АПАРАТНА РЕАЛІЗАЦІЯ МЕТОДІВ АУТЕНТИФІКОВАНОГО ШИФРУВАННЯ З АСОЦІЙОВАНИМИ ДАНИМИ ДЛЯ СИСТЕМ IoT

Караман Д. Г.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

У зв'язку із зростанням числа пристроїв «Інтернету Речей» (*IoT*) та повсюдної підключеності, безпека передачі даних стає критично важливим завданням. Однак, традиційні криптографічні методи споживають значні ресурси, що ускладнює їх застосування в малопотужних пристроях, що мають обмежену енергоємність та обчислювальні ресурси.

Останнім часом активно розвиваються методи так званої «легкої» криптографії (*lightweight cryptography*), які забезпечують високий рівень захисту даних за порівняно низького споживання ресурсів: площі кристалу у мікросхемі, енергії, часу на виконання. Ці методи можуть бути використані у пристроях *IoT* для забезпечення безпечної передачі даних.

Застосування енергоефективної та легкої криптографії в системах *IoT* не тільки забезпечує безпеку передачі даних, але й дозволяє збільшити термін служби пристроїв, особливо за умови використання автономних малопотужних джерел споживання, що є важливим фактором для успішної експлуатації систем *IoT*.

Особливого розвитку в системах *IoT* набули методи аутентифікованого шифрування з асоційованими даними (*AEAD*). *AEAD* є методом криптографічного захисту інформації, що поєднує в собі алгоритми шифрування та аутентифікації. Головною особливістю цих методів є шифрування лише частини даних (прикладної інформації), що передаються, тоді коли аутентифікується увесь набір даних. Таким чином, одночасно забезпечується захист чутливих даних та цілісність усього пакету, включно з незашифрованими даними: заголовками пакетів, адресами кінцевих та проміжних вузлів, технічними характеристиками пакету, статистичною інформацією та мітками часу. Відкриті, але аутентифіковані дані дозволяють організовувати складні механізми маршрутизації та доставки пакету даних до адресата. Водночас, гарантується цілісність та автентичність інформації та надійність її джерела.

У лютому 2023 року Національний інститут стандартів та технологій США (*NIST*) повідомив про завершення конкурсу на найефективніший стек криптографічних алгоритмів для забезпечення *AEAD* у системах енергозаощадливої електроніки та пристроях «Інтернету Речей». Фіналістом стала група алгоритмів, яку назвали *ASCON*. Під час конкурсу було розглянуто багато реалізацій алгоритмів цього стеку та проаналізовано на предмет ефективності. У докладі розглянуто основні підходи для реалізації цих алгоритмів на ПЛІС типу *FPGA* та методики аналізу отриманих реалізацій на предмет заощадливості ресурсів та енергії.