ВІДГУК

офіційного опонента д.т.н., професора Рудницького Володимира Миколайовича на дисертацію Жмурко Тетяни Олександрівни «Методи підвищення ефективності протоколів квантової криптографії», представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність. З огляду на бурхливий розвиток, в останні два десятиріччя, такого напрямку захисту інформації як квантова криптографія, який має цілу низку переваг в порівняні з існуючими методами криптографії, у дисертаційній роботі Жмурко Т.О. поставлена актуальна науково-практична задача розробки та дослідження нових ефективних методів забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів псевдовипадкових послідовностей та оцінювання їх якості (можливості використання для криптографічних застосувань), що має теоретичне і практичне значення.

Актуальність наукового дослідження також підтверджується науково-дослідними роботами, з якими вона пов'язана, а саме 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.

Окрім того, 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»).

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.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Ступінь обґрунтованості нових положень та висновків у дисертації обумовлена коректністю застосування сучасних методів квантової теорії інформації, квантової механіки та імітаційного моделювання (моделювання процесу передавання кутритів, моделювання методів забезпечення стійкості від некогерентних атак, дослідження кібератак на квантові системи), традиційної криптографії (розробка методів забезпечення стійкості та формування трійкових послідовностей), об'єктно-орієнтованого програмування (розробка програмного забезпечення для реалізації запропонованих методів) та математичної статистики (розробка низки статистичних тестів для оцінювання якості трійкових послідовностей).

Ідентичність змісту автореферату й основних положень дисертації

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації. Структура дисертації відповідає вимогам, які ставляться до кандидатських дисертацій. Дисертаційна робота 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. Загальний обсяг роботи 193 сторінки.

Результати дисертації викладено послідовно та структуровано, відповідно до поставлених задач дослідження. Зауважу, що для основних положень дисертації та змісту автореферату характерна повна ідентичність.

Оцінка змісту дисертації

Викладені наукові положення та висновки є повністю обґрунтованими, а достовірність теоретичних положень підтверджується експериментальними даними і результатами верифікації запропонованих методів. Отримані під час експериментів дані відповідають теоретичним висновкам та повністю підтверджують їх.

У вступі автором представлена загальна характеристика роботи, сформульовано мету та задачі дослідження, відображені наукова новизна та практична цінність отриманих результатів, приведено дані щодо апробації та впровадження результатів роботи.

У першому розділі проведено аналіз літературних джерел за темою дисертації (провідних, переважно, закордонних публікацій у фахових виданнях), проаналізовано сучасні методи квантової криптографії, виявлено переваги та недоліки, розглянуто практичні реалізації та сучасний стан

галузі,визначено основні напрями дослідження, чітко сформульовано задачі наукового дослідження.

У другому розділі узагальнено класифікацію методів квантової криптографії, що дало змогу розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації (на основі квантового прямого безпечного зв'язку та інших квантових технологій) та розроблено метод забезпечення стійкості тритових протоколів квантової криптографії, що не потребує великих часових та ресурсних затрат, і дозволяє підвищити швидкість роботи протоколу при збережені стійкості до некогерентних атак.

Третій розділ присвячено розробці методів генерування, в основі якого лежить розроблений алгоритм TriGen та оцінювання якості (що складається з шести етапів) трійкових псевдовипадкових послідовностейTritSTS.Метод генерування дозволяє формувати трійкові незбалансовані псевдовипадкові послідовності, що можуть використовуватись для реалізації метода забезпечення стійкості тритових протоколів квантової криптографії до некогерентних атак, а також для інших криптографічних застосувань в сучасних інформаційно-комунікаційних технологіях. Метод TritSTS дозволяє оцінювати криптостійкість тритових генераторів псевдовипадкових послідовностей та доцільність їх використання для криптографічних застосунків.

У четвертому розділі роботи здобувач проводить верифікацію та дослідження розроблених методів. Розроблено методику проведення експериментального дослідження, в якій визначено мету та основні задачі експерименту, вхідні та вихідні параметри, критерії, а також послідовність дій. Для проведення експерименту, на основі описаних у розділах 2 і 3 методів розроблено консольне програмне забезпечення «TriGen», «TritSTS» та програму «ModelofQKDprotocol», які реалізують всі розроблені автором методи. Результати проведених експериментів підтверджують адекватність, достовірність та точність отриманих здобувачем наукових положень та практичних рішень.

У висновках стисло сформульовано основні наукові та практичні результати роботи.

У додатках наведено акти впровадження результатів дисертації та фрагменти вихідних текстів програм, що відображають практичну частину дисертаційного дослідження.

Новизна отриманих результатів

У дисертаційній роботі Жмурко Т.О. «Методи підвищення ефективності протоколів квантової криптографії» отримано теоретичне узагальнення та новий розв'язок актуальної науково-практичної задачі, яка полягає в розробці і дослідженні нових ефективних методів забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів псевдовипадкових послідовностей та оцінювання їх якості.

