University
of Bielsko-Biala

UNIVERSITY OF BIELSKO-BIALA
DEPARTMENT OF COMPUTER SCIENCE
AND AUTOMATICS
2 Willowa St, Bielsko-Biala, 43-309 Poland
tel. 33 827 92 64

Prof. Dr.Sc. **Mikolaj Karpinski**
Chairman of Department of Computer Science and Automatics

В.о. ученого секретаря спеціалізованої вченої ради
Д 26.062.17 д.т.н., проф. В.П. Кваснікову
Національний авіаційний університет
проспект Космонавта Комарова, 1
м. Київ, 03058, Україна

Wasze pismo z dnia:	Znak:	Nasz znak:	Data:
		K18/ 48 /2016	12.04.2016

ВІДГУК

офіційного опонента д.т.н., професора Карпінського Миколи Петровича
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 теми. Стрімкий розвиток новітніх інформаційних технологій та розповсюдження сучасних комп'ютерних систем та мереж, окрім надання якісних інформаційних послуг, зумовлюють і суттєве збільшення ризиків та можливих загроз інформаційній безпеці, загострюють існуючі протиріччя між необхідністю оброблення та передачі великих обсягів інформації у зазначені терміни та підвищення вимог до їх безпеки. Конфіденційність інформації, як правило, забезпечується методами симетричної та асиметричної криптографії, що не позбавлені певних недоліків. Симетричним методам, зокрема, характерна проблема розподілу секретних ключів, а асиметричні методи є повільними і потребують значних обчислювальних ресурсів. Крім того, стійкість усіх традиційних криптосистем базується на гіпотетичній неможливості розв'язання певного класу математичних задач за поліноміальний час – пошук по повністю невпорядкованій базі даних, факторизація та логарифмування в дискретних полях великого розміру. Проте ця гіпотеза може бути спростована за допомогою багатокубітних квантових комп'ютерів (D-Wave 2X), GRID-технологій, HPC та інших сучасних інформаційно-комунікаційних технологій. З огляду на це, великий інтерес викликає квантова криптографія, що кардинально відрізняється від усіх існуючих на сьогодні методів захисту інформації.

Тому вважаю, що розробка і дослідження нових ефективних методів забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів псевдовипадкових послідовностей (ПВП) та оцінювання їх якості

43-309 Bielsko-Biała, ul. Willowa 2
phone: (33) 8279 264, fax: (33) 8279 264
Regon: 072728961, NIP: 547-19-43-784
mkarpinski@ath.bielsko.pl, www.ath.bielsko.pl

810/05
15.04.2016

(можливості використання для криптографічних застосувань) є *актуальною науково-практичною задачею*, що має теоретичне і практичне значення.

Актуальність дисертаційної роботи також підтверджується тим, що тематика дисертаційної роботи Жмурко Т.О. та одержані автором 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»). Також актуальність роботи підтверджується науково-дослідними роботами, з якими вона пов'язана: 1) НДР НАУ «Організація систем захисту інформації від кібератак» (д.р. № 0111U000171), 2) НДР НАУ «Методи та засоби захисту інформації на основі квантових технологій» (реєстраційний номер № 43/14.02.04), 3) НДР НАУ «Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах» (реєстраційний номер № 61/09.01.08), 4) НДР НАУ «Новітні технології криптографічного захисту інформації» (реєстраційний номер № 100/14.01.06), 5) НДР НАУ «Методи підвищення ефективності систем квантової криптографії» (реєстраційний номер № 26/09.01.08) та НДР 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.

Метою дисертаційної роботи Жмурко Т.О. є підвищення ефективності протоколів квантової криптографії шляхом розробки методів забезпечення стійкості кутритових протоколів і систем, побудови тритових генераторів ПВП та оцінювання їх якості.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій.

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

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета і задачі дослідження, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проаналізовано вітчизняну та зарубіжну літературу за темою дисертаційного дослідження: визначено передумови виникнення такого напряму як квантова криптографія, зазначено теоретичні основи базування принципової відмінності протоколів квантової криптографії від інших існуючих на сьогодні методів захисту інформації, проаналізовано світові тенденції розвитку протоколів квантової криптографії та їх класифікації, зазначено існуючий прогрес переходу від теоретичних положень до практичної реалізації, у вигляді аналізу сучасних комерційних систем квантового розподілу ключів. Показано стан наступного найближчого до практичного застосування напряму квантової криптографії, а саме квантового прямого безпечного зв'язку, який не потребує використання додаткового шифрування інформації, та може використовуватись за вже наявного обсягу квантової пам'яті. На онові проведеного аналізу сформульована

необхідність побудови узагальненої класифікації сучасних квантових технологій захисту інформації з урахуванням базової ознаки стійкості до певного роду кібератак.

