ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

Каптьола Євгенія Юрійовича

«Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу»,

яка подається на здобуття наукового ступеня доктора філософії

з галузі знань 12 – Інформаційні технології

за спеціальністю 125 – Кібербезпека та захист інформації

1. Оцінка роботи здобувача у процесі підготовки дисертації і виконання індивідуального плану навчальної та наукової роботи.

Здобувач Каптьол Євгеній Юрійович виконав у повному обсязі Індивідуальний план виконання освітньо-наукової програми підготовки доктора філософії. Освітня програма в обсязі 40 кредитів ECTS виконана у повному об'ємі. Він успішно склав наступні дисципліни:

- залік з навчальної дисципліни «Філософські засади та методологія наукових досліджень» (97 балів);
- іспит з навчальної дисципліни «Іноземна мова для аспірантів (англійська)» (86 балів);
- залік з навчальної дисципліни «Підготовка наукових публікацій та презентація результатів досліджень» (94 бали);
- залік з навчальної дисципліни «Реєстрація прав інтелектуальної власності» (95 балів);
- іспит з навчальної дисципліни «Математичні методи в кібербезпеці» (91 бал);
- залік з навчальної дисципліни «Методи побудови телекомунікаційних протоколів фізичного та канального рівнів» (90 балів);
- іспит з навчальної дисципліни «Моделі і методи комп'ютерної стеганографії» (90 балів);

Всі заплановані види робіт були виконані своєчасно. Здобувач плідно співпрацював з науковим керівником протягом усього терміну навчання.

2. Обґрунтування вибору теми дослідження.

Нині на міжнародному та національному рівні є актуальним питання забезпечення криптографічної стійкості стандартизованих асиметричних криптографічних перетворень, обґрунтування та стандартизації електронних підписів, які б забезпечували безумовну стійкість до класичних та квантових атак та атак сторонніми каналами (спеціальними каналами). Вказане пов'язано з тим, що для них розроблено математичні методи для реалізації атак, як на основі класичного, так і квантового криптоаналізу. Також важливу роль відіграє те, що за прогнозами в найближчі роки можливо буде розроблений надпотужний квантовий комп'ютер, який зможе зламувати існуючі криптосистеми орієнтуючись на використання вже існуючих квантових математичних методів. Також велику загрозу можуть становити спеціальні атаки, що ґрунтуються на витоках бічними каналами та на основі помилок. Тому важливо, як в теоретичному, так і в практичному змісті, зреагувати на можливості криптоаналітиків найвищого рівня та визначити вимоги та розробити методи оцінки і порівняння у відповідності до цих вимог перспективних захищених асиметричних криптографічних перетворень як серед вже стандартизованих, так і кандидатів на стандартизацію.

До основних методів і задач криптоаналізу, що можуть бути вирішені за допомогою квантового комп'ютера та становлять загрозу для сучасних криптоперетворень можна віднести наступні:

1. алгоритм Гровера для пошуку в несортованій базі;
2. алгоритм факторизації Шора;
3. алгоритм Шора для розв'язку дискретного логарифму в скінченному полі;
4. алгоритм Шора для розв'язку дискретного логарифму в групі точок еліптичної кривої.

Саме через загрозу з боку квантових технологій NIST США було організовано конкурс NIST PQC, де було проведено три раунди відбору

кандидатів на стандартизацію, розроблено проєкти стандартів та продовжено дослідження в четвертому раунді. Після проведення трьох раундів NIST PQC для стандартизації було обрано 4 кандидати (електронні підписи (ЕП) Crystals-Dilithium, Falcon та SPHINCS+ та механізм інкапсуляції ключа Crystals-Kyber). Також було визначено кандидатів для участі в четвертому раунді (криптографічні перетворення механізмів інкапсуляції ключів BIKE, Classic McEliece, HQC та SIKE), один з яких його розробники визнали ненадійним для використання (SIKE).

Специфіка обраних завдяки трьом раундам конкурсу NIST PQC алгоритмів призвела до потреби у пошуку для стандартизації додаткових кандидатів з числа електронних підписів загального призначення. Для цього було розпочато окремий процес стандартизації схем електронного підпису (також відомий як «процес стандартизації додаткових підписів»). Одним з критеріїв, що призвели до цього є потреба у ЕП, що не базуються на використанні решіток (хоча слід зауважити, що попри це у додатковому раунді все одно беруть участь схеми ЕП, що базуються на решітках). Серед видів ЕП поданих на розгляд до першого раунду додаткового процесу стандартизації наявні наступні: підписи засновані на кодах, підписи на ізогеніях, багатовимірні підписи, симетричні підписи, MPC-in-the-head та підписи визначені NIST як "інші".

