Ученому секретарю
спеціалізованої вченої ради Д 26.062.17
при Національному
авіаційному університеті

03680, м. Київ, пр. Любомира Гузара, 1

ВІДГУК

офіційного опонента, професора кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна доктора технічних наук, професора Кузнецова Олександра Олександровича на дисертацію Охріменка Андрія Олександровича «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

1. Актуальність теми дисертації

На сьогоднішній день в Україні створено, уведено в дію та ефективно функціонує національна система електронного підпису, що надає послуги з виготовлення та обслуговування сертифікатів відкритих ключів декільком мільйонам користувачів. Широке застосування електронних довірчих послуг здійснюється у ЄС, США, інших розвинутих країнах, завдяки чому суттєво поліпшено виконання електронних операцій на цифрових електронних ринках та у державному управлінні.

Слід зазначити, що практичний досвід експлуатації систем електронного підпису демонструє зростання навантаження на діючу інфраструктуру. Це пов'язано як зі збільшенням кількості користувачів системи, так і з інтенсифікацією інформаційного обміну, впровадженням систем електронного документообігу, електронних платежів та інших електронних сервісів. Підвищується кількість звернень до всіх складових національної системи електронного підпису та, як наслідок, виникає загроза відмови в обслуговуванні або стрімкої деградації якості надання електронних довірчих послуг.

Таким чином, підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів національної інфраструктури відкритих ключів є важливою та актуальною задачею вдосконалення технічних засобів і програмно-математичних комплексів, що застосовуються у різних складових системи.

Одним із шляхів вирішення протиріччя між підвищеними вимогами до швидкості перетворень зі встановленими рівнями безпеки та сучасними можливостями діючої інфраструктури є удосконалення спеціального

програмного та математичного забезпечення в частині удосконалення методів арифметичних перетворень над великими цілими числами для криптографічних застосувань. Саме цей напрямок досліджень розвинуто в дисертації Охріменка А.О. Тема роботи «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань» є важливою та актуальною, тісно пов'язаною з виконанням завдань та положень, визначених Стратегією кібербезпеки України та законами України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги» тощо.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

У вступі дисертації наведено відомості щодо актуальності теми дисертаційної роботи, її зв'язок з науковими програмами, планами, темами, наголошено мету та задачі дослідження, сформульовано об'єкт та предмет, описано методи дослідження, наголошено наукову новизну результатів роботи та їх практичну значимість, наведено відомості щодо публікації, апробації, особистого внеску автора до спільних публікацій. Закінчується вступ короткою інформацією щодо структури роботи та її обсягів.

2.1. У першому розділі дисертаційної роботи проаналізовано особливості функціонування національної інфраструктури відкритих ключів, досліджено використання цілих чисел в криптографічних перетвореннях та методи їх представлення, проведено аналіз арифметичних перетворень з цілими числами в двійковому представлені.

Автор докладно аналізує кількість власників сертифікатів електронного підпису, структуру національної інфраструктури відкритих ключів, встановлені процедури сертифікації тощо. За результати аналізу автор упевнено доходить висновку стосовно необхідності оптимізації обчислень, що виконуються центрами сертифікації ключів. Далі автор аналізує математичні перетворення та базові арифметичні операції, що виконуються криптографічними алгоритмами. У висновках за розділом наголошено на результатах проведеного аналізу та зконцентровано увагу на меті подальших досліджень.

Головним **недоліком** цього розділу є переобтяженість загальновідомими положеннями та відомостями, зокрема викладення алгоритмів базових арифметичних обчислень треба було віднести до додатків.

2.2. У другому розділі досліджено представлення цілих чисел з відкладеним переносом (перетворення двійкового числа у нове, запропоноване автором DCF представлення; перетворення DCF числа у двійкове представлення), операції з числами в DCF представленні (додавання; зсув; множення; піднесення до квадрату; приведення за модулем; ділення; порівняння інше). Фактично, в цьому розділі автор вводить всі необхідні в

подальшому математичні визначення, означення, базові арифметичні перетворення у веденій формалізації, описує мовою алгоритмів окремі методи обчислень та ілюструє ці алгоритми наочними діаграмами. Розділ легко читається, змістовна частина сприймається однозначно, всі математичні викладення прозорі. На мою думку, автору вдалося систематизувати відомі підходи до оптимізації арифметичних обчислень при поданні вихідних даних у бінарному вигляді через введення додаткових бітів даних, виділених під перенос. Крім того, в дисертації через узагальнення відомих результатів та власного досвіду створення великих програмних продуктів зі складними обчисленнями запропоновано оригінальне подання алгоритмів оптимізації арифметичних обчислень.