Найбільш **суттєві наукові результати** дисертаційної роботи:

1) *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;

2) *отримав подальший розвиток* метод генерування псевдовипадкових послідовностей, який, за рахунок виконання нової послідовності операцій (підстановок, лінійного розсіювання, динамічного циклічного зсуву та додавання за модулем) над вектором внутрішніх станів, дозволяє формувати трійкові незбалансовані псевдовипадкові послідовності;

3) *отримав подальший розвиток* метод оцінювання якості псевдовипадкових послідовностей, який, за рахунок комплексної інтерпретації згенерованих чисел, введення диференційованих ймовірностей і трійкових коефіцієнтів для функції помилок танеповної гамма функції, дає можливість оцінювати статистичні параметри і закономірності тритових псевдовипадкових послідовностей.

Практична значимість одержаних результатів:

– розроблено класифікацію методів квантової криптографії, яка, за рахунок розширення множини відомих базових ознак і часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії, дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації;

– результати дисертаційного дослідження впровадженні у діяльність ТОВ «Сайфер БІС» (28.10.2015 року) та Bilfinger HSG (Німеччина) (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.

Завершеність та стиль викладення

Дисертація Жмурко Тетяни є завершеною кваліфікаційною науковою роботою, виконаною та оформленою відповідно до затверджених вимог. Робота написана зрозуміло та грамотно, науково-технічна і вузькоспеціалізована термінологія (у галузі квантової криптографії) використовується коректно, структура роботи логічна.

Основні результати роботи опубліковано у повній мірі у 24 наукових працях, у тому числі – 1 колективна монографія, 10 наукових статей (з яких 2 статті у міжнародних рецензованих журналах, що входять до бази даних SCOPUS, 6 – у вітчизняних фахових наукових журналах та 2 статті у інших наукових виданнях), 1 заявка на отримання патенту України на корисну модель, а також 12 матеріалів і тез доповідей на конференціях. У дисертаційній роботі та у авторефераті чітко окреслено особистий внесок здобувача до всіх наукових праць написаних у співавторстві.

Структура і зміст автореферату є повністю ідентичним з рукописом дисертаційної роботи.

Зауваження

1. Як відомо, у реальних квантових каналах завжди є завади. З огляду на це, я вважаю, що у запропонованому дисертантом методі забезпечення стійкості кутритових протоколів потрібно було врахувати можливість спотворення повідомлення при передачі. Також, не зовсім зрозумілий висновок, щодо можливості зменшення частоти перемикання в режим контролю підслуховування протоколів. Таким чином, є сумнівним можливість використання цього методу на практиці.
2. В описі третього розділу дисертаційного дослідження, що наведений в авторефераті, наведено опис реалізації методу генерування псевдовипадкових послідовностей, проте не зрозуміло, які параметри використовуються (*p, n, e, n, l, b, d, s* і т.д.) та що вони означають.
3. У запропонованому методі оцінки рівня випадковості тритових послідовностей (с. 69-87 дисертації) пропонується окремо досліджувати випадковість послідовності «0»і «1», «0»і «2» та «1»і «2». Проте, математично не доведено, що такий підхід є достатнім для оцінки якості саме тритових (трійкових) послідовностей.
4. При проведені експериментів щодо оцінки швидкодії методу забезпечення стійкості (с. 92-102 четвертого розділу дисертаційної роботи) не обґрунтовано вибір вхідних параметрів протоколів квантової криптографії.
5. В алгоритмі генерації тритових псевдовипадкових послідовностей TriGen використовується операція множення вектору даних на матрицю розміром 24x24 трити. На мою думку ця операція буде виконуватись занадто повільно, з огляду на що використання цього генератора для практичних застосувань може бути не ефективним.
6. Наявність формалізованих виразів та скорочень у науковій новизні та висновках до дисертації ускладнює їх сприйняття при оцінюванні результатів дисертаційної роботи.

7. Крім того, дисертант не повністю розкрив питання працездатності й ефективності запропонованих методів за умови використання різних квантових протоколів розподілу ключів та прямого безпечного зв'язку.

Висновки

Зазначені недоліки не є суттєвими та критичними і не впливають на загальну позитивну оцінку роботи здобувача. Зміст дисертаційної роботи відповідає паспорту наукової спеціальності 05.13.21 – «Системи захисту інформації».Вважаю, що дисертаційна робота «Методи підвищення ефективності протоколів квантової криптографії» має наукову новизну та практичні значимість у галузі кібербезпеки та повністю відповідає вимогам «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», затвердженого Постановою КМУ від 24 липня 2013 року № 567, а її автор Жмурко Тетяна Олександрівна заслуговує присудження їй наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21– «Системи захисту інформації».

Офіційний опонент
Завідувач кафедри інформаційної безпеки
та комп'ютерної інженерії Черкаського
державного технологічного університету
д.т.н., професор В.М. Рудницький

Підпис д.т.н., професора Рудницького В.М.
завіряю секретар Вченої ради ЧДТУ Н.Ю. Лега