Рішення разової спеціалізованої вченої ради ДФ 26.133.080
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії Абрамов Сергій Вадимович, 1995 року народження, громадянин України, освіта вища: закінчив у 2020 році Київський столичний університет імені Бориса Грінченка, за спеціальністю «Комп'ютерні науки», працює системним адміністратором у Київському столичному університеті імені Бориса Грінченка виконавчого органу Київської міської ради (Київської міської державної адміністрації) з 2019 р., виконав акредитовану освітньо-наукову програму «Інформаційна безпека держави».

Разова спеціалізована вчена рада ДФ 26.133.080 утворена наказом Київського столичного університету імені Бориса Грінченка виконавчого органу Київської міської ради (Київської міської державної адміністрації), місто Київ, від 27 лютого 2025 року №112, у складі:

Голови разової спеціалізованої вченої ради:

ГУЛАК Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Рецензенти:

КОРШУН Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка;

ЖДАНОВА Юлія Дмитрівна кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Офіційних опонентів:

ОПІРСЬКИЙ Іван Романович, доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп'ютерних технологій,

автоматики та метрології Національного університету «Львівська політехніка»;

СМІРНОВ Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Механіко-технологічного факультету Центральноукраїнського національного технічного університету.

На засіданні 15 квітня 2025 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології Абрамову Сергію Вадимовичу на підставі прилюдного захисту дисертації «Моделі і методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса» за спеціальністю 125 Кібербезпека.

Дисертацію виконано у Київському столичному університеті імені Бориса Грінченка виконавчого органу Київської міської ради (Київської міської державної адміністрації), місто Київ.

Науковий керівник: Соколов Володимир Юрійович, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Дисертацію подано у вигляді спеціально підготовленого рукопису Абрамова Сергія Вадимовича «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає пп. 6–9 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 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 року за

№155/30023. Дисертація Абрамова Сергія Вадимовича та наукові публікації, в яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності. Абрамов Сергій Вадимович на високому рівні оволодів методологією наукової та педагогічної діяльності, набув теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом. Здобувач вільно володіє матеріалом.

Основні результати дисертації висвітлено у 11 наукових публікаціях: 1 стаття у науковому виданні, включеному на дату опублікування до переліку наукових фахових видань України; 3 статті у періодичних наукових виданнях, проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection; 7 публікацій (з них 5 у співавторстві), у яких додатково відображено результати дисертації. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Наукові статті, опубліковані у періодичних наукових виданнях, проіндексованих у базах даних Scopus і Web of Science Core Collection

1. Bessalov, A., & Abramov, S. (2022). Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves. Cybernetics and Systems Analysis, 58(683), 851–861. 2022 https://doi.org/10.1007/s10559-023-00518-w (Scopus Q3)
2. Bessalov, V., & Abramov, S. (2023). PQC CSIKE Algorithm on Non-Cyclic Edwards Curves. Cybernetics and Systems Analysis, 59(6), 867–879. 2023 https://doi.org/10.1007/s10559-023-00622-x (Scopus Q3)
3. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. Cryptography, 8(3), 1–17. https://doi.org/10.3390/cryptography8030038 (Scopus Q2 &WoS)

У дискусії взяли участь голова і члени разової спеціалізованої вченої ради та висловили зауваження.

КОРШУН Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка; зауваження:

1. В постквантової криптографії існує багато криптоалгоритмів. Було б цікаво перевірити як розробки Абрамова С.В. можна було б застосувати до інших криптоалгоритмів і як це допоможе поліпшити їх якість.

2. В розділі 2 стверджується, що використання нециклічних кривих Едвардса приводить до подвоєння швидкодії або довжини секретного ключа. Варто було б більш детально пояснити механізм цього подвоєння

3. Метод обчислення ізогеній, який використовує автор є досить складним і тому було б доцільним докладніше його описати та навести алгоритми. Крім того, залишилося нез'ясованим, як саме скорочення діапазону ступенів ізогеній дає лінійну оцінку прискорення в 1,5 рази.

ЖДАНОВА Юлія Дмитрівна, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, зауваження:

1. У другому розділі роботи запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари. Втім не висвітлено механізм, який гарантував би рівномірність вибору та унеможливлював передбачення

2. В побудованій моделі інкапсуляції ключа CSIKE було б доцільним вказати розподіл ймовірностей, який може бути використаний для рандомізації ступеня ізогенії на кожному кроці ланцюжка ізогеній

3. В опису методу CRS та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса стверджується, що замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до НКЕ породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Проте не вказано, як саме відбувається це породження і як визначається їх незалежність.

СМІРНОВ Олексій Анатолійович, доктор технічних наук, завідувач кафедри кібербезпеки та програмного забезпечення Механіко-технологічного

факультету Центральноукраїнського національного технічного університету, зауваження:

1. У постквантовому середовищі існує досить багато типів криптосистемі, резистентних до квантових атак. Порівняння їх з розробками дисертанта значно підвищили би наукову цінність роботи

2. У загальному вигляді крива Едвардса має два параметри a та d, але у роботі криві ідентифікуються тільки параметром d, а параметр a майже не використовується. Це певним чином порушує строгість подання цього питання і потребує обґрунтування.

3. В методі удосконалення обчислення ізогеній відбувається заміна обчислення ізогенних функцій $\varphi(R)$ на обчислення параметра d. Варто було б детальніше пояснити, як саме відбувається така заміна.

ОПІРСЬКИЙ Іван Романович, доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка», зауваження:

1. Автор пропонує використовувати замість одної циклічної повної кривої Едвардса дві нециклічні кривих з випадковим вибором однієї з кривих пари. Доцільно було б дослідити, яким чином використання двох нециклічних кривих впливає на безпеку криптосистеми у порівнянні з використанням однієї циклічної кривої.

2. Автор створив ряд методів та перевірив їх на моделях. Але дослідження набуло б більшого науково-практичного значення, якби дисертант довів ці методи та принципи до стану стандартизації.

3. Важливою характеристикою криптосистем є стійкість до різних атак. Але у роботі розглядається тільки один вид атак – атаки побічними каналами. Було б варто дослідити уразливість і до інших атак та провести порівняльний аналіз стійкості до криптоаналізу між запропонованими системами та класичними алгоритмами.

Результати відкритого голосування:

«За» – 5 членів ради,

«Проти» – немає.

На підставі результатів відкритого голосування разова спеціалізована вчена рада ДФ 26.133.080 присуджує АБРАМОВУ Сергію Вадимовичу ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої
вченої ради ДФ 26.133.080 Геннадій ГУЛАК