Недоліки та зауваження:

- в цьому розділі автором описано 18 (!) нових методів арифметичних перетворень. І хоча в констатуючій частині дисертації новизну цих методів скромно позначено як «удосконалено», не можна погодитися з авторським визначенням «методу». Зазначені результати правильно номінувати алгоритмами, бо вони представляють конкретну послідовність кроків (або інструкцій), що описують порядок дій для досягнення певного результату, рішення обчислювальної задачі за кінцевий час. Методом є сукупність зазначених алгоритмів та, насамперед, ведених способів подання чисел через виділення окремої частки бітів під переноси, введені моделі та формалізації цих перетворень тощо. Описані 18 обчислювальних алгоритмів є по суті практичним втіленням нових прийомів та операцій з оптимізації арифметичних обчислень. На мій погляд перший та другий науковий результат, зазначені в авторефераті, слід об'єднати, оскільки йдеться про окремі частини одного наукового результату;
- з точки зору категорії новизни методу (удосконалено) можна погодитися з автором дисертації. Але за текстом бракує послідовного та еволюційного викладення цього удосконалення. Звісно, що більшість переносів в арифметичних обчисленнях зазвичай керується відповідними прапорцями (як програмно, так і апаратно), але при оптимізації виконання конкретної обчислювальної програми можуть застосовуватися й інші підходи. Внесення надмірності до оброблювання даних для переносів – звичайна річ, цей прийом застосовувався раніше та буде застосовуватися у подальшому. Автору слід було обов'язково вказати про це, навести приклади, систематизувати та узагальнити їх, і, на підставі цих відомостей, ввести своє тлумачення обчислювальної оптимізації, її формалізацію і т.і. Наразі, за дійсним текстом дисертації виглядає так, що автор запропонував новаторське рішення, яке згодом змінить всі діючі системи обчислень та, загалом, всю архітектуру мікропроцесорної техніки. Звісно, що це не так, адже йдеться лише про оптимізацію арифметичних обчислень для дуже вузького класу задач з підходящими вихідними умовами та обмеженнями;

- у продовження попереднього недоліку слід вказати, що для запропонованих методів (насправді алгоритмів) існує певний діапазон параметрів, щодо яких присутній виграш в швидкості обчислень. І цей діапазон, а точніше, повний перелік умов та вимог до застосування і повинен бути основним предметом дослідження автора. Наявна оптимізаційна задача, яку автор повинен був сформулювати та вирішити. На жаль, в цьому розділі є тільки опис алгоритмів, без дослідження їх ефективності та застосовуваності, бракує обґрунтування умов та вимог до практичного використання методу і це головний недолік розділу;
- висновки за розділом подано у вигляді анотацій здобутих результатів.

2.3. Третій розділ дисертації присвячено дослідженню підходів до розпаралелювання окремих арифметичних операцій з відкладеним переносом, зокрема, автором досліджуються методи множення, піднесення до квадрату, приведення за модулем. Автор застосовує той же прийом, що й в попередньому розділі, а саме викладає відомі методи оптимізації арифметичних обчислень але із застосуванням введеної ним формалізації щодо виділення бітів під переноси. Загалом розділ містить опис низки обчислювальних алгоритмів, які дозволяють розпаралелити виконання окремих операцій із відкладеним переносом.

Недоліки та зауваження:

- автором пропонується 9 методів, які знов краще назвати обчислювальними алгоритмами (як і в зауваженнях до другого розділу). Ці дев'ять обчислювальних алгоритмів у сукупності зі способом подання арифметичних операцій з відкладеним переносом та операцій розпаралелювання складають один науковий результат (третій з перерахованих в авторефераті);
- автором розглядається лише один маловідомий метод множення Comba, щодо якого й отримано більшість результатів. Але відомі й інші, більш ефективні методи множення, про які згадано в першому розділі дисертації й у авторефераті, наприклад, Карацуби-Офмана, Тоома-Кука, Шенхаге-Штрассена, Фюрера тощо. Звичайно, що формалізація кожного методу у введених означеннях з виділенням окремих бітів на перенос є трудомістким завданням, але в дійсній редакції дисертації неможливо переконатися в тому, що обраний варіант множення є найкращим. Це, як на мене, головний недолік другого розділу дисертації;
- висновки за розділом подано у вигляді анотацій здобутих результатів.

