор технічних наук, професор **Карпінський Микола Петрович,** Університет у Бєльсько-Бялій, керівник кафедри інформатики та автоматизації;

доктор технічних наук, професор **Рудницький Володимир Миколайович,** Черкаський державний технологічний університет, завідувач кафедри інформаційної безпеки та комп'ютерної інженерії.

Захист відбудеться «26» квітня 2016 р. о 13^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «__»_____ 2016 р.

В.о. ученого секретаря спеціалізованої вченої ради д.т.н., професор В.П. Квасніков

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Впроваджені в усі найважливіші сфери діяльності суспільства новітні інформаційно-комунікаційні технології (ІКТ), з одного боку, відкривають широкі можливості щодо створення та використання сучасних мережевих та Інтернет сервісів, а з іншого боку – породжують цілу низку нових уразливостей та специфічних загроз. Відкритість та публічність таких сервісів разом з еволюцією атак у кіберпросторі (кібератак), суттєвим збільшенням користувачів ІКТ і обсягів інформації, яка обробляється, зберігається та передається за допомогою ІКТ, ставлять під загрозу конфіденційність інформації. Як правило, конфіденційність інформації забезпечується методами симетричної та асиметричної криптографії, що не позбавлені певних недоліків. Для симетричних методів, зокрема, характерна проблема розподілу секретних ключів, а асиметричні методи повільні та потребують значних обчислювальних ресурсів. Крім того, стійкість усіх традиційних криптосистем залежить від обчислювальних можливостей порушника і базується на гіпотетичній неможливості розв'язання певного класу математичних задач за поліноміальний час – пошук у повністю невпорядкованій базі даних, факторизація та логарифмування в дискретних полях великого розміру тощо. Проте ця гіпотеза може бути спростована за допомогою багатокубітних квантових комп'ютерів (D-Wave 2X), GRID-технологій, HPC та інших сучасних ІКТ. З огляду на це, великий інтерес викликає квантова криптографія (КК), яка не залежить від обчислювальних потужностей порушника, використовує специфічні унікальні властивості квантових частинок і ґрунтується на непорушності законів квантової фізики. Основними перевагами методів КК є можливість точного виявлення порушника і забезпечення, в деяких випадках, теоретико-інформаційної (абсолютної) стійкості. На сьогодні такі методи і системи пройшли складний шлях від теоретичних гіпотез і лабораторних експериментів до повноцінних комерційних рішень.

Значний внесок у розвиток теорії й практики квантової криптографії внесли такі вітчизняні та закордонні вчені: Ф. Балаж, Ч. Беннет, Ж. Брассар, Є. Васіліу, Н. Гісін, С. Гнатюк, О. Гомонай, А. Еккерт, П. Завадскі, У. Збінден, Ш. Імре, В. Кінзерявий, С. Кілін, О. Корченко, Н. Лютенхаус, С. Ніколаєнко, М. Нільсен, К. Румянцев, А. Семенов, В. Скарані, А. Цайлінгер, І. Чанг та ін.

Переважна більшість досліджень є орієнтованими на методи квантового розподілу ключів (BB84, B92, SARG, E91, Гольденберга-Вайдмана, Коаші-Імото тощо), які дозволяють вирішити проблему розподілу ключів шифрування в умовах секретності і використовуються, як правило, у комплексі з симетричними криптографічними методами (AES, 3DES). Іншим важливим напрямком КК є використання методів квантового прямого безпечного зв'язку (КПБЗ), які дозволяють передавати інформацію відкритим каналом (без попереднього її шифрування – проблема розподілу ключів нівелюється). На сьогодні запропоновано велику кількість методів КПБЗ, що базуються на різних квантових технологіях і можуть використовуватись як для захищеного передавання інформації (за допомогою кубітів або кудитів), так і для розподілу криптографічних ключів. З точки зору інформаційної місткості найбільш ефективними методами є ті, що використовують трійкові квантові системи (кутрити), оскільки найбільшу щільність запису інформації має система числення з основою рівною основі натуральних логарифмів, тобто рівною числу Ейлера (для цілочисельних – це трійкова або тритова система). Зважаючи на асимптотичну стійкість методів КПБЗ відомий підхід до підвищення стійкості до некогерентних атак, зокрема кутритових методів, шляхом застосування зворотного хешування за допомогою оборотних трійкових матриць.

Генерування останніх потребує великих часових та ресурсних затрат (значна кількість математичних перетворень над полем $GF(3)$), а з огляду на те, що відомі методи генерування (генератори) орієнтовані на бінарні системи, а методи оцінки рівня випадковості, як правило, працюють з двійковими псевдовипадковими послідовностями (ПВП), то складно оцінити ефективність і доцільність застосування запропонованого підходу до підвищення стійкості методів КПБЗ.

З огляду на це, розробка і дослідження нових ефективних методів забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів ПВП та оцінювання їх якості (можливості використання для криптографічних застосувань) є *актуальною науково-практичною задачею,* що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки» в частині п.1.2.8.1. «Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії», зі Стратегією національної безпеки України від 26 травня 2015 року № 287/2015 у контексті п.4.12 «Забезпечення кібербезпеки і безпеки інформаційних ресурсів, зокрема реформування системи технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС», зі Стратегією кібербезпеки України від 15 березня 2016 року №96/2016 і Рамковою програмою ЄС з досліджень та інновацій «Горизонт 2020», зокрема за напрямками DS-05-2016 та DS-06-2017 («Нові напрямки інноваційних наукових досліджень в Європі щодо забезпечення кібербезпеки як відповідь на сучасні виклики, зокрема квантова криптографія»). Результати роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету «Організація систем захисту інформації від кібератак» (д.р. № 0111U000171), «Методи та засоби захисту інформації на основі квантових технологій» (реєстраційний номер № 43/14.02.04), «Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах» (реєстраційний номер № 61/09.01.08), «Новітні технології криптографічного захисту інформації» (реєстраційний номер № 100/14.01.06), «Методи підвищення ефективності систем квантової криптографії» (реєстраційний номер № 26/09.01.08) та Кіровоградського національного технічного університету «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах», (д.р. № 0115U003103), у яких здобувач брав участь у якості виконавця.

Мета і задачі дослідження. Метою дисертаційної роботи є підвищення ефективності протоколів квантової криптографії шляхом розробки методів забезпечення стійкості кутритових протоколів і систем, побудови тритових генераторів псевдовипадкових послідовностей та оцінювання їх якості.

Для досягнення поставленої мети **необхідно розв'язати такі основні задачі:**

– проаналізувати сучасні методи та протоколи квантової криптографії, їх ефективність і стійкість до різного роду кібератак для їх класифікації і чіткого визначення завдання дослідження;

– розробити метод забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, що не потребує великих часових та ресурсних затрат;

– розробити метод генерування тритових псевдовипадкових послідовностей для криптографічних застосувань, зокрема для реалізації методу забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак;

– розробити метод оцінювання якості (рівня випадковості) тритових псевдовипадкових послідовностей для визначення криптостійкості (оцінювання статистичних параметрів та закономірностей) тритових генераторів і доцільності використання сформованих трійкових послідовностей для криптографічних застосувань;

– розробити спеціалізоване програмне забезпечення та методику для проведення експериментів і верифікації запропонованих методів.

Об'єктом дослідження є процес захисту інформації методами квантової криптографії.

Предметом дослідження є методи, способи та моделі підвищення ефективності протоколів квантового прямого безпечного зв'язку.

Методи дослідження. Проведені дослідження базуються на сучасних методах квантової теорії інформації, квантової механіки та імітаційного моделювання (моделювання процесу передавання кутритів за протоколами КПБЗ, моделювання методів забезпечення стійкості від некогерентних атак, дослідження кібератак на квантові системи), традиційної криптографії (розробка методів забезпечення стійкості та формування трійкових ПВП), об'єктно-орієнтованого програмування (розробка програмного забезпечення (ПЗ) для реалізації запропонованих методів) та математичної статистики (розробка низки статистичних тестів для оцінювання якості трійкових ПВП).

