**Кирилащук Т.Г.**

**Соловей В.С.**

# Покращений криптоаналіз SIMON і SPECK

Вінницький національний технічний університет

***Анотація***

*Ця робота аналізує полегшені блокові шифри SIMON та SPECK від АНБ. Для SIMON виведено замкнену формулу для кореляцій та диференціальних імовірностей його основного нелінійного перетворення φ(x)=x⊙S1(x) та детально описано його DDT/LAT. Для SPECK, зосередившись на модульному додаванні, переоцінено його властивості та розроблено прості алгоритми для оптимальних вихідних масок/різниць. Ці результати прискорюють криптоаналіз обох шифрів, зменшуючи складність лінійних та диференціальних атак, водночас пояснюючи їхню притаманну стійкість.*

***Ключові слова***: SIMON,SPECK,криптоаналіз, DDAT/LAT

***Abstract***

*This paper analyzes the NSA's lightweight block ciphers SIMON and SPECK. For SIMON, we derive a closed formula for the correlations and differential probabilities of its main nonlinear transformation φ(x)=x⊙S1(x) and describe its DDT/LAT in detail. For SPECK, focusing on modular addition, we re-evaluated its properties and developed simple algorithms for optimal output masks/differences. These results accelerate the cryptanalysis of both ciphers, reducing the complexity of linear and differential attacks while explaining their inherent robustness.*

**Keywords:** SIMON, SPECK, cryptanalysis, DDAT/LAT

## Вступ

У сучасному світі інформаційні технології щодня невпинно розвиваються, тому необхідність в ефективних та безпечних криптографічних рішеннях для пристроїв з обмеженими ресурсами (на кшталт IoT та вбудованих систем) стає більш актуальною, ніж будь-коли. Серед численних полегшених блокових шифрів, розроблених, зокрема, SIMON та SPECK, створені АНБ, виділяються своєю архітектурною простотою та високою продуктивністю. Їхня значна популярність у сфері інформаційних технологій підкреслює нагальність ретельного та поглибленого вивчення їхньої криптографічної стійкості, особливо до лінійного та диференціального криптоаналізу.

Мета цієї тези — не лише розширити теоретичне розуміння, але й надати практичні інструменти для аналізу SIMON та SPECK. Запропоновано нові формули та алгоритми, що здатні суттєво оптимізувати процес криптоаналізу та оцінки стійкості цих шифрів, сприяючи глибшому розумінню їхніх внутрішніх механізмів безпеки.

**Результати дослідження**

SIMON: Аналіз Квадратичного Перетворення

«Для шифру SIMON була приділена увага на його єдиній нелінійній операції — квадратичному перетворенню, еквівалентному φ(x)=x⊙S 1 (x). Основні результати включають :Аналітичний вираз для диференціальних імовірностей та квадратів кореляцій φ. Ця формула дозволяє точно обчислювати, як розподіляються різниці та кореляції через функцію φ, забезпечуючи чітку математичну основу для аналізу. Повне представлення DDT та LAT для φ: було систематизовано набори всіх припустимих вхідних/вихідних масок та різниць, зокрема, використовуючи псевдо-вісімкове представлення. Це

принципово змінює підхід до криптоаналізу: замість повного перебору ми можемо працювати лише з релевантними, допустимими значеннями, що суттєво знижує обчислювальну складність процесу.»[1]

SPECK: Властивості Модульного Додавання

«У сімействі блокових шифрів SPECK єдиною нелінійною операцією є додавання за модулем 2n. На основі існуючих досліджень лінійних та диференціальних властивостей цієї операції, було досягнуто наступні результати:

Переформулювання формул для квадратичних кореляцій та диференціальних імовірностей модульного додавання: Було надано чіткі формули для обчислення квадратичної кореляції та диференціальної імовірності для модульного додавання. Ці формули ґрунтуються на аналізі бітових послідовностей, що утворюються комбінаціями вхідних масок/різниць та вихідних масок/різниць.»[2]

«Прості алгоритми для знаходження оптимальних вихідних масок та різниць: Запропоновано конкретні алгоритми для знаходження вихідних масок з максимальною квадратичною кореляцією, а також вихідних різниць з максимальною диференціальною імовірністю за заданими вхідними різницями та масками. Ці алгоритми використовують структурований підхід, аналізуючи "блоки" та "символи" у бітовому представленні вхідних даних, що дозволяє систематично конструювати оптимальні вихідні значення. Це усуває необхідність перебору та перевірки, значно прискорюючи пошук оптимальних шляхів.

Оптимізація криптоаналізу SPECK: Як і у випадку з SIMON, запропоновані алгоритми суттєво зменшують складність пошуку лінійних та диференціальних характеристик для SPECK. Це дозволяє криптоаналітикам швидше ідентифікувати слабкі місця або, навпаки, підтвердити міцність шифру.»[3]

## Висновки

Після дослідження було отримано важливі інструменти для аналізу безпеки полегшених блокових шифрів SIMON та SPECK. Завдяки розробці аналітичних виразів та алгоритмів для їх ключових нелінійних компонентів, ми досягли значного прискорення пошуку лінійних та диференціальних характеристик, а отже, зменшили складність відповідних криптоаналітичних атак.

Крім того, результати висвітлюють фундаментальні причини стійкості цих шифрів до класичних методів криптоаналізу: це є значною мірою обумовлена обмеженою кількістю високоімовірних або висококорельованих шляхів розповсюдження.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Больє, Р.; Шорс, Д.; Сміт, Д.; Трітман-Кларк, С.; Уікс, Б.; Вінгерс, Л. Сім'ї SIMON та SPECK легких блокових шифрів. *IACR Cryptol. ePrint Arch.* **2013**, *2013*, 404.
2. Abdelraheem, M.A.; Alizadeh, J.; AlKhzaimi, H.A.; Aref, M.R.; Bagheri, N.; Gauravaram, P. Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48. У матеріалах Міжнародної конференції з криптології в Індії, Бангалор, Індія, 6-9 грудня 2015 р.; с. 153-179.
3. Kölbl, S., Leander, G., Tiessen, T. Спостереження над сімейством блокових шифрів SIMON. IACR Cryptol. ePrint Arch. 2015, 2015, 145.



***Соловей Вероніка Сергіївна***– студентка групи 1БС-24Б, факультет інформаційних технологій та комп'ютерної інженерії. Вінницький національний технічний університет, Вінниця, email: nikasolovey1@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** - аспірант групи 125-23а, асистент кафедри захисту інформації факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

***Solovei Veronika S***.—student of group 1BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nikasolovey1@gmail.com

Supervisor: ***Kyrylashchuk Tatyana Gennadiyevna*** — graduate student of group 125-23a, assistant of the department of information protection of the faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com