У **другому розділі** дисертації наведено аналіз кібератак (визначено їх основну мету, етапи реалізації та найуразливіші протоколи квантової криптографії) на системи квантової криптографії та розроблено класифікацію методів квантової криптографії, яка, завдяки розширенню множини відомих базових ознак і часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії, дає змогу розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації (на базі квантового прямого безпечного зв'язку та інших квантових технологій). Також розроблено метод забезпечення стійкості кутритових протоколів, який містить 11 етапів та дозволяє, за такої побудови роботи протоколів квантового прямого безпечного зв'язку (КПБЗ), зменшити до мінімуму частоту перемикання q між режимами їх роботи (із рекомендованого значення 0,5 до 0,05), підвищуючи при цьому швидкість роботи протоколів та все одно детектуючи втручання Єви (на етапах 5 і 9).

У **третьому розділі** дисертаційної роботи автор пропонує такі методи як: метод генерування тритових ПВП, в основі якого лежить розроблений автором алгоритм TriGen та метод оцінювання якості, що реалізується протягом шести етапів. Шляхом використання автором 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* розроблений метод дає можливість оцінювати статистичні параметри і закономірності тритових ПВП.

У **четвертому розділі** роботи здобувач проводить верифікацію та дослідження розроблених методів. Розроблено методику проведення експериментального дослідження, визначено його мету, задачі та вхідні параметри, а також необхідну послідовність дій. Проведено порівняння швидкості роботи протоколів Василіу-Ніколаєнка та розробленого методу «Model of QSDC protocol» за збереження стійкості до некогерентних атак, показано, що розроблений метод дозволяє підвищити швидкість як мінімум у 4,4 рази. Досліджено консольний застосунок «TriGen», який генерує тритові послідовності, та підтверджено можливість його застосування для криптографічних методів захисту інформації. Також автором у даному розділі обґрунтовано неможливість використання найпопулярнішої методики оцінювання якості ПВП NIST STS для тритових послідовностей, та підтверджено адекватність розробленого методу оцінювання «TritSTS».

У **додатках** наведено документи, що підтверджують впровадження результатів дисертаційної роботи, а також лістинги (коди) розроблених програмних засобів «GenSBOX3», «TriGen», «TritSTS», «Model of QSDC protocol».

Наукова новизна отриманих результатів полягає передусім у тому, що: *отримав подальший розвиток* метод забезпечення стійкості кутритових протоколів квантової криптографії, завдяки якому зведено до мінімуму кількість перемикань між режимами протоколу (передавання повідомлення та контролю підслуховування), збільшено швидкість роботи за умови збереження стійкості до некогерентних атак; *отримав подальший розвиток* метод генерування ПВП, який дозволяє формувати трійкові незбалансовані («0», «1», «2») псевдовипадкові послідовності; *отримав подальший розвиток* метод оцінювання якості ПВП, який дає змогу оцінювати статистичні параметри і закономірності тритових ПВП.

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. Результати дисертаційного дослідження *достатньо апробовані* на науково-технічних конференціях і семінарах різного рівня, зокрема, на Всесвітньому конгресі «Авіація у XXI столітті» – «Безпека в авіації та космічні технології» (Київ, 2012 р., 2014 р.), Міжнар. конф. «Computer Science & Engineering (CSE)» (Львів, 2013 р.), Міжвідомчих міжрегіональних семінарах 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.

Варто також зауважити, що основні положення дисертації та зміст автореферату повністю ідентичні.

Цінність для практики становлять: розроблена класифікація методів КК, яка дозволяє розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації (на базі КПБЗ та інших квантових технологій); результати проведених досліджень з можливістю їх використання в 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); використання результатів дисертаційного дослідження у діяльність ТОВ «Сайфер БІС» (акт від 28.10.2015 року) та Bilfinger HSG (Німеччина) (акт від 03.09.2015 року) дало змогу підвищити захищеність інформації з обмеженим доступом, що підтверджується актами впровадження; розроблена низка 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).

