Голові разової
спеціалізованої вченої ради
харківського національного
університету імені В. Н. Каразіна
професору Віталію ЄСІНУ
майдан Свободи 4, м. Харків, 61022

Рецензія

офіційного рецензента, доктора технічних наук, професора, професора кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна Олійникова Романа Васильовича на дисертаційну роботу Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації

Останні розробки в галузі безпеки електронних цифрових підписів пов’язані з тим, що на міжнародному та національному рівні є актуальним питання забезпечення криптографічної стійкості стандартизованих асиметричних криптографічних перетворень, обґрунтування та стандартизація електронних підписів, які б забезпечували безумовну стійкість до класичних та квантових атак та атак сторонніми каналами (спеціальними каналами). Цу пов’язано з тим, що зараз вже розроблено математичні методи для реалізації атак, як на основі класичного, так і квантового криптоаналізу. Також велику загрозу можуть

становити спеціальні атаки, що ґрунтуються на витоках бічними каналами та на основі помилок.

Саме через загрозу з боку технологій квантових обчислень 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.

Таким чином, тема дисертаційного дослідження, спрямованого на розробку 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, є своєчасною та важливою для вирішення актуальних науково-прикладних завдань.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі Каптьола Є. Ю., досягається коректним використанням відомих положень теорії множин, відношень, графів, математичної логіки, математичної статистики, формальних моделей безпеки, комплексним врахуванням набору загроз, вразливостей систем захисту на основі асиметричних ЕП, несуперечливістю відомим результатам, науковою апробацією результатів дисертаційних досліджень на науково-технічних і науково-практичних конференціях різного рівня.

Найвагоміші наукові результати, що містяться в дисертації

Основні наукові результати, одержані в дисертації, включають:

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, котрі входять до першого та частково другого етапів комплексної методики оцінки та порівняльного аналізу квантовостійких та перспективних асиметричних криптоперетворень. Отримані оцінки дозволяють більш точно оцінити придатність до використання оцінюваних криптоперетворень в перехідний та пост-квантовий періоди.

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

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.

Набули подальшого розвитку:

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

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 6 наукових праць, серед яких: 4 статті у фахових виданнях України, 2 статті у зарубіжних виданнях (індексується у Scopus, Web of Science), 5 матеріали та тези доповідей на конференціях.

Оцінка змісту дисертації, її завершеності в цілому і оформлення Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та

додатки. Загальний обсяг дисертації складає 180 сторінки друкованого тексту, з яких: 143 сторінки основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 4 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 73 найменувань на 10 сторінках, додатки на 8 сторінках. Робота містить 25 таблиць та 27 рисунків.

Перший розділ присвячений аналізу основних проблем, стану безпеки існуючих та обґрунтуванню вимог до методів перспективних квантовостійких електронних підписів, як методологічної основи побудови систем захисту та оцінки їхньої безпеки. На підставі проведеного аналізу робиться висновок про доцільність проведення подальших досліджень, результатом яких могла б стати методологія комплексної оцінки та порівняльного аналізу ЕП стійких до класичного та квантового криптоаналізу, що дозволило б підвищити ефективність захисту криптосистем на основі ЕП.

У другому розділі обґрунтовуються моделі порушника, загроз та безпеки. Показано множину різноманітних застосувань асиметричних електронних підписів, котрі висувають дещо відмінні один від одного вимоги до криптографічних перетворень типу асиметричний електронний підпис. Наведено переліки безумовних, умовних та прагматичних критеріїв.

Третій розділ роботи присвячений обґрунтуванню комплексної методики оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу. Запропоновано вдосконалення комплексної методики оцінки та порівняльного аналізу в частині врахування в процесі оцінки та порівняння за прагматичними критеріями мети здійснення порівняння та можливих варіантів застосування ЕП.

У четвертому розділі здійснено оцінку та порівняльний аналіз як кандидатів на стандартизацію між собою, так і вже стандартизованих для використання в перехідний та пост-квантовий періоди алгоритмів електронного підпису між собою. Проведено порівняння отриманих результатів порівняння вже стандартизованих алгоритмів з міжнародними результатами.

