Голові спеціалізованої вченої ради
ДФ 64.051.019
Харківського національного
університету імені В. Н. Каразіна
61022, м. Харків, майдан Свободи, 4

ВІДГУК

офіційного опонента, завідувача кафедри обчислювальної техніки та програмування факультету комп'ютерних та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут», доктора технічних наук, професора Семенова Сергія Геннадійовича на дисертаційну роботу **Родінко Марії Юріївни «Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів»**, подану на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки

Актуальність теми дисертаційної роботи.

Протягом багатьох років основними криптографічними примітивами, які використовуються для забезпечення конфіденційності в інформаційно-комунікаційних системах, є симетричні блокові шифри. Безперервний розвиток інформаційних технологій (зокрема, зростання потужностей наявних обчислювальних ресурсів, розробка квантових комп'ютерів, поява і розповсюдження «розумних» пристроїв та Інтернету Речей) змінює вимоги до криптографічних примітивів, в тому числі, вимагаючи удосконалення вже існуючих і створення нових блокових шифрів.

Інтернет Речей представляє собою сукупність фізичних пристроїв, об'єднаних у мережу з метою виконання різних завдань. У процесі роботи ці пристрої передають інформацію, яка часто носить конфіденційний характер, а значить потребує захисту. Застосування у таких пристроях блокових шифрів, які зазвичай використовуються з метою забезпечення конфіденційності даних (наприклад, «Калина» або AES), знаходиться під питанням у зв'язку з обмеженнями по енергоспоживанню. Таким чином, виник новий напрям у криптографії під назвою «малоресурсна

криптографія», що включає розробку примітивів, направлених на використання у пристроях з обмеженою кількістю споживання енергії.

Багато сучасних робіт присвячено розробці та аналізу малоресурсних блокових шифрів, які забезпечують високу швидкість шифрування і компактну програмну та/або апаратну реалізацію. Втім, на сьогодні ще залишається багато невирішених актуальних задач, пов'язаних з малоресурсними блоковими алгоритмами. Зокрема, недостатньо зрозумілими є перспективи використання існуючих малоресурсних блокових шифрів у постквантовий період. Крім того, через особливості побудови малоресурсні шифри погано піддаються аналізу стійкості до різних атак, що дуже ускладнює розробку теорії криптоаналізу таких примітивів. При цьому, потреба у швидких, компактних та безпечних блокових шифрах постійно зростає. Враховуючи викладене, тема дисертаційної роботи є дуже актуальною.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій.

Здобувачем виконаний ретельний аналіз сучасних методів розробки і дослідження блокових шифрів, найперспективніші з яких покладено в основу власних досліджень. Представлені у роботі наукові результати і висновки є обґрунтованими, оскільки базуються на відомих положеннях теорії аналізу та синтезу симетричних блокових шифрів. При розробці власних моделей та методів використано сучасний математичний апарат. Припущення, які висуваються здобувачем в рамках запропонованих математичних моделей, мають теоретичне та експериментальне обґрунтування і не протирічать відомим результатам у предметній області.

Оцінка змісту дисертаційної роботи.

Дисертаційна робота складається з вступу, п'яти розділів, висновків, списку використаних джерел та п'яти додатків.

Перший розділ містить відомості щодо загальних принципів побудови сучасних блокових шифрів, видів циклових функцій та схем розгортання ключів, методів криптоаналізу блокових шифрів, зокрема, особливу увагу приділено диференційному криптоаналізу. Також розглядаються сучасні малоресурсні блокові шифри, підходи до їх розробки та існуючі проблемні питання. Визначені задачі досліджень, які необхідно розв'язати.

Другий розділ присвячений удосконаленню методу генерації підстановок з високими нелінійністю та алгебраїчним імунітетом. У розділі наведено опис удосконаленого методу та результати його застосування, зокрема, приклади згенерованих підстановок з нелінійністю 104 та алгебраїчним імунітетом 3.

Третій розділ присвячений оцінці колізійних властивостей неін'єктивних схем розгортання ключів блокових шифрів. Представлена математична модель, в рамках якої отриманий вираз для обчислення ймовірності співпадіння двох послідовностей циклових ключів.

Четвертий розділ присвячений побудові та оцінці диференційних властивостей перспективного ARX-перетворення. Зокрема, розроблений малоресурсний ARX-шифр «Кипарис» та запропоновано методи пошуку одноциклових та багатоциклових диференційних характеристик для такого типу шифрів.

П'ятий розділ містить результати дослідження статистичних та лавинних властивостей розробленого шифру «Кипарис», а також порівняння його швидкодії з іншими відомими малоресурсними шифрами.

Додатки містять перелік публікацій здобувача, результати тестів NIST STS, проведених для шифру «Кипарис», вихідні коди програмної реалізації шифру «Кипарис» та методів пошуку його диференційних характеристик, а також акти впровадження результатів дисертаційної роботи.

Дисертаційна робота представляє собою цілісне, завершене дослідження, викладене логічно та зрозуміло. Зміст дисертації відповідає спеціальності 122 – Комп'ютерні науки. Робота оформлена відповідно до вимог наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій».