Зауваження:

1. В актуальності дисертаційної роботи здобувач, на мою думку, використовує не зовсім коректне формулювання, яке стосується квантової криптографії (зокрема «інтерес викликає квантова криптографія, яка не залежить від обчислювальних потужностей порушника»). Слід зазначити, що квантова криптографія базується в першу чергу на фізичних методах квантової механіки, і, на відміну від класичної криптографії, використовує принципово інші підходи до забезпечення конфіденційності інформації. Слід зазначити, що обчислювальні потужності необхідні для створення квантового каналу зв'язку, його керування та використання суміжних інформаційних систем, в яких інтегровані квантові системи обробки та захисту інформації. Це підтверджується самою дисертант, яка далі у роботі погоджується з тим, що для генерування оборотних трійкових матриць необхідні великі часові затрати та обчислювальні ресурси.
2. На рисунку 1 автореферату зображені кібератаки, що спрямовані на певні методи квантової криптографії та зв'язку (точніше було б сказати, до яких методи квантової криптографії та зв'язку є уразливими). В авторефераті рисунок наводиться з назвою «Розширена класифікація методів квантової криптографії та зв'язку» і не згадуються атаки (за винятком некогерентних атак), також немає ні тлумачення скорочень показаних атак (варто відзначити, що в дисертаційній роботі таке тлумачення наведено на сторінці 53), ні їх класифікації. Крім цього, на мою думку, не всі зазначені здобувачем атаки відносяться саме до кібератак.
3. На сторінці 60 дисертаційної роботи автор наводить схему реалізації методу забезпечення стійкості квантових протоколів від некогерентних атак (рис. 2.3), проте в тексті роботи відсутнє тлумачення цієї схеми. Для випадку, якщо вона ілюструє 11 етапів зазначеного методу, що описано у роботі раніше – необхідно було б вставити посилання по тексту опису на цей рисунок.
4. У дисертації на сторінці 63 після розрахунку питомої натурально логарифмічної щільності запису інформації дисертант наводить переваги використання трійкової логіки, проте для мене залишається не зрозумілим доцільність цього, так як в жодному з трьох розроблених методів автор не використовує логічних операцій.

5. У пункті 4.1 дисертаційної роботи автор наводить запропоновану методику проведення експерименту, проте вважаю, що потрібно було б розробити як мінімум три окремі методики (для окремої верифікації трьох запропонованих методів) – це значно спростило б розуміння процесу експериментального дослідження та аналізу отриманих результатів.

6. З автореферату та дисертації (розділ 4) не зовсім зрозуміло, чому порівнюються послідовності, згенеровані за допомогою розробленого здобувачем генератора TriGen, з послідовностями, що згенеровані за допомогою стандартного генератора C++. Чому, для прикладу, не порівнювались з послідовностями, отримані шаблонним генератором BBS, як то є в методиці NIST STS?

7. Тексти дисертаційної роботи та автореферату містять надзвичайно велику кількість скорочень, абревіатур та формул, що значно ускладнює загальний процес оцінювання й розуміння роботи при читанні.

Висновки:

Принагідно висловлені зауваження не занижують вартості дисертаційного дослідження та не впливають на його позитивну оцінку. Оцінюючи опоновану дисертаційну роботу загалом, вважаю, що вона є закінченою кваліфікаційною роботою, у ній розв'язана важлива науково-практична задача підвищення ефективності протоколів квантової криптографії, спрямована саме на розроблення та дослідження нових ефективних методів забезпечення стійкості кутритових протоколів квантової криптографії до некогерентних атак, побудови тритових генераторів ПВП та оцінювання їх якості. Вважаю, що представлена дисертаційна робота «Методи підвищення ефективності протоколів квантової криптографії» відповідає усім 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 наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – «Системи захисту інформації».

ОФІЦІЙНИЙ ОПОНЕНТ

Керівник кафедри інформатики та автоматизації
Університету у Бєльсько-Бялій (Республіка Польща)
доктор технічних наук, професор

CHAIRMAN
of Department of Computer Science
and Automatics
Prof. D.Sc. Mikołaj Karpiński

Микола Карпінський