У п’ятому розділі дисертаційного дослідження уточнено оцінки та отримано експерементальні результати порівняння електронних підписів за допомогою розробленого програмного забезпечення. Для електронного підпису Falcon запропонована атака відновлення ключів та досліджено вплив використання фіксованої точки замість плаваючої точки в процесі формування підпису на безпеку.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки асиметричних електронних підписів.

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Зв’язок роботи з науковими програмами, планами, темами

Дослідження, результати яких знайшли відображення в дисертаційній роботі, виконані на кафедрі кібербезпеки інформаційних систем, мереж і технологій Харківського національного університету імені В. Н. Каразіна та у приватному акціонерному товаристві «Інститут інформаційних технологій». Результати дисертаційних досліджень використані при розробці та прийнятті в якості національних стандартів ДСТУ 8961:2019 "Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів" та ДСТУ 9212:2023 "Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами" (акт від 06.12.2023 р.).

Результати дисертаційних досліджень були використані при підготовці та проведенні лабораторних робіт з дисципліни «Прикладна криптологія» для спеціальності «Кібербезпека та захист інформації».

Практичне значення отриманих результатів

1. Математичні моделі та аналітичні співвідношення знайшли практичне застосування в ХНУ імені В. Н. Каразіна на кафедрі кібербезпеки інформаційних систем, мереж і технологій в дисциплінах першого рівня вищої освіти “Прикладна криптологія” при проведенні лабораторних робіт.

2. Розроблено програмне забезпечення, яке дозволяє:

- проведення оцінки існуючих та перспективних методів електронного підпису;
- проведення покращеного оцінювання та порівняння ЕП із врахуванням мети здійснення оцінювання та спрямованості варіанту застосування ЕП;
- моделювання комплексної методики оцінки та порівняння існуючих та перспективних методів електронного підпису.

3. Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків (акт від 06.12.2023 р.) та були використані при розробці стандартів ДСТУ 8961:2019, ДСТУ 9212:2023.

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі Strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Дискусійні положення та зауваження до змісту дисертації

1. Розглянуто не всі види актуальних підходів до реалізації квантовостійких асиметричних електронних цифрових підписів. Так, серед кандидатів на додаткову стандартизацію наявні підписи засновані на кодах, підписи на ізогеніях,

багатовимірні підписи, симетричні підписи, MPC-in-the-head та інші підписи, визначені NIST. Автор явно зосередився на тих кандидатах, які не потрапили в стандартну класифікацію та були виділені в «інші».

2. Оцінка та порівняльний аналіз в модифікації комплексної методики оцінки та порівняльного аналізу здійснено з урахуванням практичних застосувань ЕП, але не враховано частину поширених застосувань, таких як технології Blockchain, підписання коду, електронна пошта, електронні паспорти та загальна модель інфраструктури відкритих ключів (ІВК), хоча і були розглянуті окремі підпорядковані приклади ІВК.

3. У роботі зазначаються вимоги до квантовостійких криптографічних перетворень електронного підпису, які впливають на формування критеріїв оцінки та порівняльного аналізу, проте прямих порівнянь вимог не наведено, та процес формування критеріїв розглянуто частково, хоча в роботі все ж таки наявне посилання на відповідну статтю автора.

