Голові спеціалізованої
вченої ради Д41.816.02
65029, м. Одеса, вул. Кузнечна, 1

ВІДГУК

на автореферат дисертації Лімаря Ігоря Валерійовича на тему
«Криптографічний захист системи електронного голосування з використанням протоколів квантової криптографії», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми. Нині, в економічно розвинених країнах широко впроваджуються системи електронного голосування. У зв'язку з безперервно зростаючим обсягом інформації, що циркулює в таких системах, різко зростають вимоги, що пред'являються, по-перше, як до швидкості обміну даними, так, і по-друге, до простоти апаратно-програмної реалізації систем, які здійснюють прийом-передачу повідомлень, і, нарешті, до надійності захисту таких систем від несанкціонованого доступу до конфіденційної інформації.

Одним із способів вирішення проблеми захисту інформації, що циркулює в системах електронного голосування є використання криптографічних методів та засобів захисту. З цією метою в багатьох схемах криптозахисту використовується останнім часом примітив бітового зобов'язання. На сьогодні, вказаний примітив входить у склад такої відомої системи криптографічного захисту електронних виборів як Punchscan та її криптографічної надбудови Scantegrity II. Разом з тим останнім часом надзвичайно швидкими темпами розвивається така галузь криптологічної науки як квантова криптографія. Її протоколи мають переваги у безпечності в порівнянні з класичною (не квантовою) криптографією.

Дисертаційна робота Лімаря І.В. присвячена створенню нового безпечного протоколу криптографічного захисту системи електронного голосування, в якому вперше запропоновано використовувати квантове бітове зобов'язання. Вказаний примітив автор роботи використовує спільно із квантовим розділенням секрету. Саме це й визначає актуальність виконаного дисертаційного дослідження.

Оцінка змісту автореферату: Виходячи з представлених матеріалів, автор здійснив логічну побудову дисертаційної роботи, як послідовну композицію:

теоретичної основи у вигляді розробки системи криптографічного захисту процедури електронного голосування із спільним використанням протоколу квантового бітового зобов'язання та протоколу квантового розділення секрету та розширеної класифікації атак на квантові криптосистеми, а також розробки методу підвищення інформаційної місткості джерела при передаванні інформації окремими фотонами в протоколах квантової криптографії, шляхом використання тривимірних класичних або квантових систем – тритів або кутритів замість кубітів або бітів відповідно

та практичної складової власних досліджень у вигляді програмного забезпечення оцінки швидкодії запропонованого методу, що базується на застосуванні тривалих випадкових оборотних матриць у випадку передавання тритів.

Така структура представлення результатів досліджень в авторефераті демонструє наявність комплексного підходу до вирішення наукової задачі і сформульованих в її рамках наукових завдань. Представлені в авторефераті відомості, на наш погляд, повністю характеризують зміст дисертаційної роботи і дозволяють судити про новизну і практичну значущість результатів. Приведений список наукових робіт свідчить про достатню апробацію і публікації результатів досліджень.

Характеристика новизни. Як можна судити із змісту автореферату, найбільш цінними науковими результатами, отриманими автором, є:

вперше розроблений протокол квантового розділення секрету з використанням кубітів, який може бути реалізований на сучасній технологічній базі; на відміну від раніш створених аналогів протокол не потребує використання великих обсягів квантової пам'яті;

вперше розроблений протокол квантового розділення секрету з використанням кутритів, який забезпечує підвищену інформаційну місткість у порівнянні зі схемами на основі кубітів; цей протокол орієнтований на перспективну технологічну базу; на відміну від раніш відомих також не потребує використання великих обсягів квантової пам'яті;

вперше розроблений протокол криптографічного захисту системи електронного голосування із спільним використанням протоколів квантового бітового зобов'язання та квантового розділення секрету, який відрізняється від відомих схем захисту систем електронного голосування використанням квантових криптопротоколів, що забезпечує можливість виявлення атаки перехоплення інформації у реальному часі та більш високу стійкість до інших атак.

Практичне значення одержаних результатів полягає у тому, що вони можуть бути використані для підвищення криптографічної захищеності систем електронного голосування з застосуванням квантових криптографічних протоколів.

Зауваження. Аналіз змісту автореферату дозволив виявити такі недоліки:

- в авторефераті зазначено, що у другому розділі роботи описано два квантових протоколи розділення секрету, які потребують мінімальні обсяги квантової пам'яті, а згідно блок-схемі (рисунок 1 в тексті автореферату) один з кубітів залишається на певний час у станції Боб. Проте в авторефераті не конкретизується, як саме організовано у протоколі зберігання кубіту у квантовій пам'яті, яка за твердженням автора хоча і має невеликий об'єм, але все ж передбачена схемою;

- в авторефераті зазначено, що у четвертому розділі роботи викладено результати аналізу швидкодії методу захисту інформації з використанням оборотних матриць. Дійсно, у таблиці 2 автореферату наведений середній час генерації трійкової матриці. Але, як відомо, середні значення результатів експериментів мають бути наведені з вказанням стандартної похибки середнього (±SE), чого в таблиці немає.

Висновок. Судячи зі змісту автореферату, дисертаційна робота І.В.Ломаря *«Криптографічний захист системи електронного голосування з використанням протоколів квантової криптографії»* відповідає вимогам щодо кандидатських дисертацій згідно відповідних пунктів «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами) та паспорту спеціальності 05.13.21 – системи захисту інформації, а автор роботи – Ломарь Ігор Валерійович, заслуговує на присудження йому наукового ступеня кандидата технічних наук за вказаною спеціальністю.

Завідувач кафедри інформаційної [illegible]
Факультету інформаційних технологій [illegible]
Київського університету імені Бориса Грінченка
доктор технічних наук, професор В.Л. Бурячок

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
ВЛАСНОРУЧНИЙ ПІДПИС
Бурячок В.Л.