Наукова новизна одержаних результатів полягає у такому:

– *отримав подальший розвиток* метод забезпечення стійкості кутритових протоколів квантової криптографії, який, за рахунок неквантової функції перевірки цілісності та використання тритової симетричної функції, дозволяє звести до мінімуму кількість перемикань між режимами протоколу (передавання повідомлення та контролю підслуховування), збільшити швидкість роботи при збереженні стійкості до некогерентних атак;

– *отримав подальший розвиток* метод генерування псевдовипадкових послідовностей, який, за рахунок виконання нової послідовності операцій (підстановок, лінійного розсіювання, динамічного циклічного зсуву та додавання за модулем 3 та 3^l) над вектором внутрішніх станів V_p ($V_p = \{0,1,2\}^p$, $p = 14 \cdot l$) за $r \cdot b$ циклів, дозволяє формувати трійкові незбалансовані («0», «1», «2») псевдовипадкові послідовності $V_{m \cdot b}$, $m = 4 \cdot l$;

– *отримав подальший розвиток* метод оцінювання якості псевдовипадкових послідовностей, який, за рахунок комплексної інтерпретації згенерованих чисел, введення диференційованих ймовірностей $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ і трійкових коефіцієнтів для функції помилок *erfc* та неповної гамма функції *igamc*, дає можливість оцінювати статистичні параметри і закономірності тритових псевдовипадкових послідовностей.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані для підвищення ефективності (захищеності, швидкості роботи) систем захисту на базі КПБЗ і квантового розподілу ключів, а також для деяких процедур безпеки в традиційних (неквантових) криптографічних системах захисту інформації. Практична цінність роботи полягає у такому:

– розроблено класифікацію методів КК, яка, за рахунок розширення множини відомих базових ознак і часткових узагальнень теоретичних положень та практичних досягнень у галузі КК, дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації (на базі КПБЗ та інших квантових технологій);

– використання результатів дисертаційного дослідження дозволило підвищити захищеність інформації з обмеженим доступом, що підтверджується актами впровадження у діяльність ТОВ «Сайфер ЛТД» (акт від 28.10.2015 року) та Bilfinger HSG (Німеччина) (акт від 03.09.2015 року);

– розроблено низку комп'ютерних програм, захищених свідоцтвами про реєстрацію авторського права на твір, зокрема «Імітаційна модель пінг-понг протоколу в квантовому каналі з шумом» (№ 36373 від 04.01.2011 року), «GenSBOX3» (№ 48037 від 26.02.2013 року), «TrytTon 2012» (№ 48040 від 26.02.2013 року) та «Model ping-pong protocol» (№ 48041 від 26.02.2013 року), подано заявку на отримання патенту України на корисну модель «Спосіб підсилення стійкості квантових протоколів прямого безпечного зв'язку» u201512445 від 16.12.2015);

– результати дисертації використовуються у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету (акт від 21.12.2015 року) та кафедри інформаційної безпеки Казахського національного дослідницького технічного університету ім. К.І. Сатпаєва (акт від 07.12.2015 року) для підвищення ефективності підготовки фахівців з інформаційної безпеки (кібербезпеки).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – аналіз некогерентних методів перехоплення інформації та кібератак у системах КК; [2, 4, 5, 10] – метод забезпечення стійкості кутритових протоколів КК до некогерентних атак; [3] – дослідження методу маршрутизації для безпечного передавання інформації; [6, 14-16] – метод оцінювання якості ПВП для визначення статистичних параметрів і закономірностей тритових ПВП; [7, 18] – розрахунок для деяких параметрів пінг-понг протоколу КПБЗ необхідних розмірів матриць для хешування блоків повідомлення; [8, 14, 15, 24] – метод генерування трійкових незбалансованих ПВП; [9, 17, 21, 22] – узагальнена класифікація методів КК, зокрема введення додаткових методів і класифікаційної ознаки; [11, 12] – візуалізація процесів моделювання за допомогою пакетів комп'ютерної алгебри задач Бюффона і регресії для вивчення теорії ймовірності та математичної статистики; постановка задачі і формулювання висновків у співавторстві; [17, 19, 23] – аналіз сучасних систем КК та їх комерційних реалізацій; [21] – дослідження сучасних протоколів квантової теорії ігор.

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях: МНТК «ITSEC: Безпека інформаційних технологій» (Київ, 2012 р.), МНПК «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК)» (Київ, 2011 р., 2012 р., 2013 р.), НТК студентів та молодих учених «Наукоємні технології» (Київ, 2012 р.), Всесвітній конгрес «Авіація у XXI столітті» – «Безпека в авіації та космічні технології» (Київ, 2012 р., 2014 р.), МНПК «Проблеми і перспективи розвитку ІТ-індустрії» (Харків, 2013 р.), МНТК «АВІА» (Київ, 2013 р.), Міжнар. конф. «Computer Science & Engineering (CSE)» (Львів, 2013 р.), НПК

«Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS)» (Миколаїв, 2014 р., 2015 р.), НПК «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Київ, 2015 р.), Всеукр. НПК «Перспективні напрями захисту інформації» (Одеса, 2015 р.), Міжвідомчий міжрегіональний семінар Наукової Ради НАН України «Технічні засоби захисту інформації» (Київ 2012 р., 2013 р., 2015 р.), Міжнар. конф. «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015)» (Варшава, 2015 р.) та ін.

Публікації. Основні положення дисертації опубліковано у 24 наукових працях, у тому числі – 1 колективна монографія, 10 наукових статей (2 – у міжнародних рецензованих виданнях, що входять до бази даних SCOPUS, 6 – у вітчизняних фахових наукових журналах та 2 – у інших наукових виданнях), 1 заявка на отримання патенту України на корисну модель, а також 12 матеріалів і тез доповідей на конференціях.

Структура роботи та її обсяг. Дисертація складається із вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 127 сторінок основного тексту, 39 рисунків, 16 таблиць, 44 сторінки додатків. Список використаних джерел містить 209 найменувань і займає 22 сторінок. Загальний обсяг роботи 193 сторінки.

ОСНОВНА ЧАСТИНА

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і задачі досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведено аналіз наукової літератури за темою дисертаційної роботи. Показано, що КК поєднує у собі цілу низку наукових напрямів, таких як квантова механіка, інформатика, теорія інформації, теорія кодування, квантові обчислення та традиційна криптографія. Проаналізовано передумови які сприяли появі КК, а саме проаналізовано задачі, що не мали традиційного розв'язку у перерахованих галузях (закон Мура, алгоритми Шора і Гровера тощо). Висвітлено основні положення КК та визначено головні постулати квантової механіки, на непорушності яких вони ґрунтуються (постулат вимірювання фізичних характеристик квантових систем, теорема про заборону точного клонування невідомих квантових станів, неможливість розрізнення невідомих квантових станів, квантові кореляції). Встановлено, що серед відомих на сьогодні технологій КК найбільшої популярності набули системи квантового розподілу ключів (КРК), які вже представлені на ринку цілою низкою комерційних систем (Cerberis, Arcis, Centauris, Clavis2 QKD тощо). Крім того, компанією D-Wave Systems представлено квантовий комп'ютер третього покоління D-Wave 2X, ефективність якого значно перевищує ефективність класичних комп'ютерів, що може бути використано як для задач безпеки, так і для злому систем захисту ІКТ. Одне з головних застосувань такого комп'ютера – це моделювання квантовомеханічних систем, занадто складних для моделювання на класичному комп'ютері. Науковцями всього світу проведено багато досліджень ефективності протоколів КК з передаванням кубітів (дворівневих квантових систем), але ефективність протоколів з кудитами (багаторівневими квантовими системами), які мають більшу інформаційну місткість (на один раунд протоколу зв'язку), досліджена на цей час значно менше. Враховуючи питому натурально-логарифмічну щільність запису інформації, випливає, що найбільшу щільність запису інформації має система числення з основою, рівною основі натуральних логарифмів, тобто рівною числу e, а з цілочислених – це трійкова система, у випадку квантових систем – це трирівнева квантова система (кутрит). З огляду на це, основна увага в роботі приділяється саме

кутритовим протоколам КК. Для підвищення їх ефективності у відомих системах використовують квантове надщільне кодування, квантові і неквантові методи підсилення безпеки тощо. Проте ці методи не позбавлені недоліків, з огляду на що, науково-практичною задачею роботи визначено розробку і дослідження нових методів підвищення ефективності кутритових протоколів КК. Таким чином, у першому розділі на основі проведеного аналізу стану проблеми визначено і обґрунтовано основні задачі дослідження, вирішення яких необхідне для досягнення мети, що поставлена в дисертаційній роботі.