Однак, висловлені зауваження суттєво не впливають на загальну високу оцінку дисертаційного дослідження, його цілісність та результативність. Наукова новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Загальні висновки

Дисертаційна робота Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу» є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням відповідає 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) та

наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Каптьол Євгеній Юрійович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний рецензент
доктор технічних наук, професор,
професор кафедри кібербезпеки
інформаційних систем, мереж і технологій
Навчально-наукового інституту
комп’ютерних наук та
штучного інтелекту
Харківського національного
університету імені В. Н. Каразіна

Роман ОЛІЙНИКОВ

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 19:31:28 12.05.2025

Назва файлу з підписом: Рецензія_Олійников_Каптьол.pdf.asice
Розмір файлу з підписом: 53.8 КБ

Перевірені файли:
Назва файлу без підпису: Рецензія_Олійников_Каптьол.pdf
Розмір файлу без підпису: 51.3 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: Олійников Роман Васильович
П.І.Б.: Олійников Роман Васильович
Країна: Україна
РНОКПП: 2796617236
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 19:31:21 12.05.2025
Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг
Серійний номер: 382367105294AF9704000000F9AA0F0060BBD402
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00

Голові разової спеціалізованої вченої ради Харківського національного університету імені В. Н. Каразіна професору Віталію ЄСІНУ майдан Свободи 4, м. Харків, 61022

ВІДГУК

офіційного опонента, доктора технічних наук, професора, професора кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка Толюпи Сергія Васильовича на дисертаційну роботу Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

На разі актуальним є питання забезпечення криптографічної стійкості та стандартизації асиметричних електронних підписів, які б забезпечували безумовну стійкість до класичних та квантових атак. Це пов'язано з розробкою криптоаналітично значущого квантового комп'ютера та математичних методів для реалізації атак, як на основі класичного, так і квантового криптоаналізу.

Вирішенням цього питання займаються як на анціональному, так і на міжнародному рівнях. Так, наприклад, з боку 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.

Важливим з точки зору сучасного стану забезпечення безпеки електронними підписами є потреба у розробці та покращенні засобів та методів оцінки захищеності асиметричних криптографічних примітивів та порівняння їх з метою виділення кращих по множині безумовних, умовних та прагматичних критеріїв, що обґрунтовується задачею розробки методичних основ оцінки та порівняння.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі Каптьола Є. Ю., досягається коректним використанням відомих положень теорії множин, відношень, графів,

математичної логіки, математичної статистики, формальних моделей безпеки, комплексним урахуванням набору загроз, вразливостей систем захисту на основі асиметричних ЕП, несуперечливістю відомим результатам, науковою апробацією результатів дисертаційних досліджень на науково-технічних і науково-практичних конференціях різного рівня.

Наукова новизна одержаних результатів, що містяться в дисертаційній роботі

Основні наукові результати, одержані в дисертації, включають:

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, котрі входять до першого та частково другого етапів комплексної методики оцінки та порівняльного аналізу квантовостійких та перспективних асиметричних криптоперетворень. Отримані оцінки дозволяють більш точно оцінити придатність до використання оцінюваних криптоперетворень в перехідний та пост-квантовий періоди.

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

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.

Набули подальшого розвитку:

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

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 6 наукових праць, серед яких: 4 статті у фахових виданнях України, 2 статті у зарубіжних виданнях (індексується у Scopus, Web of Science), 5 матеріали та тези доповідей на конференціях.

Оцінка змісту дисертаційної роботи, її завершеності в цілому

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 180 сторінки друкованого тексту, з яких: 143 сторінки основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 4 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 73 найменувань на 10 сторінках, додатки на 8 сторінках. Робота містить 25 таблиць та 27 рисунків.

Перший розділ присвячений аналізу основних проблем, стану безпеки існуючих та обґрунтуванню вимог до методів перспективних квантовостійких електронних підписів, як методологічної основи побудови систем захисту та оцінки їхньої безпеки. На підставі проведеного аналізу робиться висновок про доцільність проведення подальших досліджень, результатом яких могла б стати методологія комплексної оцінки та порівняльного аналізу ЕП стійких до класичного та квантового криптоаналізу, що дозволило б підвищити ефективність захисту криптосистем на основі ЕП.

У другому розділі дисертації обгрунтовано моделі порушника, загроз та безпеки. Показано, що асиметричні електронні підписи мають множину різноманітних застосувань, котрі висувають дещо відмінні один від одного вимоги до криптографічних перетворень типу асиметричний електронний підпис. Наведено переліки безумовних, умовних та прагматичних критеріїв.

