УДК 004.056.55

Білоус В. М.
Кирилащук Т. Г.

АРГУМЕНТИ РУЧКИ ТА ПАПЕРУ ДЛЯ SIMON ТА SIMON-ПОДІБНИХ ДИЗАЙНІВ

Вінницький національний технічний університет

Анотація

У тезах розглядається математичне обґрунтування стійкості полегшених блочних шифрів родини SIMON та SIMON-подібних структур до диференціального криптоаналізу. На відміну від традиційних методів, що базуються на комп'ютерному пошуку за допомогою SAT/SMT-вирішувачів, запропоновано підхід «пером та папером» для верхньої оцінки ймовірності диференціальних характеристик. Встановлено, що для повнораундових варіантів SIMON та SIMECK ймовірність будь-якої характеристики не перевищує 2^{-2m} , де 2n -довжина блоку. Це дозволяє гарантувати безпеку шифрів навіть за умови доступу зловмисника до повного кодового кнгиги.

Ключові слова: SIMON, SIMECK, диференціальний криптоаналіз, мережа Фейстеля, верхня межа ймовірності, полегшена криптографія.

Abstract

The theses consider the mathematical justification of the resistance of the SIMON family of lightweight block ciphers and SIMON-like structures against differential cryptanalysis. Unlike traditional methods based on computer-aided search using SAT/SMT solvers, a "pen and paper" approach is proposed to upper bound the probability of differential characteristics. It is established that for full-round variants of SIMON and SIMECK, the probability of any characteristic does not exceed 2^{-2n}, where 2n denotes the block length. This guarantees the security of the ciphers even if the attacker has access to the full codebook.

Keywords: SIMON, SIMECK, differential cryptanalysis, Feistel network, upper bound probability, lightweight cryptography.

Вступ

З появою нових криптографічних алгоритмів розробники мають надавати вагомі аргументи їхньої безпеки, особливо проти таких потужних векторів атак, як диференціальний та лінійний криптоаналіз. Більшість сучасних блокових шифрів будуються за стратегією «широкого сліду» (wide-trail strategy), яка дозволяє математично гарантувати стійкість до таких атак завдяки використанню лінійних кодів з оптимальною мінімальною відстанню та класичних S-блоків [4].

Однак для сучасних полегшених шифрів ситуація є іншою. Зокрема, родина шифрів SIMON, яка була розроблена та представлена Агентством національної безпеки (АНБ) США як рішення для пристроїв з обмеженими ресурсами (Інтернет речей) [3], має специфічну побітову структуру та використовує небієктивну функцію раунду (операції AND, XOR та циклічні зсуви).

Через таку нестандартну архітектуру тривалий час були відсутні формальні докази стійкості цієї родини шифрів. Попередні криптоаналітичні оцінки базувалися переважно на експериментальних даних та автоматизованому комп'ютерному пошуку за допомогою SAT/SMT-вирішувачів або методів змішаного цілочисельного лінійного програмування [2].

Незважаючи на високу точність експериментальних методів, вони не дають глибокого розуміння того, чому саме дизайн є безпечним, і не дозволяють перевірити результати без використання обчислювальних машин. Це зумовлює необхідність розробки строгих аналітичних методів (так званих аргументів «ручки та паперу»), які дозволяють зрозуміти внутрішню логіку дизайну та підтвердити його надійність математично, без застосування складних комп'ютерних засобів [1]. Тому метою даної роботи є аналіз та систематизація методології оцінки ймовірностей диференціальних характеристик для повнораундових версій SIMON-подібних шифрів. Такий підхід дозволяє сформулювати строгий аргумент безпеки, що базується виключно на математичних властивостях структури мережі Фейстля.

Результати дослідження

У ході аналізу було розглянуто узагальнення конструкції шифру SIMON шляхом декупажу раундової функції на лінійний та нелінійний компоненти. Це дозволило визначити концепцію SIMON-подібного шифру, де нелінійна функція містить частину $\rho(x) = \vartheta_1(x) \wedge \vartheta_2(x)$, що базується на побітовій операції AND над циклічно зсунутими копіями входу $\vartheta_1(x) = (x \ll a)$ та $\vartheta_2(x) = (x \ll b)$. Для класичного SIMON ці константи ротації дорівнюють (8, 1, 2), а для SIMECK - (5, 0, 1).

Головною науковою новизною є розробка методу доведення стійкості, який спирається на те, що для будь-якої вхідної різниці α множина можливих вихідних різниць утворює афінний підпростір $U\alpha$. Аналіз показав, що ймовірність диференціалу тісно пов'язана з вагою Геммінга (wt) вхідної різниці α. Було математично доведено, що у випадку $wt(\alpha)=2$ ймовірність переходу p_α не перевищує 2^{-3}. Це обмеження є критично важливим, оскільки воно дозволяє гарантувати достатню кількість переходів із низькою ймовірністю до того, як виникне нульова вхідна різниця.

Дослідження також доводить, що для ідеального гарантування безпеки лінійний рівень перетворення має володіти диференціальним розгалуженням (branch number) не менше 11. Хоча для стандартних лінійних шарів SIMON та SIMECK цей показник є нижчим, аналіз розповсюдження ваги Геммінга через структуру Фейстеля дозволяє компенсувати це. Як наслідок, для всіх повнораундових варіантів SIMON та SIMECK було доведено верхню межу ймовірності будь-якої диференціальної характеристики на рівні 2^{-2T+2}, де T - кількість раундів. Загалом ця ймовірність є нижчою за 2^{-2n}, де 2n - загальна довжина блоку шифру. Це формально гарантує, що навіть маючи доступ до повної кодової книги, зловмисник не зможе знайти робочу диференціальну характеристику.

Висновки

У роботі представлено перший неекспериментальний аргумент безпеки для повнораундових варіантів шифрів SIMON та SIMECK. Аналітичним шляхом доведено, що структура мережі Фейстеля в поєднанні з обраними параметрами ротації забезпечує надійний захист від диференціальних атак. Зокрема, встановлено, що ймовірність будь-якої диференціальної характеристики строго обмежена зверху значенням 2^{-2n}. Це гарантує безпеку досліджуваних криптоалгоритмів: навіть маючи доступ до повної кодової книги, зловмисник не зможе очікувати на успішне знаходження диференціальної характеристики. Запропонований підхід «ручки та паперу» не лише формалізує доказову базу без використання методів експериментального комп'ютерного пошуку, але й сприяє набагато глибшому розумінню архітектури та внутрішньої логіки полегшених шифрів. Отримані результати можуть бути використані для оцінки та проектування нових криптосистем із доведеною математичною стійкістю.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Beierle C. Pen and Paper Arguments for SIMON and SIMON-like Designs // Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany. – 2016. – 13 p.
2. Kölbl S., Leander G., Tiessen T. Observations on the SIMON block cipher family // Advances in Cryptology – CRYPTO 2015. – Springer Berlin Heidelberg, 2015. – P. 161–185.
3. Beaulieu R. et al. The SIMON and SPECK families of lightweight block ciphers // Cryptology ePrint Archive, Report 2013/404. – 2013.
4. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. – PhD thesis, KU Leuven, 1995.

Білоус В'ячеслав Миколайович – студент групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dokuksla@-ik@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Bilous Vyacheslav – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dokukaslavik@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com