Другий розділ присвячений класифікації методів КК та методу забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак. Розширено ***узагальнену класифікацію методів КК*** (рис. 1), яка відрізняється від найбільш повної відомої (Корченка-Василіу-Гнатюка) урахуванням протоколів квантової телепортації та квантової теорії ігор, а також базової ознаки, пов'язаної зі стійкістю протоколів до певного виду кібератак. Проаналізовано атаки, що можуть бути реалізовані в системах КК, а зокрема, в КПБЗ, та встановлено, що найбільш небезпечними і реальними з точки зору практичної реалізації на існуючому обладнанні є *некогерентні атаки* на протоколи КПБЗ: непрозорі – «перехоплення – повторної посилки кубітів (кудитів)» та напівпрозорі – використання порушником (Євою) допоміжних квантових систем (т.з. квантових проб) для переплутування їх з носіями інформації легітимних користувачів (Аліси та Боба).

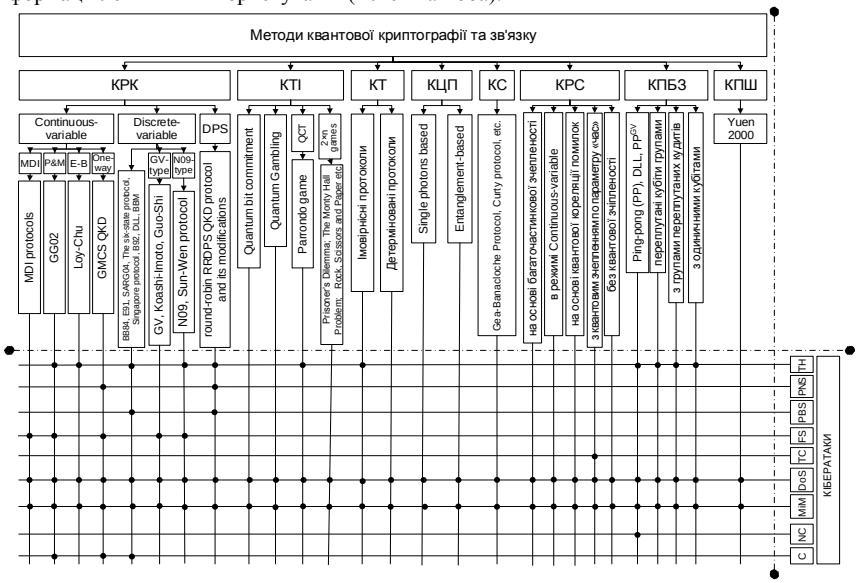

Рис. 1. Розширена класифікація методів квантової криптографії та зв'язку

У протоколах КРК допускається витік частини бітів до порушника під час передавання, а наступна оцінка кількості цих бітів дозволяє виконати процедуру підсилення секретності та звести інформацію порушника про фінальний ключ до нескінченно малої величини (якщо частка бітів, що витекли, не перевищує деякої

порогової величини), таким чином досягаючи теоретико-інформаційної (безумовної) стійкості, яка не залежить від обчислювальних та інших технічних можливостей порушника. Проте, вимоги до стійкості протоколів КПБЗ є значно вищими, ніж до стійкості протоколів КРК, адже в протоколах КПБЗ кожний біт є секретною інформацію і не повинен потрапити до порушника. Отже, хоча протоколи КПБЗ повністю знімають проблему розподілу секретних криптографічних ключів, проте мають лише асимптотичну стійкість до некогерентних атак і, безумовно, потребують методів підсилення безпеки. Оскільки ймовірність виявити цю атаку при одноразовому контролі підслуховування менше одиниці для всіх відомих протоколів КПБЗ, а крім того помилки в режимі контролю підслуховування будуть створюватися не тільки атакою, але і природним шумом в квантовому каналі зв'язку, тому необхідно виконати деяку кількість раундів контролю підслуховування перш, ніж можна буде з упевненістю виявити атаку. Так як режими контролю підслуховування і передачі повідомлення необхідно чергувати випадковим чином, то деяка кількість інформації може бути перехоплена порушником.

Для підвищення швидкості роботи при збереженні стійкості кутритових систем до некогерентних атак запропоновано ***метод забезпечення стійкості кутритових протоколів***, який виконується у такі етапи:

Eman 1. Аліса обробляє секретне повідомлення $A \in V_n$ ($V_n = \{0,1,2\}^n$, $n \in N$) тритовою симетричною функцією перетворення F_{ska}^{enc}: $B = F_{ska}^{enc}(A, K)$, де K – секретний параметр, $K \in V_k$, $k \in N$, $k < n$, F_{ska}^{enc} – симетрична функція перетворення, $F_{ska}^{enc} : V_n \to V_n$, B – перетворене секретне повідомлення, $B \in V_n$.

Eman 2. Аліса обчислює хеш-код повідомлення B: $H = F_{hf}(B)$, де F_{hf} – тритова хеш функція, $F_{hf} : V_n \to V_h$, $h \in N$, $h < n$, H – хеш-код повідомлення B, $H \in V_h$.

Eman 3. Аліса перетворює хеш-код H асиметричною функцією перетворення F_{aka}^{enc} з використанням відкритого секретного параметру Боба: $J = F_{aka}^{enc}(H, K_{op}^{B})$, де K_{op}^{B} – відкритий секретний параметр Боба, $K_{op}^{B} \in V_p$, $p \in N$, F_{aka}^{enc} – асиметрична функція перетворення, $F_{aka}^{enc} : V_h \to V_o$, $o \in N$, J – перетворений хеш-код H, $J \in V_o$.

Eman 4. Аліса формує остаточне повідомлення $C \in V_{n+o}$ для передачі Бобу: $C = (B, J)$, де $B \in V_n$, $J \in V_o$.

Eman 5. Відбувається передача повідомлення C квантовим каналом з використанням протоколів КПБЗ від Аліси до Боба. Навіть якщо Єва перехопить частину повідомлення C залишившись не виявленою, то, не знаючи секретного параметра K, вона не зможе відновити початкове повідомлення A. Слід зауважити, що Аліса і Боб можуть попередньо вибрати таке значення частоти перемикання q між режимами роботи протоколів КПБЗ (із режиму передачі повідомлення в режим контролю підслуховування), при якому ймовірність успішної атаки Єви буде незначною.

Eman 6. Боб отримує повідомлення $C' \in V_{n+o}$ та виділяє з нього частини $B' \in V_n$ та $J' \in V_o$.

Eman 7. Боб обчислює хеш-код повідомлення B': $H' = F_{hs}(B')$, де F_{hf} – тритова хеш-функція, $F_{hf} : V_n \to V_h$, H' – хеш-код повідомлення B', $H' \in V_h$.

Етап 8. Боб виконує зворотне перетворення хеш-коду H'' асиметричним шифром F_{aka}^{dec} з використанням свого закритого секретного параметру: $H'' = F_{aka}^{dec}\left(J', K_{cl}^{B}\right)$, де K_{cl}^{B} – закритий параметр Боба, $K_{cl}^{B} \in V_p$, F_{aka}^{dec} – асиметрична функція зворотного перетворення, $F_{aka}^{dec} : V_o \to V_h$.

Етап 9. Боб порівнює H' і H''. Якщо $H' \neq H''$ – це означає, що повідомлення було модифіковане під час передачі. Одразу припускається, що в сеанс зв'язку втручалась Єва. Тому Боб і Аліса переривають сеанс. Згідно теореми про заборону клонування, порушник не може виготовити точну копію квантових систем, які передаються комунікаційним каналом, щоб провести виміри над копією, а оригінал переслати легітимному користувачу каналу, не проводячи над ним вимірювання. Це змушує порушника вимірювати стан квантових систем, що передаються (або переплутувати їх зі своїми квантовими пробами), що, згідно постулату вимірювання, призводить до зміни їх станів (у такому випадку $B' \neq B$ і $H' \neq H''$). Якщо ж $H' = H''$ – це означає, що втручання Єви не було і $B' = B$.

Етап 10. Боб повідомляє Алісу про те, що при передачі повідомлень втручань не було. Аліса в свою чергу відкритим каналом зв'язку передає Бобу секретний параметр K.

Етап 11. Боб відновлює секретне повідомлення A обробляє тритовою симетричною функцією зворотного перетворення F_{ska}^{dec}: $A = F_{ska}^{dec}\left(B', K\right)$, F_{ska}^{dec} – симетрична функція зворотного перетворення, $F_{ska}^{dec} : V_n \to V_n$.