У третьому розділі дисертації (Науково-методичні основи розробки, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів за безумовними, умовними та прагматичними критеріями) обгрунтовано комплексну методику оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу. Запропоновано вдосконалення комплексної методики оцінки та порівняльного аналізу в частині врахування в процесі оцінки та порівняння за прагматичними критеріями мети здійснення порівняння та можливих варіантів застосування ЕП, що призодить до збільшення точності та відповідності отриманого результату вихідним вимогам.

У четвертому розділі дисертації (Аналіз, оцінка та порівняння існуючих та кандидатів на перспективні квантовостійкі національні та міжнародні електронні підписи за безумовними критеріями) здійснено оцінку та порівняльний аналіз як кандидатів на стандартизацію між собою, так і вже стандартизованих для використання в перехідний та пост-квантовий періоди алгоритми електронного підпису між собою. Проведено порівняння отриманих результатів порівняння вже стандартизованих алгоритмів з міжнародними результатами.

У п’ятому розділі дисертації уточнено оцінки та отримано експерементальні результати порівняння електронних підписів за допомогою розробленого

програмного забезпечення. Для електронного підпису Falcon запропонована атака відновлення ключів та досліджено вплив використання фіксованої точки замість плаваючої точки в процесі формування підпису на безпеку.

У розділі “Висновки” наведено основні результати дисертаційного дослідження.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки асиметричних електронних підписів.

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі Strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Недоліки та зауваження до змісту дисертаційної роботи

1. Види актуальних підходів до реалізації квантовостійких асиметричних ЕП розглянуто частково. Серед кандидатів на додаткову стандартизацію ЕП автор явно зосередився на тих кандидатах, котрі не влучали в стандартну класифікацію та були виділені в «інші», та не приділив достатньої уваги тим, котрі підпадіють під категорії: підписи засновані на кодах, підписи на ізогеніях, мультиваріативні підписи, симетричні підписи, MPC-in-the-head.

2. З точки зору статистики та методів експертної оцінки, для отримання точних результатів необхідні значні обсяги вибірки. В дисертаційній роботі обсяги вибірки є відносно невеликими, хоча цей недолік частково усувається завдяки високій кваліфікації експертів та різноманітності їх підходів. Цей недолік признано автором та надано рекомендації щодо коректного застосування комплексної методики оцінки та порівняння.

3. В роботі відображено виявлену в процесі оцінки Falcon атаку на реалізацію та запропоновано рекомендації з підвищення безпеки та усунення загрози реалізації атаки. Проте не було відображено порівняння безпеки Falcon до застосування та після застосування пропозицій з підвищення безпеки з точки зору комплексної методики.

4. Деякі практичні застосування електронних підписів (наприклад, ІВК, SSL/TLS, DNSSEC, S/MIME, IPsec) розглядаються досить детально, з описом протоколів та алгоритмів. Інші ж застосування (підпис коду, SIM-карти, електронні паспорти, підписання PDF, технології Blockchain, VPN) згадуються більш

поверхово, без глибокого аналізу їхніх специфічних вимог до електронних підписів. Це створює нерівномірне розуміння контексту.

5. В підрозділі 3.2. перелік безумовних критеріїв, наведений для протоколів інкапсуляції ключів (ПІК), містить критерії, які більше характерні для електронних підписів (WEП, NEП). Потрібно обґрунтувати включення цих критеріїв до оцінки ПІК або уточнити їхню інтерпретацію в цьому контексті.

Однак, висловлені зауваження не впливають суттєво на загальну високу оцінку дисертаційного дослідження, його цілісність та результативність. Наукова новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Висновок про дисертаційне дослідження

Дисертаційна робота Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу» є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12.01.2022 р. № 44.