2.4. У четвертому розділі дисертації проводяться експериментальні дослідження розроблених у попередніх розділах методів та обчислювальних алгоритмів. Автор спочатку викладає методику проведення експериментальних досліджень (підрозділ 4.1), потім докладно викладає окремі результати дослідження швидкодії арифметичних операції над цілими числами, в кільцях, полях, групах точок еліптичної кривої тощо. Результати подано, переважно, у вигляді таблиць з нормалізованими показниками швидкодії. Найбільшу

кількість таблиць з результатами винесено до додатків. Результати сприймаються легко, таблиці не переобтяжено, обрані показники та критерії для порівняння є зрозумілими та логічними.

Недоліки та зауваження:

- в підрозділі 4.1 «Методика проведення експерименту» бракує змістовної частини. Зазвичай планування експерименту проводиться для забезпечення бажаної точності та вірогідності результатів при мінімізації витрат часу та ресурсів на проведення експерименту. На жаль, автор дисертації не демонструє знання з теорією планування експерименту. Отже, про точність та вірогідність отриманих результатів в дисертації зовсім не йдеться. Тому, на мій погляд, більшість наведених результатів експериментів слід сприймати як набір точкових оцінок, які хоча й дають загальне уявлення про поведінку зазначених параметрів, але не можуть бути підставою для об'єктивних суджень (з відповідним ступенем довіри). І це головний недолік експериментальної частини роботи;
- в таблицях змістовної частини розділу наводяться діапазони значень, тобто автор намагався дати інтервальну оцінку результатів експериментів. Але спосіб її отримання та, насамперед, точність і вірогідність цієї оцінки невідомі;
- в таблицях додатків наводяться точкові оцінки, виділені кольором (червоним – при погіршенні відомого результату, зеленим – при покращенні). Це надзвичайно важливі та цікаві результати, за якими, бодай емпіричним шляхом, можна було б визначити (чи хоча б спробувати) перелік умов та вимог, щодо яких присутній виграш в швидкості обчислень. Але автором цього не зроблено. Це завдання не вирішено в другому розділі аналітичним шляхом та не підтверджено емпіричним шляхом в четвертому.

В висновках по роботі наголошено на здобутих результатах та їх впровадженні у діяльність ТОВ «Сайфер ЛТД», Національного авіаційного університету та Кваліфікованого надавача електронних довірчих послуг Офісу Генерального прокурора.

3. Достовірність отриманих результатів

Достовірність отриманих результатів обґрунтовується їх несуперечністю основним положенням теорії захисту інформації, математичного апарату теорії складності алгоритмів, теорії чисел, теорії груп, полів, кілець, прикладної криптології, методів математичного та комп'ютерного моделювання, теорії ймовірностей та математичної статистики. Достовірність підтверджується збіжністю отриманих точкових оцінок в результаті експериментальних досліджень з теоретичними результатами та аналітичними співвідношеннями.

4. Новизна отриманих результатів

У дисертаційній роботі Охріменка А.О. «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань» отримано теоретичне узагальнення та нове вирішення актуальної науково-прикладної задачі, яка полягає в розробці методів арифметичних перетворень над великими цілими числами з відкладеним переносом для підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів національної інфраструктури відкритих ключів.

Отримано такі **науково обґрунтовані результати**.

- метод представлення цілих чисел з відкладеним переносом та обчислювальні алгоритми арифметичних перетворень додавання, віднімання, зсуву вліво, зсуву вправо, множення, піднесення до квадрату, приведення за модулем, ділення та порівняння;
- метод та обчислювальні алгоритми арифметичних перетворень множення, піднесення до квадрату та приведення за модулем великих цілих чисел з відкладеним переносом та паралельним виконанням циклів множення в окремих потоках;
- метод та обчислювальні алгоритми арифметичних перетворень множення, піднесення до квадрату та приведення за модулем великих цілих чисел з відкладеним переносом та паралельним виконанням ітерацій в декілька потоків.

5. Завершеність, стиль викладення, публікації

5.1. Аналіз сукупності наукових результатів і положень, характеристику яких наведено в пп. 2-4, дозволяє зробити висновок про їх внутрішню єдність і засвідчує особистий внесок автора у науку. У дисертаційній роботі отримано розвиток методів арифметичних перетворень над великими цілими числами з відкладеним переносом для підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів національної інфраструктури відкритих ключів.

