УДК 004.056:004.032.26:621.391

Лисицький К. Є.

PhD, доцент кафедри математичного моделювання і аналізу даних Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна

Лисицька І. В.

д.т.н., професор кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна; професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки

НЕЙРОМЕРЕЖЕВИЙ КРИПТОАНАЛІЗ ТА ЗАХИСТ ВІД АТАК ПО ПОБІЧНИХ КАНАЛАХ У КРИПТОСИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Анотація. Досліджено застосування методів глибокого машинного навчання для криптоаналізу та оцінки стійкості ресурсно-обмежених симетричних шифрів у середовищі Інтернету речей (IoT). Проаналізовано ефективність побудови нейронних розрізнювачів на основі згорткових та рекурентних архітектур у порівнянні з класичними статистичними критеріями. Особливу увагу приділено профілюючим атакам по побічних каналах (DL-SCA) та розробці легковагових контрзаходів (маскування та зашумлення) без суттєвого збільшення апаратних витрат чипа. Запропоновано комплексний підхід до інтеграції нейромережевих інструментів у процес верифікації криптографічного захисту.

Ключові слова: нейромережевий криптоаналіз, глибоке навчання, атаки по побічних каналах, DL-SCA, Інтернет речей, маскування, криптографічна стійкість.

Масштабне впровадження інтелектуальних сенсорних мереж, медичних пристроїв та систем «розумного міста» зумовило необхідність створення надійних, але водночас виключно компактних криптографічних засобів. Малоресурсна криптографія вирішує це завдання шляхом оптимізації внутрішньої структури шифрів. Проте сучасний етап розвитку криптоаналізу характеризується появою якісно нових загроз, пов'язаних із використанням методів штучного інтелекту та аналізу фізичних витоків пристроїв [1].

Метою доповіді є аналіз потенціалу застосування глибоких

нейронних мереж для виявлення статистичних закономірностей у масивах шифротекстів, вивчення ефективності профілюючих атак по побічних каналах (DL-SCA) та обґрунтування методів апаратного захисту пристроїв Інтернету речей.

Нейромережеві розрізнювачі (Neural Distinguishers). Застосування згорткових нейронних мереж (CNN) та моделей на основі архітектури ResNet дозволяє виявляти нелінійні кореляційні залежності у зменшеній кількості раундів блочних шифрів, які залишаються непоміченими для традиційного лінійного чи диференціального аналізу [2]. Завдяки здатності нейромереж самостійно формувати ознаки, процес побудови диф-лінійних або інтегральних розрізнювачів істотно автоматизується.

Профілюючі атаки по побічних каналах (DL-SCA). Аналіз споживання електроенергії та електромагнітного випромінювання чипів за допомогою deep learning демонструє виключну ефективність [3]. Порівняно з класичним шаблонованим криптоаналізом (Template Attacks), глибокі мережі є стійкими до десинхронізації сигналів та часових зсувів (jitter). Це дозволяє компрометувати секретні ключі навіть за наявності базових апаратних завад.

Контрзаходи та апаратний захист. Нейтралізація нейромережевих загроз вимагає впровадження адаптивних методів захисту. Основними підходами є алгоритмічне маскування (masking) порядку 1–2 з використанням випадкових масок для S-блоків та часове зашумлення (hiding) за рахунок виконання фіктивних операцій (dummy cycles) [4]. Дослідження показують, що комбінація цих методів дозволяє підвищити вимоги до кількості необхідних фізичних трас у сотні разів без значного зростання еквівалентів логічних вентилів (GE).

Таким чином, інтеграція нейромережевих інструментів у методику оцінки стійкості криптографічних пристроїв є обов'язковим етапом проєктування сучасних LWC-систем. Забезпечення комплексної безпеки

вимагає врахування як алгоритмічної міцності шифру, так і його фізичної захищеності від витоків інформації.

Список використаних джерел

1. Benadjila R., Prouff E., Strullu R., Tallapally B., Maghrebi L. Deep learning for side-channel analysis and introduction to ASCAD database. Journal of Cryptographic Engineering. 2020. Vol. 10, № 2. P. 163–188. DOI: https://doi.org/10.1007/s13384-019-00367-6

2. Gohr A. Improving Key Recovery Attacks on Speck32/64 Using Deep Learning. Advances in Cryptology – CRYPTO 2019. Lecture Notes in Computer Science. Vol. 11693. Springer, Cham, 2019. P. 104–133. DOI: https://doi.org/10.1007/978-3-030-26951-7_4

3. Picek S., Perin G., Mariot L., Wu L., Batina L. SoK: Deep Learning-based Physical Side-channel Analysis. ACM Computing Surveys. 2023. Vol. 55, № 11. P. 1–35. DOI: https://doi.org/10.1145/3580362

4. Mangard S., Oswald E., Popp T. Power Analysis Attacks: Revealing Secrets of Smart Cards. New York: Springer Science & Business Media, 2007. 338 p.