В І Д Г У К

офіційного опонента

Смірнова Олексія Анатолійовича

на дисертацію Охріменка Андрія Олександровича

на тему «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань»,

представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Детальний аналіз дисертації Охріменка А.О. «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань» дозволяє сформулювати наступні узагальнені висновки щодо актуальності, ступеня обґрунтованості основних наукових положень, висновків, рекомендацій, достовірності наукової новизни, практичного значення, а також загальної оцінки роботи.

Актуальність теми дисертації. Процес впровадження цифрових технологій в усі сфери суспільного життя значно прискорився в останні роки в Україні та світі. Все більше державних послуг стали надаватись в електронній формі, все більше і більше громадян отримують послуги з використанням електронного підпису. Крім того, поширення систем електронного документообігу, електронної звітності, систем віддаленої ідентифікацій неможливо уявити без електронного підпису. Це призводить до збільшення кількості електронних документів та збільшення навантаження на інфраструктуру надавачів електронних довірчих послуг, що може негативно вплинути на швидкість обробки запитів чи навіть спричинити відмову в обслуговуванні. Оскільки, до надавачів електронних довірчих послуг висуваються жорсткі вимоги по надійності та доступності, то уникнути подібних сценаріїв можна або за рахунок постійної модернізації обчислювальної інфраструктури або шляхом підвищення ефективності криптографічних перетворень, що лежать в основі роботи операцій з електронним підписом. Підвищення швидкодії

криптографічних перетворень можливе, зокрема, за рахунок розробки та удосконалення методів арифметичних перетворень в полях і кільцях цілих чисел, що використовують особливості та можливості сучасних апаратних та програмних засобів.

Таким чином, вищезазначене обумовлює актуальність і наукову новизну дисертаційної роботи Охріменка А.О.

Окрім того, актуальність дисертаційної роботи також підтверджується тим, що тематика та одержані автором результати безпосередньо пов'язані з Постановою Президії Національної академії наук України №30 затвердженої 30.01.2019 р. «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019-2023 роки» та відповідають науковим напрямам в області «1.2. Інформатика». Дисертаційне дослідження пов'язане 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 «Horizon Europe». Результати роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету «Квантово-криптографічні методи захисту критичної інформаційної інфраструктури держави» (0117U006770) та «Система забезпечення конфіденційності критичної інформаційної інфраструктури держави на базі квантових детерміністичних протоколів» (д.р. № 0120U101400), у яких здобувач брав участь у якості виконавця.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків щодо основних результатів роботи, списку використаних джерел та додатків.

У **вступі** автором представлена загальна характеристика роботи, обґрунтована актуальність, сформульовані мета і задачі досліджень, відображені наукова новизна і практична цінність отриманих результатів, наведено дані про їх апробації та впровадження.

У **першому розділі** проведено аналіз вітчизняної та іноземної наукової літератури та нормативно-правових актів за темою дисертаційного дослідження. Розглянуто особливості побудови національної інфраструктури відкритих ключів України, стандарти електронного підпису, що використовуються в ній, та математичні основи, що лежать в основі криптографічних перетворень з відкритим ключем. Розглянуто особливості представлення цілих чисел та проведено аналіз арифметичних перетворень над ними, що використовуються в сучасній криптографії та обробці сигналів.

Другий розділ присвячений розробці методу представлення цілих чисел з відкладеним переносом, а також удосконаленню методів арифметичних перетворень для роботи з числами у цьому представленні. Проведений аналіз представлень цілих чисел та операцій цілих чисел показали, що операція врахування переносів при виконанні арифметичних операцій негативно позначається на їх ефективності. Використання запропонованого методу представлення цілих чисел дозволяє відкласти операцію переносу чи займу та виключити залежність між машинними словами при виконанні арифметичних перетворень, що в свою чергу призводить до підвищення швидкодії криптографічних перетворень. Наводяться удосконалені методи арифметичних перетворень з числами в представленні з відкладеним переносом та оцінка їх обчислювальної складності – більшість методів мають нижчу обчислювальну складність, ніж їх прототипи.