Наукова новизна отриманих результатів полягає в наступному:

1. **Вперше** запропоновано два методи пошуку одноциклових диференційних характеристик для визначеного класу ARX-шифрів, що дозволяють з низькою обчислювальною складністю отримувати оцінки стійкості циклової функції блокового шифру визначеного класу до диференційного криптоаналізу.

2. **Отримали подальший розвиток** методи пошуку багатоциклових диференційних характеристик для визначеного класу ARX-шифрів, що відрізняються вдосконаленим механізмом відбору вхідних різниць та

формуванням початкової множини одноциклових диференційних характеристик, що дозволяє отримати оцінку щодо стійкості повномасштабного блокового шифру визначеного класу до диференційного криптоаналізу.

3. **Удосконалений** метод градієнтного спуску для генерації нелінійних таблиць заміни, що відрізняється від відомого обґрунтованим оптимальним порядком застосування критеріїв при перевірці підстановок на відповідність криптографічним показникам, що дозволяє суттєво знизити складність генерації оптимальних S-блоків.

4. **Отримав подальший розвиток** математичний метод оцінки колізійних властивостей неін'єктивних схем розгортання ключів блокових шифрів, що відрізняється застосуванням вдосконаленої математичної моделі та більш ефективного математичного апарату та дозволяє отримати уточнену оцінку ймовірності колізії двох послідовностей циклових ключів.

Достовірність отриманих наукових результатів підтверджується коректним викладенням та доведенням наукових положень за допомогою відомого математичного апарату та ретельно проведених експериментів. Програмний код, що застосовувався для моделювання, написаний коректно. Усі теоретичні результати узгоджуються з отриманими експериментальними даними. Отримані результати пройшли апробацію на міжнародних конференціях.

Практичне значення наукових результатів.

Удосконалений метод генерації S-блоків дозволяє швидко генерувати оптимальні S-блоки на персональних комп'ютерах. Розроблений блоковий симетричний шифр «Кипарис» є швидким, компактним криптографічним примітивом, готовим до застосування. Практичне значення отриманих результатів підтверджується актами впровадження.

Повнота викладу в наукових публікаціях, що відповідають темі дисертації.

Основні результати дисертації опубліковані у 23 наукових працях, а саме: у розділі монографії, опублікованому у співавторстві, та статті у науковому виданні Словаччини, що входять до міжнародної наукометричної бази Scopus, 5 статтях у наукових фахових виданнях України, 2 статтях, що додатково висвітлюють результати дисертації, 2 патентах на винахід та 12

матеріалах наукових та науково-практичних конференцій. Отримані наукові результати повністю викладено у публікаціях.

Відсутність порушення академічної доброчесності.

Представлені у дисертації наукові результати є новими та отримані здобувачем самостійно. Дисертаційна робота не містить плагіату та порушення вимог академічної доброчесності.

Зауваження та дискусійні питання. До дисертаційної роботи є наступні зауваження.

1. У розділі 2 сказано, що час генерації одного S-блока з оптимальними показниками на персональному комп'ютері становить приблизно 30 хвилин, проте не зазначено, на якому саме комп'ютері був отриманий цей результат. Доцільно було б навести характеристики цього комп'ютера (модель і тактова частота процесора, об'єм оперативної пам'яті), а також провести експерименти на комп'ютерах з різними характеристиками та порівняти отримані результати.
2. У розділі 4 (стор. 89) запропоновані певні константи для значень циклічних зсувів у цикловій функції шифру «Кипарис», але не обґрунтовано, чому було обрано саме такі значення.
3. У розділі 4 доцільно було б описати деталі експерименту з пошуку найбільш ймовірних багатоциклових диференційних характеристик шифру «Кипарис», наприклад, зазначити, скільки часу зайняв пошук найкращої знайденої диференційної характеристики.
4. У розділі 4 доцільно було б порівняти стійкість шифру «Кипарис» до диференційного криптоаналізу на різних циклах шифрування зі стійкістю інших відомих малоресурсних блокових шифрів.
5. Доцільно було б оцінити складність апаратної реалізації малоресурсного блокового шифру «Кипарис».

Загальні висновки.

Дисертаційна робота Родінко Марії Юріївни «Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів» є завершеним науковим дослідженням, результати якого мають важливе значення для розвитку теорії аналізу та синтезу малоресурсних симетричних примітивів.

Зміст роботи відповідає спеціальності 122 – Комп'ютерні науки та вимогам наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій» і «Тимчасового порядку присудження ступеня доктора філософії» (постанова Кабінету Міністрів України від 06.03.2019 р. № 167 зі змінами), а її автор Родінко Марія Юріївна заслуговує на присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

Офіційний опонент:
завідувач кафедри обчислювальної
техніки та програмування факультету
комп'ютерних та інформаційних технологій
Національного технічного університету
«Харківський політехнічний інститут»,
доктор технічних наук, професор Сергій СЕМЕНОВ

Підпис Сергія СЕМЕНОВА
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
Заковоротний О.Ю.
06 08 2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *