ЗАСТОСУВАННЯ ПЛІС У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Пугач К. О.
Науковий керівник – к.т.н., доц. Воргуль О.В.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки,14, каф. КРіСТЗІ, тел. (057) 702-14-30
e-mail: kateryna.puhach@nure.ua

The relevance of this article lies in the fact that in connection with the increase in the number of cyberattacks on the devices of the Internet of Things, the actual scientific and practical task is getting involved in the development of hardware methods and in the acquisition of digital attachments for illegal access.

Вступ. Кількість пристроїв Інтернету речей, з'єднаних між з собою, зростає разом із кількістю криптографічних атак на дану групу пристроїв. У зв'язку з цим, актуальною науковою та практичною задачею вважається розробка апаратних методів і засобів захисту цифрових пристроїв від нелегального доступу до інформації.

Якісним апаратним методом прискорення роботи реалізованих алгоритмів шифрування є використання програмованих логічних інтегральних схем. Перш за все, це пояснюється високою швидкістю криптографічних операцій. Швидкість обумовлена великою кількістю логічних елементів [4]. Наприклад, возведення у ступінь по модулю, що широко застосовується при шифруванні на відкритих ключах, можна здійснити на FPGA зі швидкістю 1000 транзакцій у секунду. Завдяки максимальній швидкості шифрування даних, на базі ПЛІС створюються криптографічні системи, що потребують зміни алгоритму шифрування після кожного сеансу. ПЛІС такого типу застосовуються в реалізації DES, 3DES, Blowfish, CAST, IDEA і ін. [1].

Так само ПЛІС широко використовуються в задачах генерації випадкових чисел. Апаратно реалізований генератор випадкових чисел має аналоговий та цифровий модулі. При цьому цифровий модуль виконаний на логічному масиві. Для значного зменшення проценту забракованих масивів були розроблені оригінальні алгоритми обробки випадкових чисел, реалізованих в ПЛІС [2].

Будь-яка реалізована криптосистема може мати канали, які пропускають непотрібну інформацію. Прикладами таких каналів можуть бути лінії електроживлення або електромагнітне випромінювання. Аналізуючи споживану ПЛІС потужність при виконанні криптографічних операцій можна визначити області, які корелюють з ключем або іншими потрібними кріптоаналітичними параметрами. Метод застосовується для злому програмних засобів або ASIC, але немає ніяких перешкод для використання його при спробах зламати ПЛІС.

Якщо криптосистема представляє собою ПЛІС, і аналітик має вільний доступ до входів і виходів, то набравши необхідну статистику і,

використовуючи карту Карно, він може отримати внутрішню логіку ПЛІС і скомпрометувати шифр. Цей спосіб буде дієвим, якщо аналітик володіє достатніми обчислювальними потужностями і має вільний доступ до системи. В даний час це не є реальною загрозою через складність і розміри сучасних ПЛІС. Реалізовані потокові або блокові шифри мають занадто довгі ключі, щоб шукати їх методом перебору.

Для більшості пристроїв типу FPGA передбачена спеціальна функція «readback», призначена для читання конфігурації схеми з метою полегшення налагодження [3]. Зловмисник може спробувати використовувати її через JTAG або інтерфейс програмування. Запобігти доступу до конфігурації можна за допомогою бітів безпеки. Однак, використання спеціальних регістрів не гарантує повної захищеності і, використовуючи апаратні збої і деактивування бітів безпеки, аналітик може отримати доступ до конфігурації. Вразливість усувається збільшенням кількості бітів безпеки і встановленням ПЛІС в безпечне середовище, в якому, при виявленні втручання, вся конфігурація видаляється або пристрій самознищується.

Висновки. Використання програмного забезпечення логічних інтегральних схем широко застосовується в різних варіантах реалізації системи захисту інформації. ПЛІС відноситься до апаратного методу прискорення роботи реалізованих алгоритмів шифрування. Застосовувані схеми використовуються за допомогою багатопроцесорної швидкості завдяки можливості моментальної заміни компрометованого або застарілого алгоритму шифрування, гнучкості чисто програмних методів та потужності апаратних реалізацій, таких як ASIC.

Список використаних джерел:

1. Protecting against Cryptographic Trojans in FPGAs // Field-Programmable Custom Computing Machines (FCCM), 2015 IEEE 23rd Annual International Symposium on. — 2015.

2. Iryna Svyd, Oleksandr Vorgul, Valerii Semenets, Oleg Zubkov, Valeriia Chumak, Natalia Boiko. Special Features of the Educational Component “Design of Devices on Microcontrollers and FPGA”. // II International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2020, pp. 55-57. doi: 10.35598/mcfpga.2020.017

3. И.Тарасов, к.т.н. ПЛИС Xilinx и цифровая обработка сигналов // Электроника. — 2011. — № 3. — С. 70 - 74.

4. Iryna Svyd, Oleksandr Maltsev, Liliia Saikivska, Oleg Zubkov. Review of Seventh Series FPGA Xilinx. // First International Scientific and Practical Conference «Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» MC&FPGA-2019, Kharkiv, Ukraine, July 26-27, 2019. – Kharkiv: 2019. – P. 25-26.