У **третьому розділі** розглядається удосконалення методів арифметичних перетворень множення, піднесення до квадрату та приведення за модулем з відкладеним переносом за рахунок використання двох різних підходів до розпаралелювання – паралельне виконання двох циклів множення та паралельне

виконання ітерацій двох циклів множення. Саме завдяки використанню відкладеного переносу можливе удосконалення методів арифметичних перетворень з застосуванням розпаралелювання. Наводиться оцінка обчислювальної складності удосконалених методів арифметичних перетворень.

У **четвертому розділі** приводиться методика експериментального дослідження та результати експериментальних досліджень, що були отримані на сучасних апаратних та програмних засобах. Результати експериментальних досліджень методів арифметичних операцій в кільці цілих чисел, в полі простих чисел GF(p), в групі точок еліптичної кривої над простим полем GF(p), в криптосистемі ECDSA над простим полем GF(p), в криптосистемі RSA свідчать про ефективність запропонованих та удосконалених автором методів.

У **висновках** стисло сформульовано основні отримані автором наукові та практичні результати дисертаційної роботи.

У **додатках** розміщено акти впровадження дисертаційної роботи, що підтверджують практичну цінність дисертаційного дослідження. Також, в додатках наведено результати багаточисельних експериментальних досліджень розроблених та удосконалених автором методів (а саме, методів арифметичних операцій: над цілими числами, в кільці цілих чисел, в полі простих чисел GF(p), в групі точок еліптичних кривих над простим полем GF(p), в криптосистемі ECDSA над простим полем GF(p), в криптосистемі ДСТУ 4145-2002 над двійковим полем $GF(2^m)$, в криптосистемі RSA), що були проведені автором роботи, які демонструють практичну направленість роботи.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Наукові положення та висновки, представлені автором, є повністю обґрунтованими, а достовірність теоретичних положень підтверджується коректним застосуванням відомого математичного апарату, експериментальними даними та результатами верифікації запропонованих методів, а також

впровадженням в практичну діяльність, що підтверджена відповідними актами впровадження.

Новизна отриманих результатів дисертаційної роботи, полягає у наступному:

– *вперше розроблено* метод представлення цілих чисел з відкладеним переносом, який за рахунок можливості відкласти операцію переносу зі старших розрядів в молодші та операцію займу з молодших розрядів у старші, дозволяє виключити взаємозалежність між машинними операціями при виконанні арифметичних перетворень та в свою чергу підвищити швидкодію криптографічних перетворень з відкритим ключем.

– *удосконалено* методи арифметичних перетворень додавання, віднімання, зсуву вліво, зсуву вправо, множення, піднесення до квадрату, приведення за модулем, ділення та порівняння, які за рахунок використання цілих чисел в представленні з відкладеним переносом дозволяють підвищити швидкодію перетворень в полях та кільцях цілих чисел, що в свою чергу призводить до підвищення швидкодії криптографічних перетворень з відкритим ключем.

– *удосконалено* методи арифметичних перетворень множення, піднесення до квадрату та приведення за модулем великих цілих чисел з відкладеним переносом та паралельним виконанням двох циклів множення в двох окремих потоках, що дозволяє підвищити швидкодію криптографічних перетворень з відкритим ключем.

– *удосконалено* методи арифметичних перетворень множення, піднесення до квадрату та приведення за модулем великих цілих чисел з відкладеним переносом та паралельним виконанням ітерацій двох циклів множення в декілька потоків, що дозволяє підвищити швидкодію криптографічних перетворень з відкритим ключем.

