ОПТИМІЗАЦІЯ ARX АЛГОРИТМУ ШИФРУВАННЯ PRESENT ЗА ДОПОМОГОЮ МЕТОДУ ВЕКТОРІВ ПЕРЕСТАНОВКИ

Бакаєв С. В., Руженцев В. І.
Харківський національний університет радіоелектроніки, Харків, Україна

Методи криптографічного захисту у вбудованих системах стали основою «легковажної» криптографії. Вони базуються на 3 операціях: додавання (addition), циклічний зсув(rotation), логічне множення (xor). Прикладом цієї методології являється алгоритм PRESEN. Шифр базується на SP-мережі і складається з 31 раунда. Довжина блоку - 64 біта, підтримуються дві довжини ключів - 80 та 128 біт. Стандартна реалізація алгоритму з розміром ключа 80-біт та 64-бітному відкритому тексті та складає 32 такти процесору на шифрування блоку.

Даний шифр був представлений на конференції CHES 2007. У 2012 році організації ISO і IEC включили алгоритми PRESENT разом з CLEFIA в міжнародний стандарт полегшеного шифрування ISO / IEC 29192-2.

Методика оптимізації «векторів перестановок» полягає у використанні інструкцій перестановки векторів для реалізації пошуку у таблицях за допомогою механізму SIMD, який присутній у більшості сучасних процесорів. Спершу будуються таблиці у кількості 64/m, де m = 8, таблиця наповнюється сусідніми 4-бітними S-box та найменш значимими 4-бітними словами у стані шифру. Після цього для поточного стану шифру використовується раунд підстановки та перестановки виконується в одну дію за допомогою інструкції перестановки(pshufb).

Метою доповіді є програмна реалізація шифру PRESENT та застосування до готової реалізації методики векторів перестановки. Аналіз швидкодії шифру з урахуванням сучасних SSE3 інструкцій. Приводиться аналіз швидкодії не оптимізованого шифру та з оптимізованого. За рахунок сучасних SSE3 інструкцій та їх паралельного використання значно зменшується кількість тактів процесора на виконя одного етапу алгоритму.

Список літератури

1. Л. Стасенко Современные технологии радиочастотной идентификации // Системы без-опасности №2(56), 2004

2. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher.[Текст] / In Pascal Paillier and Ingrid Verbauwhede, editors, CHES, volume 4727 of Lecture Notes in Computer Science, pp.. 450–466. Springer, 2007.

3. ISO/IEC 29192-2:2019 Information security – Lightweight cryptography – Part 2: Block ciphers