5.2. Дисертація є завершеною науковою роботою, виконаною й оформленою відповідно до встановлених вимог.

5.3. Дисертаційну роботу написано зрозуміло, науково-технічна термінологія використовується коректно, структура роботи є логічною.

5.4. Основні результати досліджень опубліковані досить повно у в 36 наукових публікаціях: 16 наукових статей (5 – у міжнародних рецензованих виданнях, що входять до баз даних Scopus та 9 – у вітчизняних фахових наукових журналах та 2 – у інших наукових виданнях), 3 розділи колективної монографії, 5 патентів України на корисну модель, 12 матеріалів та тез доповідей.

5.5. Структура і зміст автореферату повністю відповідають тексту дисертації.

6. Практична значимість

6.1. В дисертаційній роботі розроблено спеціальне програмне та математичне забезпечення та практичні рекомендації щодо впровадження отриманих наукових та практичних результатів, зокрема:

- Удосконалено обчислювальні алгоритми арифметичних перетворень: множення великих цілих чисел з відкладеним переносом; з використанням відкладеного переносу та паралельним виконанням двох циклів множення в двох окремих потоках; відкладеного переносу та паралельним виконанням ітерацій двох циклів множення в декілька потоків;
- Удосконалено обчислювальні алгоритми арифметичних перетворень у кільці цілих чисел, у простому полі цілих чисел, у групі точок еліптичної кривої над простим полем, у криптосистемі ECDSA, у криптосистемі RSA;

6.2. Зазначені результати підтверджені та захищені авторським правом (отримано п'ять патентів України на корисну модель).

6.3. Отримані результати реалізовано у бібліотеках криптографічних примітивів «Шифр+ v.2.1» системи криптографічного захисту інформації «Шифр-X.509» ТОВ «Сайфер ЛТД», що має експертний висновок Держспецзв'язку України від 16.05.2017 № 04/03/02-1674, Акт № 22/17 від 04.08.2017 р. (https://cipher.com.ua/uk/products/cipher-plus-version-2-1).

6.4. Результати дисертації впроваджено у діяльність ТОВ «Сайфер ЛТД», Національного авіаційного університету та Кваліфікованого надавача електронних довірчих послуг Офісу Генерального прокурора.

7. Недоліки та зауваження

Основні недоліки та зауваження викладено при аналізі наукових результатів дисертанта (п.2).

До недоліків також слід додати певні вади змістовної частини автореферату. Наприклад, тотожна змістовна частина міститься в різних розділах автореферату. Зокрема, ті самі результати з нормалізованими показниками швидкодії подано тричі (у загальній характеристиці роботи, в розділі 4 основної частини та у висновках).

Але вищеозначені недоліки та зауваження не впливають на загальний позитивний висновок про дисертаційну роботу. Дослідження носить яскраво виражену практичну спрямованість, більшість з отриманих результатів є оригінальними та корисними напрацюваннями автора, які вже впроваджено до діючих інформаційних систем. Отриманий корисний ефект виявляється в прискоренні програмно-технічних комплексів інформаційно-телекомунікаційних систем центрів сертифікації ключів національної інфраструктури відкритих ключів, що є безумовно важливим та актуальним, особливо в контексті постійного зростання обчислювального навантаження на діючу інфраструктуру.

8. Загальні висновки

8.1. Дисертація є закінченою науково-дослідною роботою, яка містить теоретичне узагальнення та нове рішення актуальної науково-прикладної задачі, яка полягає в розробці методів арифметичних перетворень над великими цілими числами з відкладеним переносом для підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів національної інфраструктури відкритих ключів.

8.2. Зміст дисертації відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

8.3. Дисертаційна робота Охріменко А.О. «Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань» має певну наукову новизну і практичну значимість у галузі безпеки інформаційних технологій, відповідає вимогам п. 9, 11-14 "Порядку присудження наукових ступенів", а її автор заслуговує присудження наукового ступеня кандидата технічних наук.

Професор кафедри безпеки інформаційних систем і технологій
Харківського національного університету імені В.Н. Каразіна
доктор технічних наук, професор

О.О. КУЗНЕЦОВ

"12" 11 2020 р.

Підпис доктора технічних наук,
професора КУЗНЕЦОВА О.О. засвідчую.

Підпис засвідчую
Начальник служби управління
персоналом