Таким чином, можна зробити висновок, що сучасний стан забезпечення безпеки електронними підписами потребує розробки та покращення засобів та методів оцінки захищеності асиметричних криптографічних примітивів та порівняння їх з метою виділення кращих за множиною безумовних, умовних та прагматичних критеріїв, що обґрунтовується задачею розробки методичних основ оцінки та порівняння. В таких методичних основах повинні бути обґрунтовані безумовні критерії оцінки безпечності електронних підписів від класичних, квантових атак та атак бічними каналами та на основі помилок. По суті, ці задачі зводяться до теоретичного доведення стійкості електронних підписів по моделі безпеки EUF-CMA (existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенційної підробки в умовах адаптивного вибору повідомлення. Під квантовостійкими будемо

розуміти електронні підписи, що є стійкими як до класичних, так і до квантових атак. Проблеми захищеності від атак бічними каналами у зв'язку зі складністю в цій роботі не розглядаються.

Мета і завдання дослідження. Метою дисертаційної роботи є обґрунтування вибору, аналіз та дослідження, оцінка та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Основні завдання дисертаційного дослідження:

1. Розробка удосконаленої методології оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по безумовним, умовним та прагматичним критеріям, яка б дозволила оцінити, порівняти і обрати найбільш перспективні ЕП, і в тому числі виявити вразливості в них.

2. Оцінка та порівняння перспективних квантовостійких національних та міжнародних стандартів електронних підписів ДСТУ 9212:2023 та FIPS 204.

3. Аналіз безпеки математики Falcon і Сокіл, реалізація атаки на відновлення таємних ключів та розробка пропозицій щодо захисту від неї.

4. Застосування методології для порівняння існуючих, перспективних окремо та існуючих та перспективних квантовостійких електронних підписів.

Об'єкт та предмет дослідження.

Об'єкт дослідження – процеси вибору, аналізу та дослідження, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Предмет дослідження – методи аналізу та дослідження, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Методи дослідження.

Методи досліджень визначені сутністю розв'язуваних задач і включають методи системного аналізу та прийняття рішень, методи прикладної криптології, методи класичного та квантового криптоаналізу, методи оцінки та порівняння асиметричних електронних підписів, що відповідають сучасним вимогам до національних та міжнародних стандартів, методи математичного моделювання,

методи захищеності від квантового криптоаналізу на основі масштабування. Експериментальні дослідження та чисельні розрахунки виконувалися на мові програмування Python.

3. Зв'язок роботи з науковими програмами, планами, темами.

Результати дисертаційних досліджень були використані при підготовці та проведенні лабораторних робіт по дисципліні «Прикладна криптологія» для спеціальності «Кібербезпека».

4. Особистий внесок дисертанта в отриманні наукових результатів та їх новизна.

Особистий внесок дисертанта в отриманні наукових результатів та їх новизна полягає у наступному:

1. Вперше отримано оцінки порівняльного аналізу вже стандартизованих та кандидатів на стандартизацію квантовостійких ЕП із математичною адаптацією вимог, викликаних особливостями різних варіантів застосування. Попередні дослідження фокусувалися на безпекових вимогах з меншою увагою до умовних та прагматичних. Отримані оцінки дозволяють більш точно оцінити придатність до використання оцінюваних криптоперетворень в перехідний та пост-квантовий періоди.

2. Удосконалено комплексну методику оцінки та порівняльного аналізу асиметричних ЕП, стійких до класичного та квантового криптоаналізу, що відрізняється від існуючих тим, що враховує спрямованість та мету здійснення оцінки та порівняльного аналізу та вводить коефіцієнти значущості, котрі збільшують точність визначення найбільш відповідного переможця.

3. Вперше отримано оцінку ймовірності реалізації атаки та впливу виявлених недоліків методу та потенційних векторів атак на захищеність Falcon із врахуванням релевантних моделей безпеки.

4. Обґрунтовано особливостей заміни плаваючої точки на фіксовану точку з метою усунення загрози атаки на відновлення ключів на алгоритм з переліку порівнюваних.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі, забезпечується: адекватністю припущень, які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів. Результати проведених чисельних розрахунків узгоджуються з отриманими теоретичними висновками.

Основні результати дисертаційного дослідження опубліковані в індексованих наукових журналах та доповідалися на міжнародних наукових конференціях. Висновки дисертаційної роботи є обґрунтованими.

6. Наукове, теоретичне та практичне значення результатів дисертації.