У якості симетричної функції перетворення та зворотного перетворення можуть бути використані як трійкові блокові, так і потокові перетворення (проте, ці процедури не є шифруванням, так як K передається відкритим каналом для встановлення легітимності користувача, а це не відповідає принципам криптографії). Зауважимо, що при такій побудові роботи протоколів КПБЗ, частоту перемикання q між режимами їх роботи можна зменшити до мінімуму (із рекомендованого значення 0,5 до 0,05), при цьому підвищиться швидкість роботи протоколів і втручання Єви все одно буде детектуватись (на етапах 5 і 9).

Отже, отримав подальший розвиток метод забезпечення стійкості кутритових протоколів квантової криптографії, який, за рахунок неквантової функції перевірки цілісності та використання тритової симетричної функції, дозволяє звести до мінімуму кількість перемикань між режимами роботи протоколу (передавання повідомлення та контролю підслуховування), збільшити швидкість роботи (числовий показник виграшу обчислюється в четвертому розділі роботи) при збереженні стійкості до некогерентних атак.

У **третьому розділі** наведено розробку методів генерування тритових ПВП та оцінювання їх якості (рівня випадковості). Підвищення інформаційної місткості протоколів КК, у нашому випадку, відбувається за рахунок використання багаторівневих квантових систем (кудитів). Враховуючи питому натуральнологарифмічну щільність запису інформації, яка описується функцією $Y(\mathrm{a}) = \dfrac{\ln y(\mathrm{a})}{a} = \dfrac{\ln a}{a}$, де a – основа системи числення, випливає що найбільшу щільність запису інформації має система числення з основою рівною основі натуральних логарифмів (рис. 2), тобто рівною числу Ейлера ($e \approx 2{,}718281828459045$), а з цілочислених – це трійкова система, у випадку квантових систем – це *трирівнева квантова система (кутрит).*

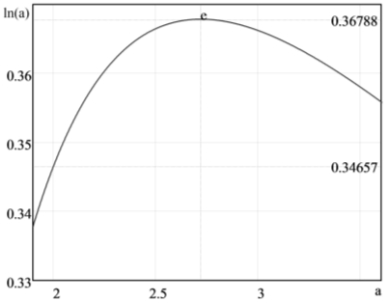

Рис. 2. Питома натуральнологарифмічна щільність запису інформації

З огляду на це, у роботі отримав подальший розвиток ***метод генерування псевдовипадкових послідовностей***, який дозволяє формувати трійкові незбалансовані ПВП. Цей метод ξ має множину векторів внутрішніх станів V_p ($V_p = \{0, 1, 2\}^p$), множину секретних ключів V_n, множину векторів ініціалізації V_e та множину вихідних послідовностей V_m, де $p = 14 \cdot l$, $n = 4 \cdot l$, $e = p - n = 10 \cdot l$, $m = b \cdot n$, $l = d \cdot s$ і b, d, s – натуральні числа.

Для генерації вихідної тритової послідовності виконуються такі етапи:

Eman 1. Виконується початкова ініціалізація вектора внутрішнього стану U на основі вектора ініціалізації VI та секретного ключа K, $U \in V_p$, $VI \in V_e$, $K \in V_n$.

Нехай $U = (x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, k_1, k_2, k_3, k_4)$, де x_i, y_j, k_j – частини вектора внутрішнього стану U ($x_i \in V_l$, $y_j \in V_l$, $k_j \in V_l$, $i \in \overline{1,6}$, $j \in \overline{1,4}$); $VI = (VI_1, VI_2, VI_3, VI_4, VI_5, VI_6, VI_7, VI_8, VI_9, VI_{10})$, де VI_o – частини вектора ініціалізації VI ($VI_o \in V_l$, $o \in \overline{1,10}$); $K = (K_1, K_2, K_3, K_4)$, де K_w – частини секретного ключа K ($K_w \in V_l$, $w \in \overline{1,4}$). Тоді внутрішній стан вектора U ініціалізується таким чином:

$$x_i = VI_i,\ y_j = VI_{6+j},\ k_j = K_j,\ i \in \overline{1,6},\ j \in \overline{1,4}.$$

Eman 2. На основі поточних значень внутрішнього стану вектора U виконується поступова генерація вихідної послідовності $M = (M_1,...,M_b)$, $M \in V_m$, M_q – частини вихідної послідовності M, $M_q \in V_n$, $q \in \overline{1,b}$. Зауважимо, що при генерації кожного M_q поточні значення внутрішнього стану вектору U весь час змінюються.

2.1. Для генерації частини вихідної послідовності M_q r-разів ($q \in \overline{1,b}$, $r \in N$) виконуються наступні дії:

2.1.1. *Розраховуються нові значення векторів* x_1, x_2, x_3. Спочатку визначається x_1: $x_1' = Sbox(x_1 + k_1)$; $x_1 = (x_1' \oplus x_4) <<< k_4$. Далі обраховується x_2: $x_2' = Sbox(x_2 + k_2)$; $x_2 = (x_2' + x_5) >>> k_3$. Наприкінці розраховується x_3: $x_3' = (x_3 + x_6) \oplus y_3$; $x_3 = Mix(x_3') <<< x_1$.

2.1.2. *Обчислюються нові значення векторів* k_1, k_2, y_1, y_2. Спочатку визначаються k_1 та k_2: $k_1' = Sbox(x_1 \oplus k_1) + x_5$; $k_1 = Sbox(k_1' \oplus y_1)$; $k_2' = Mix(x_2 + k_2 + x_6)$; $k_2 = Sbox(k_2' \oplus y_2)$. Далі обраховуються значення y_1 та y_2: $y_1' = (k_1 + y_1) <<< x_2$; $y_1 = Sbox(y_1' \oplus k_3)$; $y_2' = ((k_2 + y_2) >>> x_3) \oplus k_4$; $y_2 = Mix(Sbox(y_2'))$.

2.1.3. *Розраховуються нові значення векторів* x_4, x_5, x_6. Спочатку визначається x_4: $x'_4 = Sbox(x_4 + k_3)$; $x_4 = (x'_4 \oplus x_1) <<< k_2$. Далі обраховується x_5: $x'_5 = Sbox(x_5 + k_4)$; $x_5 = (x'_5 + x_2) >>> k_1$. Наприкінці розраховується x_6: $x'_6 = (x_6 + x_3) \oplus y_1$; $x_6 = Mix(x'_6) <<< x_4$.

2.1.4. *Обчислюються нові значення векторів* k_3, k_4, y_3, y_4. Спочатку визначаються k_3 та k_4: $k'_3 = Sbox(x_4 \oplus k_3) + x_2$; $k_3 = Sbox(k'_3 \oplus y_3)$; $k'_4 = Mix(x_5 + k_4 + x_3)$; $k_4 = Sbox(k'_4 \oplus y_4)$. Далі обраховуються значення y_3 та y_4: $y'_3 = (k_3 + y_3) <<< x_5$; $y_3 = Sbox(y'_3 \oplus k_1)$; $y'_4 = ((k_4 + y_4) >>> x_6) \oplus k_2$; $y_4 = Mix(Sbox(y'_4))$.

2.2. За допомогою конкатенації векторів y_i обраховується вихідна послідовність M_q: $M_q = (y_1, y_2, y_3, y_4)$.

У зазначених вище формулах, символи $\oplus$ та $+$ відповідають операціям покоординатного додавання за модулем 3 та алгебраїчну операцію додавання за модулем 3^l відповідно. Під операцією $X <<< Y$ розуміємо операцію циклічного зсув вліво числа X на Y разів, а під $X >>> Y$ − циклічного зсуву вправо числа X на Y разів. Під операцією $Sbox(X)$ розуміємо операцію в якій X розбивається на d частин довжиною s тритів, над кожною з яких виконується підстановка на множині V_s: $Sbox(X) = (S(X_1),...,S(X_d))$, де $X = (X_1, ..., X_d)$, $X \in V_l$, $X_i \in V_s$, $i \in \overline{1,d}$, а S − підстановки на зазначеній множині. $Mix(X)$ відповідає операції у якій виконується лінійне розсіювання тритів вектора X.