Практична значимість полягає у тому, що автором вирішено актуальну науково-практичну задачу підвищення якості обслуговування клієнтів центрів сертифікації ключів, за рахунок зменшення часу обробки запитів сервісами OCSP та TSP за допомогою зменшення часу виконання криптографічних перетворень електронного підпису. Робота практично направлена: удосконалено велику

кількість методів арифметичних перетворень, що в свою чергу дає можливість підвищити швидкодію криптографічних перетворень різних криптосистем, крім того автором розроблено та отримано п'ять патентів України на корисну модель, а саме «Спосіб множення цілих чисел» (Патент 111632, опубліковано 26.11.2016, бюлетень № 22), «Спосіб піднесення до квадрату цілих чисел» (Патент 118065, опубліковано 25.07.2017, бюлетень № 14), «Спосіб приведення за модулем цілих чисел» (Патент 118065, опубліковано 25.07.2017, бюлетень № 14), «Спосіб криптографічного перетворення інформації з використанням подовжених кодів» (Патент 123375, опубліковано 26.02.2018, бюлетень №4), «Спосіб криптографічного перетворення інформації з використанням укорочених кодів» (Патент 123379, опубліковано 26.02.2018, бюлетень №4).

Розроблені та удосконалені методи арифметичних перетворень реалізовано у бібліотеках криптографічних примітивів «Шифр+ v.2.1» системи криптографічного захисту інформації «Шифр-X.509» ТОВ «Сайфер ЛТД», що має дійсний позитивний експертний висновок Держспецзв'язку України від 16.05.2017 № 04/03/02-1674 (Акт № 22/17 від 04.08.2017 р.). Результати дисертаційних досліджень впроваджено у діяльність Кваліфікованого надавача електронних довірчих послуг Офісу Генерального прокурора України (Акт №18\10\2-8654-19 від 08.10.2020 р.) та Національного авіаційного університету (Акт від 25.09.2020 р.).

Відповідність змісту автореферата дисертації. Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі і задовольняє встановленим вимогам.

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

Основні результати роботи опубліковані в 36 наукових працях, у тому числі – 3 колективних монографіях, 16 наукових статях (5 – у міжнародних рецензованих виданнях, що входять до бази даних SCOPUS, 9 – у вітчизняних фахових наукових журналах та 2 – у інших наукових виданнях), 5 патентів України на корисну модель, а також 12 матеріалів і тез доповідей на конференціях, що повністю задовольняє

чинні вимоги МОН України до кандидатських дисертацій. Основні положення дисертаційної роботи пройшли обов'язкову апробацію на міжнародних конференціях.

Недоліки та зауваження.

1. В роботі представлені результати експериментальних досліджень для 4 сучасних апаратних платформ, проте не обґрунтовується їх вибір.
2. В 4 розділі не вистачає графічного представлення отриманих результатів експериментальних досліджень, що дозволило б спростити їх аналіз.
3. Використання запропонованого методу представлення чисел з відкладеним переносом та удосконалених методів арифметичних перетворень не обмежуються лише криптографією і можуть використовуватись і в інших галузях, проте на цьому не акцентується увага.
4. При аналізі методів представлення цілих чисел одним з аргументів проти існуючих методів була обмеженість сфери використання деяких представлень, проте представлення з відкладеним переносом також не є універсальним і має свої обмеження.
5. У якості прототипу для методу множення вибрано метод Комба, а в якості алгоритму приведення за модулем – метод Баррета, проте не пояснюється чи можливо використання представлення цілих чисел з відкладеним переносом в інших методах множення та приведення за модулем, які також використовуються в криптографії.
6. З тексту роботи та результатів експериментального дослідження не зрозуміло в яких випадках і за яких умов краще застосовувати удосконалені методи арифметичні перетворенням з одним підходом до розпаралелювання, а в яких випадках з іншим.

Проте, слід зазначити, що наведені зауваження та недоліки не є принциповими та суттєво не впливають на загальне позитивне враження від роботи, не знижують її якість, наукову цінність чи практичне значення.

Загальні висновки. Загалом дисертаційна робота Охріменка Андрія Олександровича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку теорії й практики криптографічних алгоритмів, що у подальшому можуть використовуватися для підвищення ефективності сучасних систем захисту інформації.

Вважаю, що дисертаційна робота «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань» повністю відповідає вимогам МОН України, а її автор Охріменко Андрій Олександрович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент

Завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор О.А. Смірнов

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи
Центральноукраїнського національного технічного університету,
доктор економічних наук, професор О.М. Левченко
“____” _____ 2020 року