Виходячи з цього, вважаю, що Каптьол Євгеній Юрійович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

ОФІЦІЙНИЙ ОПОНЕНТ
доктор технічних наук, професор,
професор кафедри кібербезпеки та захисту інформації Київського національного університету Імені Тараса Шевченка Сергій ТОЛЮПА

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 16:53:52 13.05.2025

Назва файлу з підписом: Відгук Каптьола.pdf.asice
Розмір файлу з підписом: 243.0 КБ

Перевірені файли:
Назва файлу без підпису: Відгук Каптьола.pdf
Розмір файлу без підпису: 243.7 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ТОЛЮПА СЕРГІЙ ВАСИЛЬОВИЧ
П.І.Б.: ТОЛЮПА СЕРГІЙ ВАСИЛЬОВИЧ
Країна: Україна
РНОКПП: 2231818791
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 16:53:54 13.05.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F04000000FEFFC100BF690006
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними для перевірки (XAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00

Голові разової
спеціалізованої вченої ради
харківського національного
університету імені В. Н. Каразіна
професору Віталію ЄСІНУ
майдан Свободи 4, м. Харків, 61022

Відгук

офіційного опонента, доктора технічних наук, професора, начальника кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут Чевардіна Владислава Євгенійовича на дисертаційну роботу Каптьола Євгенія Юрійовича "Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу", подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

В умовах стрімкого розвитку квантових технологій на міжнародному та національному рівнях вирішується питання обрання та стандартизації квантовостійких криптографічних перетворень. Це пов'язано зі значним зростанням швидкості обчислень та викликами для безпеки криптографічних перетворень, що прогнозуються за умови використання для криптоаналізу квантового комп'ютера достатньої потужності.

Через це з боку NIST було запроваджено конкурс NIST PQC, призначений для обрання кандидатів для стандартизації в сфері квантовостійких криптографічних перетворень. З іншого боку, велику загрозу можуть становити спеціальні атаки, що ґрунтуються на витоках бічними каналами та на основі помилок. Тому як на міжнародному, так і на національному рівнях, важливо

зреагувати на можливості криптоаналітиків найвищого рівня та визначити вимоги і розробити перспективні захищені криптоперетворення електронного підпису та стандартизувати їх в тому числі на національному рівні.

Сучасний стан процесу забезпечення безпеки електронними підписами потребує розробки та покращення засобів і методів оцінки та порівняння захищеності асиметричних криптографічних примітивів з метою виділення кращих за множинами, зокрема безумовних, умовних та прагматичних критеріїв.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі Каптьола Є. Ю., досягається коректним використанням відомих положень теорії множин, відношень, графів, математичної логіки, математичної статистики, формальних моделей безпеки, комплексним врахуванням набору загроз, вразливостей систем захисту на основі асиметричних ЕП, несуперечливістю відомим результатам, науковою апробацією результатів дисертаційних досліджень на науково-технічних і науково-практичних конференціях різного рівня.

Наукова новизна одержаних результатів, що містяться в дисертаційній роботі

Основними науковими результатами, одержаними в дисертації, є наступні:

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, котрі входять до першого та частково другого етапів комплексної методики оцінки та порівняльного аналізу квантовостійких та перспективних асиметричних криптоперетворень. Отримані оцінки дозволяють більш точно оцінити придатність до використання оцінюваних криптоперетворень в перехідний та постквантовий 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.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 6 наукових праць, серед яких: 4 статті у фахових виданнях України, 2 статті у зарубіжних виданнях (індексується у Scopus, Web of Science), 5 матеріали та тези доповідей на конференціях.

Оцінка змісту дисертаційної роботи, її завершеності в цілому

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 180 сторінки друкованого тексту, з яких: 143 сторінки основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 4 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 73 найменувань на 10 сторінках, додатки на 8 сторінках. Робота містить 25 таблиць та 27 рисунків.