На основі метода генерування тритових ПВП ξ розроблено *алгоритм TriGen* (псевдокод алгоритму див. рис. 3). У алгоритмі TriGen використовуються такі параметри: $d = 4$, $s = 6$, $l = d \cdot s = 24$, $p = 14 \cdot l = 336$, $n = 4 \cdot l = 96$, $e = p - n = 10 \cdot l = 240$, $m = b \cdot n = 96 \cdot b$, $r = 4$, $b \in N$. У операції $Sbox(X)$ використовується одна таблиця підстановок, що побудована за допомогою обрахунку зворотного елементу поля $(X)^{-1} \in GF(3^6)$ з подальшим виконанням афінного перетворення над полем $GF(3)$: $S(X) = M \cdot (X)^{-1} + V$, де $X, V \in GF(3^6)$. Кінцеве поле $GF(3^6)$ фіксувалось кільцем многочленів з операціями за модулем незвідного многочлена $m(x) = x^6 + x + 2$. Для побудови таблиці замін були обрані такі значення матриці M та вектора V:

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 & 2 & 1 \\ 1 & 0 & 1 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 & 1 \\ 1 & 0 & 2 & 1 & 0 & 1 \\ 1 & 1 & 0 & 2 & 1 & 0 \end{pmatrix}, V = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 2 \\ 0 \\ 2 \end{pmatrix}.$$

В операції $Mix(X)$ квадратна невироджена матриця M' над полем $GF(3)$ розміром 24×24 тритів множиться на X (представлений у вигляді вектора-стовпчика) над полем $GF(3)$. Матриця M' побудована на основі масиву U таким чином: $M'[i][j]=U\left[(j+24-i)\bmod 24\right]$, де $i,j=\overline{0,...,23}$, а масив U приймає значення: U = { 1, 0, 1, 2, 1, 0, 2, 0, 2, 1, 0, 2, 0, 1, 2, 2, 0, 1, 0, 1, 1, 2, 0, 2 }.

TriGen

Input: вектор ініціалізації VI, секретний ключ K, $VI\in V_{240}$, $K\in V_{96}$, параметр b.

Output: вихідна послідовність $M=(M_1,...,M_b)$, $M\in V_{96b}$, $M_q\in V_{96}$, $q\in\overline{1,b}$.

1. $x_i=VI_i$, $y_j=VI_{6+j}$, $k_j=K_j$, $i\in\overline{1,6}$, $j\in\overline{1,4}$.

2. *For* $q=1;\ q\le b;\ q{+}{+}$ *do*

2.1. *For* $j=0;\ j<4;\ j{+}{+}$ *do*

2.1.1. $x_1=\left(Sbox(x_1+k_1)\oplus x_4\right)<<<k_4$; $x_2=\left(Sbox(x_2+k_2)+x_5\right)>>>k_3$;

$x_3=Mix\left(\left(x_3+x_6\right)\oplus y_3\right)<<<x_1$;

2.1.2. $k_1=Sbox\left(\left(Sbox(x_1\oplus k_1)+x_5\right)\oplus y_1\right)$; $k_2=Sbox\left(Mix(x_2+k_2+x_6)\oplus y_2\right)$;

2.1.3. $y_1=Sbox\left(\left((k_1+y_1)<<<x_2\right)\oplus k_3\right)$; $y_2=Mix\left(Sbox\left(\left((k_2+y_2)>>>x_3\right)\oplus k_4\right)\right)$;

2.1.4. $x_4=\left(Sbox(x_4+k_3)\oplus x_1\right)<<<k_2$; $x_5=\left(Sbox(x_5+k_4)+x_2\right)>>>k_1$;

$x_6=Mix\left(\left(x_6+x_3\right)\oplus y_1\right)<<<x_4$;

2.1.5. $k_3=Sbox\left(\left(Sbox(x_4\oplus k_3)+x_2\right)\oplus y_3\right)$; $k_4=Sbox\left(Mix(x_5+k_4+x_3)\oplus y_4\right)$;

2.1.6 $y_3=Sbox\left(\left((k_3+y_3)<<<x_5\right)\oplus k_1\right)$; $y_4=Mix\left(Sbox\left(\left((k_4+y_4)>>>x_6\right)\oplus k_2\right)\right)$.

2.2. $M_q=(y_1\,|\,y_2\,|\,y_3\,|\,y_4)$

Рис. 3. Псевдокод алгоритму TriGen

Статистичні властивості згенерованих ПВП не мають відрізнятись від випадкових послідовностей (для криптографічних застосувань), для їх визначення використовують низку методик статистичного тестування, такі як методика графічних тестів, методика NIST STS, методика FIPS 140-2, методика Д. Кнута, система DIEHARD Дж. Марсалья, система CRYPT-S Х. Густавсона, методика статистичного тестування Горбенка-Потія. Однак, всі вони орієнтовані на оцінювання бінарних ПВП.

Запропонований ***метод оцінювання якості ПВП,*** що дає можливість оцінювати статистичні параметри і закономірності тритових ПВП, реалізується в такі етапи:

Eman 1. Перевірка частотним тритовим тестом (Freqeuncy Monotrit Test, FMT).

Eman 2. Дослідження частотним блоковим тестом (Frequency Trit Block Test, FTBT).

Eman 3. Перевірка тритовим тестом серій (Trit Runs Test, TRT).

Eman 4. Дослідження тритовим тестом найдовших серій (Trit Test for the Longest Run in a Block, TTLROB).

Eman 5. Перевірка тритовим тестом на співпадіння з шаблоном без перекриття (Non-overlapping Template Matching Trit Test, NTMTT).

Етап 6. Дослідження тритовим тестом шаблонів із перекриттям (Trit Overlapping Template Matching Test, TOTMT).

На кожному з шести зазначених етапів послідовність перевіряється таким чином:

Спочатку кожна вхідна трійкова послідовність $A_{012} = \{0, 1, 2\}^{n_{012}}$ розбивається на 3 підпослідовності: $A_{01} = \{0, 1\}^{n_{01}}$ (послідовність A_{012} із видаленими 2), $A_{02} = \{0, 2\}^{n_{02}}$ (послідовність A_{012} із видаленими 1), $A_{12} = \{1, 2\}^{n_{12}}$ (послідовність A_{012} із видаленими 0).

Кожна із отриманих послідовностей окремо перевіряється тритовими тестами, подібно до методики NIST. У результаті перевірки кожним тестом отримуємо 3 значення $P-value$: $P-value_{01}$, $P-value_{02}$, $P-value_{12}$. Як і в тестах NIST STS $P-value_{XY}$ (під XY тут і надалі розуміємо одну із трьох можливих комбінацій послідовностей: «01», «02» та «12») відповідатиме ймовірності того, що досліджувана послідовність A_{XY} не гірша, ніж істино-випадкова, тобто якщо $P-value_{XY} = 1$, то згенерована послідовність є ідеально випадковою, а якщо $P-value_{XY} = 0$, то послідовність є повністю передбачуваною.

Визначені значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ кожного тесту порівнюється із α (помилкою першого роду – ймовірність того, що випадкова послідовність є забракованою). Якщо $P-value_{XY} \geq \alpha$, то послідовність A_{XY} є випадковою з рівнем довіри 99%, у іншому випадку $P-value_{XY} \leq \alpha$ – послідовність A_{XY} відбраковується з рівнем довіри 99%. Будемо вважати кожен тест пройденим послідовністю A_{012}, якщо усі отримані значення $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ будуть випадковими з рівнем довіри 99%, тобто виконуватимуться нерівності $P-value_{01} \geq \alpha$, $P-value_{02} \geq \alpha$ та $P-value_{12} \geq \alpha$.

Якщо досліджувана тритова послідовність пройде усі визначені тести, то вважатимемо її ПВП. До того ж, у випадку не проходження хоча б одного із етапів, перевірка завершується і послідовність вважається передбачуваною та непридатною для криптографічних застосувань. У роботі детально описано кожен із зазначених етапів реалізації методу.

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням розроблених рішень. Розроблено методику проведення експериментального дослідження, обгрунтовано доцільність вибору бази експерименту, визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, достатність експериментальних об'єктів та послідовність необхідних дій.

Для дослідження, запропонованого у другому розділі методу забезпечення стійкості протоколів КПБЗ, було виконане порівняння його швидкодії з відомим методом забезпечення стійкості.

Нехай потрібно передавати протоколом КПБЗ повідомлення $A \in V_n$ ($V_n = \{0,1,2\}^n$, $n = r \cdot l$, $r \in N$ – розмір блоку даних, а $l \in N$ – кількість таких блоків). Для порівняння швидкодії передачі повідомлення A протоколом КПБЗ (з частотою перемикання в режим підслуховування q) був оцінений час виконання кожного конкретного етапу. Для цього було введено такі позначення: V_{gen} – швидкість

генерування тритових послідовностей; V_{kv} та V_{kl} − швидкості передачі тритових послідовностей квантовим та класичним каналом відповідно; V_x − швидкість виконання арифметичних операцій в полі $GF(3)$, в табл. 1 наведено основні етапи протоколу КПБЗ для різних методів забезпечення стійкості та час їх виконання.

Оцінка часу виконання етапів протоколу КПБЗ *Таблиця 1*

№ Ет.	*Відомий метод*		*Запропонований метод*	
	Операція	Час виконання, *c*	Операція	Час виконання, *c*
1	$M_i = F_{gen}\left(K, i, r^2\right)$	$\frac{l \cdot r^2}{V_{gen}}$	$k_i = F_{gen}\left(K, i, r\right)$	$\frac{l \cdot r}{V_{gen}}$
2	$B_i = A_i \cdot M_i$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$B_i = A_i + k_i$	$\frac{l \cdot r}{V_x}$
3	$B_i' = F_{kv}\left(B_i, q\right)$	$\left(\frac{l \cdot r}{V_{kv}}\right) \cdot (1+q)$	$H = F_{hf}\left(B\right)$ $J = F_{aka}^{enc}\left(H, K_{op}^{B}\right)$	$\frac{4 \cdot l \cdot r}{V_x}$
4	$M_i' = F_{kl}\left(M_i\right)$	$\frac{l \cdot r^2}{V_{kl}}$	$B_i' = F_{kv}\left(B_i, q\right)$ $J' = F_{kv}\left(J, q\right)$	$\left(\frac{l \cdot r + 96}{V_{kv}}\right) \cdot (1+q)$
5	$\left(M_i'\right)^{-1} = F_{obr}\left(M_i'\right)$	$\frac{l \cdot (4r^3 - 4r^2)}{V_x}$	$H' = F_{hf}\left(B'\right)$ $H'' = F_{aka}^{dec}\left(J', K_{cl}^{B}\right)$	$\frac{4 \cdot l \cdot r}{V_x}$
6	$A_i' = B_i' \cdot \left(M_i'\right)^{-1}$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$K' = F_{kl}\left(K\right)$	$\frac{96}{V_{kl}}$
7	–	0	$k_i' = F_{gen}\left(K', i, r\right)$	$\frac{l \cdot r}{V_{gen}}$
8	–	0	$A_i' = B_i' - k_i'$	$\frac{l \cdot r}{V_x}$

Швидкість передачі повідомлення A за протоколом КПБЗ $V = \frac{r \cdot l}{t}$ (трит/с), де t − загальний час роботи протоколу КПБЗ, $t = \sum_{i=1}^{8} t_i$, t_i − час виконання i-го етапу, $i = \overline{1,8}$.

Для оцінки швидкодії протоколу КПБЗ для різних методів забезпечення стійкості було розроблено консольне ПЗ, що дозволяє розрахувати швидкість протоколу при різних параметрах r, l, q, V_{gen}, V_{kv}, V_{kl} та V_x. На рис. 4 наведено швидкість протоколу КПБЗ при таких параметрах $V_x = V_{kl} = 10^6$ трит/сек, $V_{gen} = 10^4$ трит/сек, $V_{kv} = 10^3$ трит/сек, $l = 1000$, $q = 0{,}5$ − для відомого методу забезпечення стійкості протоколів КПБЗ, а $q = 0{,}05$ для запропонованого методу.

Відповідно до результатів розрахунків, швидкість протоколу КПБЗ із запропонованим методом забезпечення стійкості мінімум у 1,52 раз більша за швидкість відомого методу.

Проте зауважимо, що така кількість разів отримана для $r = 4$, хоча для ефективного використання існуючого методу рекомендований розмір $r \geq 20$, у такому випадку швидкодія запропонованого методу краща у 4,4 рази.

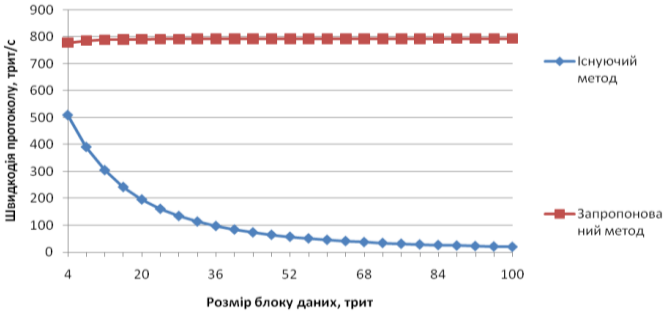

Рис. 4. Порівняння швидкісних характеристик розробленого методу з відомим

Для оцінки методу генерації тритових послідовностей було розроблене консольне ПЗ TritSTS (на основі методу оцінювання якості ПВП). Було проаналізовано тритові послідовності згенеровані запропонованим алгоритмом TriGen та генератором C++. На рис. 5 зображено один із статистичних портретів згенерованих генератором TriGen.

Рис. 5. Статистичний портрет генератора TriGen отриманий у ПЗ TritSTS

У табл. 2 наведено усереднені результати проходження тестів TritSTS досліджуваних алгоритмів.

Усереднені результати перевірки ПВП *Таблиця 2*

Генер.	$P_{value_{01}} \geq 0,01$	$P_{value_{02}} \geq 0,01$	$P_{value_{12}} \geq 0,01$	Кількість тестів у яких тестування пройшло	
				99%	96%
TriGen	152,2 (99,47%)	152,4 (99,60%)	152,4 (99,60%)	123,4 (80,60%)	152,8 (99,86%)
C++	142,6 (93,20%)	143,4 (93,72%)	141,2 (92,28%)	111,8 (73,07%)	149,4 (97,64%)

Згідно отриманих результатів послідовності згенеровані запропонованим алгоритмом TriGen показали кращі результати ніж ПВП згенеровані стандартним генератором C++.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи і лістинги (фрагменти кодів) розробленого у роботі ПЗ «GenSBOX3», в основі якого алгоритм TriGen, «TritSTS» та «Model of QSDC protocol».

ВИСНОВКИ

Результатом виконаної роботи є розв'язання актуальної науково-практичної задачі розробки і дослідження нових більш ефективних методів забезпечення стійкості тритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів псевдовипадкових послідовностей, оцінювання їх якості та можливості використання для криптографічних застосувань.

У процесі виконання дисертаційної роботи отримані такі вагомі результати:

1. Проведено якісний аналіз сучасних методів та протоколів квантової криптографії, визначено їх переваги і недоліки, стійкість та уразливість до різного роду кібератак (зокрема, до некогерентних атак). На підставі часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії, розроблено розширену класифікацію методів квантової криптографії, яка дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації. Така класифікація також дала можливість чітко визначити завдання дисертаційного дослідження щодо подальшої розробки методів забезпечення стійкості тритових протоколів і систем, побудови тритових генераторів псевдовипадкових послідовностей та оцінювання їх якості.

2. Розроблено метод забезпечення стійкості тритових протоколів квантової криптографії, що не потребує великих часових та ресурсних затрат і, за рахунок неквантової функції перевірки цілісності та використання тритової симетричної функції, дозволяє підвищити швидкість роботи протоколу в 4,4 рази при збереженні стійкості до некогерентних атак.

3. Розроблено метод генерування псевдовипадкових послідовностей, який, за рахунок виконання нової послідовності операцій (підстановок $Sbox(X)$, лінійного розсіювання $Mix(X)$, динамічного циклічного зсуву і додавання за модулем 3 $\oplus$ та 3^l +) над вектором внутрішніх станів V_p ($V_p = \{0,1,2\}^p$, $p = 14 \cdot l$) за $r \cdot b$ циклів, дозволяє формувати трійкові незбалансовані («0», «1», «2») псевдовипадкові послідовності $V_{m \cdot b}$, $m = 4 \cdot l$, що можуть використовуватись для реалізації запропонованого метода забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, а також для інших криптографічних застосувань в сучасних інформаційно-комунікаційних технологіях;

4. Розроблено метод оцінювання якості псевдовипадкових послідовностей, який, за рахунок комплексної інтерпретації згенерованих чисел, введення диференційованих ймовірностей $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ і введення трійкових коефіцієнтів для функції помилок *erfc* та неповної гамма функції *igamc,* дає принципову можливість оцінювати загальноприйняті статистичні параметри та закономірності (FMT, FTBT, TRT, TTLROB, NTMTT та TOTMT) для тритових псевдовипадкових послідовностей і, відповідно, оцінювати криптостійкість тритових генераторів псевдовипадкових послідовностей та доцільність їх використання для криптографічних застосувань.