У наукових статтях, опублікованих у співавторстві, здобувачу належать наступні результати:

- Порівняння наборів параметрів фіналісту третього раунду NIST PQC алгоритму Rainbow за критеріями захищеності та порівняння методів атак на алгоритм Rainbow за критеріями складності;

- Верифікація атаки на алгоритм Falcon, оцінка ймовірності її реалізації та впливу виявлених недоліків методу та потенційних векторів атак на захищеність ЕП Falcon із врахуванням релевантних моделей безпеки;

- Формування безумовних критеріїв оцінки та порівняння із врахуванням моделей порушника, загроз та безпеки, проведення аналізу та оцінки криптографічних перетворень за безумовними критеріями та програмне моделювання процесів оцінки за безумовними критеріями;

- Дослідження кандидатів на стандартизацію в якості квантовостійкого стандарту електронного підпису на конкурсі NIST зі стандартизації додаткових електронних підписів, що базуються на нових квантовостійких проблемах, за безумовними критеріями.

Розроблено програмне забезпечення, яке дозволяє:

1) Проведення оцінки існуючих та перспективних методів електронного підпису.

2) Проведення покращеного оцінювання та порівняння ЕП із врахуванням мети здійснення оцінювання та спрямованості варіанту застосування ЕП.

3) Моделювання комплексної методики оцінки та порівняння існуючих та перспективних методів електронного підпису.

Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків та були використані при розробці стандартів ДСТУ 8961:2019 та ДСТУ 9212:2023.

7. Повнота викладення матеріалів дисертації в роботах, опублікованих автором.

Основні результати дисертаційних досліджень опубліковано у **6** наукових працях, серед яких: **4** статей у фахових виданнях України, **2** статті у зарубіжних виданнях (індексується у Scopus, Web of Science), **5** матеріали та тези доповідей на конференціях.

Наукова публікація у зарубіжних виданнях, що входять до міжнародних наукометричних баз Scopus та Web of Science:

1. Potii, O., Kachko, Potii, O., Kachko, O., Kandii, S., Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 52–59.

(Особистий внесок здобувача: Верифікація та аналіз результатів здійснення атаки. Оцінка ймовірності реалізації атаки та впливу виявлених недоліків методу та потенційних векторів атак на захищеність алгоритму із врахуванням релевантних моделей безпеки).

1. Kachko O.G., Gorbenko Y.I., Kandii S.O., Kaptol Y.Y. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern-European Journal of Enterprise Technologies. 2024. Vol. 4, Is. 9, P. 6–17.

(Особистий внесок здобувача: оцінено вплив на безпекуелектронного підпису застосування фіксованої точки замість плаваючої точки на етапі генерації підпису)

Наукові публікації у фахових виданнях України

2. Kaptiol, Y. Y. (2022). Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion. // Каптьол, Є. Ю. Аналіз стану постквантового алгоритму

електронного підпису RAINBOW та атак на нього на період завершення третього раунду NIST PQC. Radiotekhnika, 2(209), 87–92.

(Особистий внесок здобувача: Аналіз фіналісту третього раунду NIST PQC алгоритму Rainbow за критеріями захищеності. Порівняння наборів загальносистемних параметрів алгоритму електронного підпису Rainbow. Аналіз та порівняння методів атак на алгоритм Rainbow за критеріями складності. Відповідні результати наведені в теоретичній та практичній частині роботи).

3. Yu.I. Gorbenko, M.V. Yesina, V.A. Ponomar, I.D. Gorbenko, E.Yu. Kapt'ol Scientific and methodological bases of analysis, evaluation and results of comparison of existing and promising (post-quantum) asymmetric cryptographic primitives of electronic signature, protocols of asymmetric encryption and key encapsulation protocols // Ю.І. Горбенко, М.В. Єсіна, В.А. Пономар, І.Д. Горбенко, Є.Ю. Каптьол. Науково-методичні основи аналізу, оцінки та результати порівняння існуючих та перспективних (постквантових) асиметричних криптографічних примітивів електронного підпису, протоколів асиметричного шифрування та протоколів інкапсуляції ключів. Radiotekhnika, 212, 42-66.

(Особистий внесок здобувача: Формування безумовних критеріїв оцінки та порівняння із врахуванням моделей порушника, загроз та безпеки, що базуються на міжнародних вимогах дотримання моделей EUF-CMA для ЕП та IND-CCA2 для АСШ. Аналіз та оцінка за критеріями безумовної стійкості, програмне моделювання процесів оцінки за безумовними критеріями).

4. Є. Ю. Каптьол, І. Д. Горбенко. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері. Radiotekhnika, 202, 37-48.