Перший розділ присвячений аналізу основних проблем, стану безпеки існуючих та обґрунтуванню вимог до методів перспективних квантовостійких електронних підписів, як методологічної основи побудови систем захисту та оцінки їхньої безпеки. На підставі проведеного аналізу робиться висновок про

доцільність проведення подальших досліджень, результатом яких могла б стати методологія комплексної оцінки та порівняльного аналізу ЕП стійких до класичного та квантового криптоаналізу, що дозволило б підвищити ефективність захисту криптосистем на основі ЕП.

У другому розділі обґрунтовуються моделі порушника, загроз та безпеки, множина різноманітних застосувань асиметричних електронних підписів, котрі висувають дещо відмінні один від одного вимоги до безпеки. Наведено переліки безумовних, умовних та прагматичних критеріїв.

Третій розділ роботи присвячений обґрунтуванню комплексної методики оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу та вдосконаленню комплексної методики оцінки та порівняльного аналізу з метою врахування в процесі оцінки та порівняння за прагматичними критеріями мети здійснення порівняння та можливих варіантів застосування ЕП.

Четвертий розділ присвячено здійсненню оцінки та порівняльного аналізу як кандидатів на стандартизацію між собою, так і вже стандартизованих для використання в перехідний та постквантовий періоди алгоритмів електронного підпису між собою, а також проведенню порівняння отриманих результатів порівняння вже стандартизованих алгоритмів з міжнародними результатами.

У п’ятому розділі дисертаційного дослідження уточнено оцінки та отримано експериментальні результати порівняння електронних підписів за допомогою розробленого програмного забезпечення. Разом з тим, для електронного підпису Falcon запропонована атака відновлення ключів та проведено дослідження впливу використання фіксованої точки замість плаваючої точки в процесі формування підпису на безпеку схеми.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки асиметричних електронних підписів.

Оформлення дисертації

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі Strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Недоліки та зауваження до змісту дисертаційної роботи

1. У роботі було розглянуто в процесі оцінки та порівняння актуальні підходи до реалізації квантовостійких асиметричних ЕП, проте значна їх частина залишилась поза фокусом оцінки та порівняння. Так, наприклад, серед кандидатів на додаткову стандартизацію ЕП не були розглянуті підписи засновані на кодах, мультиваріативні підписи, симетричні підписи, тощо. Хоча комплексна методика і передбачає можливість її застосування до будь-якої множини ЕП, демонстрація застосування її до ширшого кола кандидатів на квантову стійкість посилила б обґрунтованість отриманих результатів.

2. У роботі зазначаються вимоги до квантовостійких криптографічних перетворень електронного підпису як на національному, так і на міжнародному рівнях. Ці вимоги є витоками критеріїв оцінки та порівняльного аналізу, проте в роботі питання процесу формування критеріїв з вимог знайшло лише часткове відображення.

3. У формулі 5.1 застосовується ділення на 10 як базис нормалізації зважених оцінок, проте в роботі не пояснюється, чому обрано саме це значення.

4. У роботі приділено увагу конкурсу NIST PQC, зокрема описано криптоаналітичні атаки на алгоритм Rainbow. Водночас інші кандидати, які були

відхилені за результатами третього раунду (зокрема, GeMSS і Picnic), не згадані, хоча вони також належать до класу квантовостійких електронних підписів. Згадка про них могла б надати більш повну картину процесу оцінювання та відбору кандидатів і висвітлити обмеження окремих криптографічних підходів.

Однак, висловлені зауваження не впливають суттєво на загальну позитивну оцінку дисертаційного дослідження, його цілісність та результативність.

Висновок про дисертаційне дослідження

Дисертаційна робота Каптьола Євгенія Юрійовича "Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу" є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Каптьол Євгеній Юрійович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Протокол засідання кафедри кібербезпеки від 10.05.2025 №17.