5. Розроблено спеціалізоване програмне забезпечення, за допомогою якого проведено експерименти, що дозволило верифікувати запропоновані методи з точки зору підвищення ефективності протоколів квантової криптографії і реалізації деяких процедур забезпечення безпеки в традиційних (неквантових) криптографічних системах захисту інформації. Розроблені програмні продукти захищені вітчизняними свідоцтвами про реєстрацію авторського права на твір.

6. Зазначені результати роботи впроваджено у діяльність ТОВ «Сайфер ЛТД» (акт впровадження від 28.10.2015 року) та Bilfinger HSG (Німеччина) (акт впровадження від 03.09.2015 року), Національного авіаційного університету (акт від 21.12.2015 року) та Казахського національного дослідницького технічного університету ім. К.І. Сатпаєва (акт від 07.12.2015 року), що підтверджено відповідними актами впровадження, які містяться у додатках до дисертаційної роботи.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Методы перехвата информации в информационно-коммуникационных системах на основе квантових технологий / А.Г. Корченко, Е.В. Василиу, Т.А. Жмурко, С.А. Гнатюк // Информационные технологии и системы в управлении, образовании, науке: Монография [под. ред. В.С. Пономаренко]. – Харків: Цифрова друкарня № 1, 2013. – С. 98-110.

2. Gnatyuk S. Efficiency Increasing Method for Quantum Secure Direct Communication Protocols / S. Gnatyuk, T. Zhmurko, P. Falat // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – P. 468-472.

3. Odarchenko R. Improved Method of Routing in UAV Network / R. Odarchenko, O. Tkalich, S. Gnatyuk, T. Zhmurko // Proceedings of the 2015 IEEE 3rd International Conference on Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), Kyiv, Ukraine, October 13-15, 2015. – P. 145-150.

4. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів / В.М. Кінзерявий, Є.В. Васіліу, Т.О. Жмурко, С.О. Гнатюк // Захист інформації. – 2012. – №2 (55). – С. 79-87.

5. Zhmurko T.O. Efficiency Increasing of the Quantum Cryptography Systems Based on the Ping-Pong Protocol / T.O. Zhmurko, V.M. Kinzeryavyy, S.O. Gnatyuk // Сучасний захист інформації. – 2012. – №3. – С. 5-11.

6. Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань / С.О. Гнатюк, Т.О. Жмурко, В.М. Кінзерявий, Н.А. Сєйлова // Information Technology and Security. – 2015. – Vol. 3. – № 2(5). – С. 108-116.

7. Security Amplification of the Ping-Pong Protocol with Many-Qubit Greenberger-Horne-Zeilinger States / Ye.V. Vasiliu, S.O. Gnatyuk, S.V. Nikolaenko, T.O. Zhmurko // Безпека інформації. – 2012. – Т. 18. – №2. – С. 84-88.

8. Метод генерування тритових псевдовипадкових послідовностей для систем квантової криптографії / С.О. Гнатюк, Т.О. Жмурко, В.М. Кінзерявий, Н.А. Сєйлова // Безпека інформації. – 2015. – № 2. – Т. 22. – С. 140-147.

9. Узагальнена класифікація сучасних методів квантової криптографії та зв'язку / Т.О. Жмурко, В.М. Кінзерявий, Х.І. Юбузова, А.С. Стояновіч // Безпека інформації. – 2015. – № 3. – Т. 22. – С. 287-293.

10. Спосіб підсилення безпеки протоколів квантового прямого безпечного зв'язку // Заявка на отримання патенту України на корисну модель, № u201512445 від 16.12.2015.

11. Жмурко О.І. Моделі до освоєння регресії / О.І. Жмурко, Т.О. Жмурко // Актуальні проблеми математики, фізики і технологічної освіти. Зб. наук. пр.– Вінниця: ФОП Данилюк В.Г., 2012. – Вип. 9 – С. 58-62.

12. Жмурко О.І. Моделювання задачі Бюффона – ефективний шлях до розуміння випадкових величин / О.І. Жмурко, Т.О. Жмурко // Актуальні проблеми математики, фізики і технологічної освіти. Зб. наук. пр. – Вінниця: ФОП Данилюк В.Г., 2012. – Вип. 9 – С. 62-67.

13. Жмурко Т.О. Оцінка рівня випадковості трійкових послідовностей / Т.О. Жмурко // Наукоємні технології: наук.-техн. конф. студ. та мол. учених, 14-18 листопада 2011 р. : тези доп. – К., 2012. – С. 15.

14. Гнатюк С.О. Метод генерування та оцінки випадкових послідовностей для кутритових систем квантового прямого безпечного зв'язку / С.О. Гнатюк, Т.О. Жмурко // Безпека інформаційних технологій (ITSEC-2012) : II міжнар. наук.-техн. конф., 24-25 квітня 2012 р. : тези доп. – К., 2012. – С. 16-17.

15. Гнатюк С.О. Генерування та оцінка випадкових послідовностей для підвищення ефективності кутритових квантових криптосистем / С.О. Гнатюк, Т.О. Жмурко // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2012) : V міжнар. наук.-практ. конф., 15-16 травня 2012 р. : тези доп. – К., 2012. – С. 305-307.

16. Zhmurko T.O. Assessment of Randomness for Ternary Sequences in Quantum Cryptography / T.O. Zhmurko, S.O. Gnatyuk // Aviation in the XXI-st century. Safety in Aviation and Space Technologies: V World Congress, September 25-27, 2012. – Kyiv, 2012. – P. 1.7.50-1.7.53.

17. Zhmurko T.O. Modern Quantum Key Distribution Protocols / T.O. Zhmurko, S.O. Gnatyuk // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2013) : VI міжнар. наук.-практ. конф., 27-29 травня 2013 р. : тези доп. – К., 2013. – С. 289-291.

18. Kinzeryavyy V.M. Improvement of Ping-Pong Protocol with Many-Qubit GHZ-States / V.M. Kinzeryavyy, T.O. Zhmurko, S.O. Gnatyuk // ABIA-2013 : XI міжнар. наук.-техн. конф., 21-23 травня 2013 р. : тези доп. – К., 2013. – С. 2.22-2.26.

19. Gnatyuk S.O. Contemporary Commercial Quantum Information Security Systems / S.O. Gnatyuk, T.O. Zhmurko, M.O. Riabyi // Computer Science & Engineering: 6th Int. Conf. of Young Scientists CSE-2013, November 21-23. – Lviv, 2013. – P. 74-77.

20. Жмурко Т.О. Протоколи квантової теорії ігор / Т.О. Жмурко // Політ. Сучасні проблеми науки: тези доп. XIV міжнар. наук.-практ. конф. молодих учених і студентів, м. Київ, 2-3 квітня 2014 р., НАУ / редкол.: М.С. Кулик [та ін.]. – С. 6.

21. Гнатюк С.А. Квантовые протоколы защиты информации в информационно-коммуникационных системах / С.А. Гнатюк, Т.А. Жмурко, М.А. Рябый // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2014): 6 всеукр. наук.-практ. конф., 09-12 вересня 2014 р. – Миколаїв – Коблево, 2014 – С. 59-62.

22. Zhmurko T.O. Quantum Game Theory in Classification of Quantum Information Security Methods / T.O. Zhmurko, S.O. Gnatyuk // Aviation in the XXI-st century. Safety in Aviation and Space Technologies: VI World Congress, September 23-25, 2014. – Kyiv, 2014. – V. 1 – P. 1.11.36-1.11.39.

23. Zhmurko T.O. Practical Aspects of Quantum Cryptography Using in Real Information & Communication Systems / T.O. Zhmurko, S.O. Gnatyuk // Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: наук.-практ. конф., 25-28 лютого 2015 р. : тези доп. – К., 2015. – С. 34-36.

24. Метод формування трійкових псевдовипадкових послідовностей / С.О. Гнатюк, Т.О. Жмурко, В.М. Кінзерявий, Р.С. Одарченко // Перспективні напрями захисту інформації: матеріали першої всеукр. наук.-пр. конф., 7-9 вересня 2015 р. – Одеса: ОНАЗ, 2015. – С. 11-15.

