UDC 004.738.5

СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ ДЛЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

Д. Є. Омельченко[1], *Д. Г. Караман*[2]

[1] *магістрант кафедри АУТС, НТУ «ХПІ», Харків, Україна*
[2] *старший викладач кафедри АУТС, НТУ «ХПІ», Харків, Україна*
dmytro.omelchenko@cit.khpi.edu.ua
dmytro.karaman@cit.khpi.edu.ua

У сучасному світі Інтернет речей (IoT) відіграє ключову роль у розвитку та трансформації різних сфер життя, від інтелектуальних будинків і міської інфраструктури до промислових та медичних систем. Проте зростання кількості підключених пристроїв і передачі даних у відкритих мережах зумовлює нові загрози для безпеки та конфіденційності інформації. Одним із найважливіших завдань у цьому контексті є забезпечення захищеного обміну даними між IoT-пристроями, які мають обмежені обчислювальні та енергетичні ресурси.

Ефективні та прості алгоритми симетричного шифрування є важливим інструментом для забезпечення безпеки в IoT. На відміну від методів потокового шифрування, які дуже часто реалізуються та застосовуються у таких випадках, симетричні алгоритми є більш універсальними, вони забезпечують більший рівень захисту при співставних вимогах та рівні складності, завдяки особливостям їх побудови вони є більш стійкими до найпоширеніших видів атак, в тому числі і до атак, які орієнтуються на особливості реалізації (side-channel attacks). При співставних характеристиках блокові симетричні алгоритми шифрування забезпечують досить швидку обробку даних і низьке енергоспоживання, що є критично важливим для пристроїв з обмеженими ресурсами. Проте реалізація таких алгоритмів вимагає знаходження ретельного балансу між рівнем захисту, швидкістю роботи та апаратурними витратами, щоб забезпечити надійну безпеку без надмірного навантаження на пристрої.

У доповіді розглядається приклад створення апаратної реалізації ефективного та простого алгоритму симетричного шифрування PRESENT [1-3] для подальшого використання у сфері IoT. Реалізація виконана за допомогою мови опису апаратури VHDL. Також проведено цикл функціонального моделювання для усіх можливих режимів роботи алгоритму, виконано технологічний синтез на базі ПЛІС FPGA Xilinx з родини Artix-7. Виконано оцінку витрачених ресурсів, розраховано очікуваний рівень швидкодії для зазначеної тактової частоти, проведено оцінку енергоспоживання мікросхеми в різних режимах роботи системи шифрування.

List of references:

1. *Bogdanov, A*. PRESENT: An Ultra-Lightweight Block Cipher. / *A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin & C. Vikkelsoe* // Cryptographic Hardware and Embedded Systems – CHES 2007. Publ. at Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. 2007. pp. 450–466. https://doi.org/10.1007/978-3-540-74735-2_31.

2. *Pandey, J. G.* Hardware architectures for PRESENT block cipher and their FPGA implementations. / *Pandey, J. G., Goel, T., Karmakar, A.* // IET Circuits Devices Syst., Vol. 13. 2019. pp. 958-969. https://doi.org/10.1049/iet-cds.2018.5273

3. *ISO Standard. "ISO/IEC 29192-2:2019, Information security - Lightweight cryptography - Part 2: Block ciphers". Retrieved 2020-08-12.*