Офіційний опонент
доктор технічних наук, професор,
начальник кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імен Героїв Крут

Владислав ЧЕВАРДІН

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 10:30:10 14.05.2025

Назва файлу з підписом: Відгук Каптьол ХНУ Каразіна.pdf.asice
Розмір файлу з підписом: 126.6 КБ

Перевірені файли:
Назва файлу без підпису: Відгук Каптьол ХНУ Каразіна.pdf
Розмір файлу без підпису: 130.9 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: ЧЕВАРДІН ВЛАДИСЛАВ ЄВГЕНІЙОВИЧ
П.І.Б.: ЧЕВАРДІН ВЛАДИСЛАВ ЄВГЕНІЙОВИЧ
Країна: Україна
РНОКПП: 2883718934
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 10:30:08 14.05.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000009CAB8201746A4E06
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Серійний номер носія особистого ключа: 020
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними ЦСК для перевірки (CAdES-X Long)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00

Голові разової
спеціалізованої вченої ради
харківського національного
університету імені В. Н. Каразіна
професору Віталію ЕСІНУ
майдан Свободи 4, м. Харків, 61022

Відгук

офіційного опонента, доктора технічних наук, професора, професора кафедри безпеки інформаційних технологій національного авіаційного університету Корченко Олександра Григоровича на дисертаційну роботу Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертаційної роботи

Нині, як на національному так і на міжнародному рівні є актуальним питання забезпечення криптографічної стійкості стандартизованих асиметричних криптографічних перетворень, обгрунтування та стандартизації електронних підписів, які б забезпечували безумовну стійкість до класичних та квантових атак. Вказане пов’язано з тим, що для них розроблено математичні методи для реалізації атак, як на основі класичного, так і квантового криптоаналізу.

До основних методів і задач криптоаналізу, що можуть бути вирішені за допомогою квантового комп’ютера та становлять загрозу для сучасних

криптоперетворень можна віднести: алгоритм Гровера для пошуку в несортованій базі; алгоритм факторизації Шора; алгоритм Шора для розв'язку дискретного логарифму в скінченному полі; алгоритм Шора для розв'язку дискретного логарифму в групі точок еліптичної кривої.

Також велику загрозу можуть становити спеціальні атаки, що ґрунтуються на витоках побічними каналами та на основі помилок.

Таким чином, для забезпечення безпеки електронними підписами потребується розробка та покращення засобів та методів оцінки захищеності асиметричних криптографічних примітивів та порівняння їх з метою виділення кращих по множині безумовних, умовних та прагматичних критеріїв.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій

Обгрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертаційній роботі Каптьола Є. Ю., досягається коректним використанням відомих положень теорії множин, відношень, графів, математичної логіки, математичної статистики, формальних моделей безпеки, комплексним урахуванням набору загроз, вразливостей систем захисту на основі асиметричних ЕП, несуперечливістю відомим результатам, науковою апробацією результатів дисертаційних досліджень на науково-технічних і науково-практичних конференціях різного рівня.

Наукова новизна одержаних результатів, що містяться в дисертаційній роботі

Основними науковими результатами, одержаними в дисертації, є наступні:

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, котрі входять до першого та частково другого етапів комплексної методики оцінки та порівняльного аналізу квантовостійких та перспективних асиметричних криптоперетворень. 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. Обгрунтовано особливостей заміни плаваючої точки на фіксовану точку з метою усунення загрози атаки на відновлення ключів на алгоритм з переліку порівнюваних.

Апробація дисертації та публікації

Основні результати дисертаційної роботи були апробовані та відповідним чином опубліковані у фахових виданнях. Відповідно основному переліку робіт, за темою дисертаційної роботи було опубліковано 6 наукових праць, серед яких: 4 статей у фахових виданнях України, 2 статей у зарубіжних виданнях (індексується у Scopus, Web of Science), 5 матеріали та тези доповідей на конференціях.

Оцінка змісту дисертаційної роботи, її завершеності в цілому

Дисертаційна робота містить: вступ, 5 розділів, висновки, перелік посилань та додатки. Загальний обсяг дисертації складає 180 сторінки друкованого тексту, з яких: 143 сторінки основного тексту, 10 сторінок анотації, список публікацій здобувача за темою дисертації на 4 сторінках, 3 сторінки змісту, 2 сторінки переліку умовних позначень, список використаних джерел із 73 найменувань на 10 сторінках, додатки на 8 сторінках. Робота містить 25 таблиць та 27 рисунків.