(Особистий внесок здобувача: Дослідження стану побудови квантових комп'ютерів на предмет оцінки можливості створення криптоаналітично значущого квантового комп'ютера. Виділення математичних методів квантового криптоаналізу для оцінки властивостей існуючих квантових комп'ютерів. Реалізація масштабованого методу квантового криптоаналізу на

квантовому комп'ютері. Порівняння теоретичних розрахунків застосування обраного методу з результатами практичного застосування).

5. Gorbenko, I., Kaptol, Y. (2023). Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems. Radiotekhnika, 4(215), 31–45.

(Особистий внесок здобувача: Дослідження кандидатів стандартизацію в якості квантовостійкого стандарту електронного підпису на конкурсі NIST зі стандартизації додаткових електронних підписів. Виділення безумовних критеріїв для оцінки та порівняння кандидатів на стандартизацію, що базуються на нових квантовостійких проблемах. Оцінка та порівняння обраних кандидатів на стандартизацію за безумовними критеріями).

8. Дотримання академічної доброчесності.

На підставі вивчення тексту дисертації здобувача, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній інтернет-системі Strikeplagiarism.com) встановлено, що дисертаційна робота виконана самостійно, текст дисертації не містить плагіату, а дисертація відповідає вимогам академічної доброчесності.

9. Апробація матеріалів дисертації.

Результати проведених досліджень представлялись на міжнародних та вітчизняних наукових конференціях у формі доповідей, за результатами яких були опубліковані матеріали конференцій:

1. Каптьол Є.Ю. Аналіз квантових методів криптоаналізу постквантового електронного підпису Rainbow // "Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку" збірник матеріалів I Міжнародної науково-технічної конференції. Київ – 2021. pp. 146 – 147.

2. Євгеній Каптьол. Key encapsulation mechanisms security in the random oracle model / Безпека механізмів інкапсуляції ключів у моделі випадкового оракула // "Захист інформації і безпека інформаційних систем" збірник матеріалів IX Міжнародної науково-технічної конференції. Львів – 2023. pp. 67 – 68.

3. Yevhenii Kaptol. Analysis of quantum attacks against rainbow post-quantum electronic signature // Information protection and information systems security proceedings of VIIIth International Scientific and Technical Conference November 11–12, 2021. Lviv Polytechnic Publishing House 2021. pp. 77-78.

4. Каптьол. Є.Ю. Порівняння електронних підписів, що грунтуються на нових постквантових проблемах // Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів III Міжнародної науково-технічної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2023, pp. 166-167 DOI: https://doi.org/10.61929/viti.mntk.3.2023

5. Потій О. В., Качко О. Г., Кандій С. О., Каптьол Є. Ю. Дослідження впливу плаваючої точки на безпеку алгоритму електронного підпису Falcon // Кіберборотьба: розвідка, захист та протидія: тези доповідей II Міжнародної науково-практичної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2024.-57с.

10. Оцінка структури, мови та стилю дисертації.

Матеріал дисертації викладено в логічній послідовності та доступно для сприйняття. Дисертація написана науковим стилем мовлення, структура дисертації відповідає алгоритму здійсненого автором дослідження. Зміст, структура, оформлення дисертації та кількість публікацій відповідають вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 12.01.2022 р. № 44), наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

11. Відповідність змісту дисертації спеціальності, за якою вона подається до захисту.

За своїм фаховим спрямуванням, науковою новизною і практичною значимістю дисертаційна робота Каптьол Є. Ю. «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу» повністю відповідає спеціальності

125 – Кібербезпека та захист інформації. Здобувачем повністю виконано освітню та наукову складову третього (освітньо-наукового) рівня вищої освіти.

12. Результати обговорення та проведення презентації. Рекомендація дисертації до захисту.

Здобувач представив основні результати своєї дисертаційної роботи на розширеному засіданні кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна щодо попередньої експертизи дисертації (Витяг з протоколу № 8 розширеного засідання кафедри кібербезпеки інформаційних систем, мереж і технологій від 10 березня 2025 р.) у формі презентації та наукової дискусії після її завершення. На даному засіданні були присутні 16 співробітників Харківського національного університету імені В. Н. Каразіна, із яких 4 докторів наук та 9 кандидатів наук. Дисертанту було задано 5 запитань, на які він надав вичерпні відповіді. Також виступили 4 науковця, які позитивно відізвались про дисертаційне дослідження Каптьола Є. Ю.

У рамках цього розширеного засідання було ухвалено одноголосно (16 голосів) рекомендувати дисертаційну роботу здобувача Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу» до захисту на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації.

Головуючий,
в.о. завідувача кафедри кібербезпеки
інформаційних систем, мереж і
технологій навчально-наукового
інституту комп'ютерних наук та
штучного інтелекту
кандидат технічних наук, доцент Марина ЄСІНА