АНОТАЦІЯ

Жмурко Т.О. Методи підвищення ефективності протоколів квантової криптографії. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Національний авіаційний університет, Київ, 2016.

Дисертаційна робота присвячена розв'язанню актуальної науково-практичної задачі розробки і дослідження нових більш ефективних методів забезпечення стійкості тритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів псевдовипадкових послідовностей та оцінювання їх якості (можливості використання для криптографічних застосувань). Отримані в дисертаційній роботі результати можуть бути використані для підвищення ефективності (захищеності, швидкості роботи) систем захисту на базі КПБЗ і квантового розподілу ключів, а також для деяких процедур безпеки в традиційних (неквантових) криптографічних системах захисту інформації. У роботі розроблено класифікацію методів КК, яка, за рахунок розширення множини відомих базових ознак і часткових узагальнень теоретичних положень та практичних досягнень у галузі КК, дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації (на базі КПБЗ та інших квантових технологій). Отримав подальший розвиток метод забезпечення стійкості кутритових протоколів квантової криптографії, який, за рахунок неквантової функції перевірки цілісності та використання тритової симетричної функції, дозволяє звести до мінімуму кількість перемикань між режимами протоколу (передавання повідомлення та контролю підслуховування), збільшити швидкість роботи при збереженні стійкості до некогерентних атак. Отримав подальший розвиток метод генерування псевдовипадкових послідовностей, який, за рахунок виконання нової послідовності операцій (підстановок, лінійного розсіювання, динамічного циклічного зсуву та додавання за модулем 3 та 3^l) над вектором внутрішніх станів, дозволяє формувати трійкові незбалансовані псевдовипадкові послідовності. Окрім того, отримав подальший розвиток метод оцінювання якості псевдовипадкових послідовностей, який, за рахунок комплексної інтерпретації згенерованих чисел, введення диференційованих ймовірностей $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ і трійкових коефіцієнтів для функції помилок *erfc* та неповної гамма функції *igamc*, дає можливість оцінювати статистичні параметри і закономірності тритових псевдовипадкових послідовностей.

Ключові слова: квантова криптографія, трит, кутрит, квантовий прямий безпечний зв'язок, псевдовипадкова послідовність, тритовий генератор, оцінка якості генератора псевдовипадкових послідовностей.

АННОТАЦИЯ

Жмурко Т.А. Методы повышения эффективности протоколов квантовой криптографии. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Национальный авиационный университет, Киев, 2016.

Диссертационная работа посвящена решению актуальной научно-практической задачи разработки и исследования новых более эффективных методов обеспечения устойчивости тритовых протоколов квантовой криптографии к некогерентным атакам, построения тритовых генераторов псевдослучайных последовательностей, а также

оценке качества троичных псевдослучайных последовательностей и возможности их использования для криптографических приложений. Полученные в диссертационной работе результаты могут быть использованы для повышения эффективности (защищенности, скорости работы) систем защиты на основе квантовой прямой безопасной связи и квантового распределения ключей, а также для некоторых процедур безопасности в традиционных (не квантовых) криптографических системах защиты информации.

В работе разработана классификация методов квантовой криптографии, которая за счет расширения множества известных базовых признаков (учтена стойкость протоколов к различным кибератакам) и частичных обобщений теоретических положений (учтены протоколы квантовой телепортации и квантовой теории игр, а также в классификацию внесены новые протоколы квантовой прямой безопасной связи и квантового распределения ключей) и практических достижений в области квантовой криптографии (проанализировано существующие коммерческие решения), позволяет расширить возможности выбора соответствующих методов для построения современных квантовых систем защиты информации (на основе квантовой прямой безопасной связи и других квантовых технологий). Классификация дала возможность четко определить задание диссертационного исследования по дальнейшей разработке методов обеспечения устойчивости тритовых протоколов и систем, построения тритовых генераторов псевдослучайных последовательностей и оценки их качества.

Получил дальнейшее развитие метод обеспечения стойкости кутритовых протоколов квантовой криптографии, который, за счет неквантовой функции проверки целостности и использования тритовой симметричной функции (в качестве которой могут быть использованы троичные как блоковые так и потоковые преобразования), позволяет свести к минимуму (с рекомендованного значения 0,5 до 0,05) количество переключений между режимами протокола (передачи сообщения и контроля подслушивания) и увеличить скорость работы протокола в 4,4 раза при сохранении стойкости к некогерентным атакам.

Получил дальнейшее развитие метод генерирования псевдослучайных последовательностей, который, за счет выполнения новой последовательности операций (подстановок, линейного рассеивания, динамического циклического сдвига и сложения по модулю 3 и 3^l) над вектором внутренних состояний V_p ($V_p = \{0,1,2\}^p$, $p = 14 \cdot l$) за $r \cdot b$ циклов, позволяет формировать троичные несбалансированные псевдослучайные последовательности $V_{m \cdot b}$, $m = 4 \cdot l$.

Кроме того, получил дальнейшее метод оценивания качества псевдослучайных последовательностей, который, за счет комплексной интерпретации сгенерированных чисел, введения дифференцированных вероятностей $P-value_{01}$, $P-value_{02}$, $P-value_{12}$ и троичных коэффициентов для функции ошибок *erfc* и неполной гаммы функции *igamc*, дает возможность оценивать статистические параметры и закономерности тритовых псевдослучайных последовательностей. Метод оценивания реализуется такими этапами: Проверка частотным троичным тестом (FMT); исследование частотным блочным тестом (FTBT); проверка тритовым тестом серий (TRT); исследование троичным тестом самых длинных серий (TTLROB); проверка троичным тестом на совпадение с шаблоном без перекрытия (NTMTT); исследование троичным тестом шаблонов с перекрытием (TOTMT).

Разработано специальное программное обеспечение «GenSBOX3», «TritSTS» и «Model of QSDC protocol», с помощью которого проведены эксперименты, что позволило верифицировать предложенные методы с точки зрения повышения эффективности протоколов квантовой криптографии и реализации некоторых процедур обеспечения безопасности в традиционных (неквантових) криптографических системах защиты информации. Все разработанные программные продукты защищены отечественными свидетельствами о регистрации авторского права на произведение.

Ключевые слова: квантовая криптография, трит, кутрит, квантовая прямая безопасная связь, псевдослучайная последовательность, тритовый генератор, оценка качества генератора псевдослучайных последовательностей.

ABSTRACT

Zhmurko T.O. Methods for improving the efficiency of quantum cryptography protocols. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 – information security systems. – National Aviation University, Kyiv, 2016.

Thesis is devoted to applied scientific research task to develop and study new, more efficient methods for ensuring sustainability of quantum cryptography qutrit protocols to non-coherent attacks; constructing trit generator of pseudorandom sequences and evaluation of its quality (possibility of using them in cryptographic applications). The results obtained in the thesis can be used to improve efficiency (security level and speed) of security systems based on quantum direct secure communication and quantum key distribution, and can be used for security procedures in traditional (non-quantum) cryptographic information security systems. In this work developed classification of quantum cryptography methods, which, by extending the set of known basic features, partial theoretical generalizations and study practical achievements in quantum cryptography, can expand opportunities for choosing appropriate methods to construct modern quantum information security systems (based on quantum direct secure communication and other quantum technologies). Was further developed a method for ensuring stability of quantum cryptography qutrit protocols, which, with the use of quantum integrity checking function and trit symmetric function, allows to minimize the amount of switching between protocol modes (message transmission and eavesdropping control), and increase speed by a factor of 4.4, while maintaining the resistance to non-coherent attacks. Also, was further developed a method of generating pseudorandom sequences, which, through the implementation of new operation sequence (substitutions, linear diffusion, dynamic rotate shift, modular 3 and 3^l addition) over internal states vector allows to create ternary unbalanced pseudorandom sequences. In addition, further developed a method for evaluating pseudorandom sequence quality, which, through complex interpretation of generated numbers, by adding differentiated probability $P-value_{01}$, $P-value_{02}$, $P-value_{12}$, ternary coefficients for the error function *erfc* and incomplete gamma function *igamc*, enables to evaluate the statistical parameters and laws of ternary pseudorandom sequences.

Keywords: quantum cryptography, ternary, qutrit, quantum secure direct communication, pseudorandom sequence, ternary generator, quality assessment of pseudorandom sequence generator.