Список використаних у роботі джерел свідчить про те, що під час роботи були проаналізовані сучасні результати наукових досліджень.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям забезпечення безпеки баз даних.

Оформлення дисертації

Оформлення дисертації повністю відповідає вимогам, що висуваються до дисертаційних робіт відповідно до наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Дотримання академічної доброчесності

При аналізі дисертаційної роботи, наукових праць здобувача та Протоколу контролю оригінальності (перевірку наявності текстових запозичень виконано в антиплагіатній Інтернет-системі Strikeplagiarism.com) встановлено, що текст дисертації не містить запозичень, дисертаційна робота виконана самостійно і відповідає вимогам академічної доброчесності.

Недоліки та зауваження до змісту дисертаційної роботи

1. Проведені оцінка та порівняльний аналіз в модифікації комплексної методики оцінки та порівняльного аналізу здійснені лише для таких засобів як: SSL/TLS, SIM-карти, IPSec, DNSSEC, VPN та підписання PDF, а порівняння для решт, таких як технології Blockchain, підписання коду, електронна пошта, електронні паспорти не були розглянуті. Автор обґрунтовує це подібністю цих застосувань до вже обраних та меншою їх релевантністю для прийняття оцінюваних алгоритмів за стандарт, проте це б забезпечило більшу повноту аналізу засобів пов'язаних з предметом дослідження.

2. У дисертаційній роботі висувається пропозиція з використання фіксованої точки замість плаваючої в процесі формування електронного підпису Falcon. Доцільно здійснити порівняння безпеки Falcon до та після застосування пропозицій з усунення загрози реалізації атаки та інших варіантів усунення такої загрози реалізації.

3. Наведені в дисертаційній роботі оцінки та порівняння мають обмежений обсяг вибірки, що призводить до зниження неупередженості отриманої оцінки.

4. В роботі використовується підхід до оцінювання та порівняльного аналізу на основі експертних методів, проте інші методи проведення оцінювання та порівняльного аналізу не розглянуто.

Висловлені зауваження не суттєво впливають на загальну високу оцінку дисертаційного дослідження, його цілісність та результативність. Наукова новизна та практична значущість отриманих результатів залишаються вагомими та не применшуються зазначеними дискусійними моментами.

Висновок про дисертаційне дослідження

Дисертаційна робота Каптьола Євгенія Юрійовича «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного

та квантового криптоаналізу» є завершеним науковим дослідженням, що має наукову новизну і практичну значущість. Дана дисертаційна робота за актуальністю, змістом та повнотою викладу її результатів у наукових публікаціях, обсягом і оформленням цілком відповідає 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) та наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження Вимог до оформлення дисертації».

Виходячи з цього, вважаю, що Каптьол Євгеній Юрійович заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент
Перший проректор Державного університету
інформаційно-комунікаційних технологій,
член-кореспондент НАН України,
лауреат Державної премії України
в галузі науки і техніки,
Заслужений діяч
науки і техніки України,
доктор технічних наук, професор Олександр КОРЧЕНКО

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 14:25:00 14.05.2025

Назва файлу з підписом: Каптьол PDF.pdf.asice
Розмір файлу з підписом: 238.1 КБ

Перевірені файли:
Назва файлу без підпису: Каптьол PDF.pdf
Розмір файлу без підпису: 244.9 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: КОРЧЕНКО ОЛЕКСАНДР ГРИГОРОВИЧ
П.І.Б.: КОРЧЕНКО ОЛЕКСАНДР ГРИГОРОВИЧ
Країна: Україна
РНОКПП: 2242506733
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 14:24:58 14.05.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000001C75FA002DAF1806
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підпис та дані в архіві (розширений) (ASiC-E)
Формат підпису: З повними даними для перевірки (XAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2025.02.05 13:00