МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 28-го МІЖНАРОДНОГО
МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2024 р.

Том 3

КОНФЕРЕНЦІЯ «ІНФОРМАЦІЙНІ РАДІОТЕХНОЛОГІЇ ТА ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

Харків 2024

УДК 004.31

АСПЕКТИ БЕЗПЕКИ БІТОВОГО ПОТОКУ В ПРИСТРОЯХ ARTIX 7 СЕРІЇ

Вовсянікер М.Ю.
Науковий керівник – асистент Білоцерківець О.Г.
Харківський національний університет радіоелектроніки, каф. МТС,
м. Харків, Україна
тел. +38057-702-0229, e-mail: d_mts@nure.ua

This artitle delves into the various security measures available for FPGA bitstreams, focusing on encryption techniques. Discussing the paramount importance of preventing reverse engineering, it explores protection levels. Furthermore, it elucidates integrated encryption and decryption logic within FPGA devices, showcasing the inherent security benefits, particularly evident in the AES decryption capabilities of Series 7 devices. The process of generating encrypted bitstreams using tools like BitGen is highlighted, emphasizing the pivotal role of encryption keys.

Безпека бітового потоку має велике значення для захисту інтелектуальної власності та важливих конфігураційних даних в пристроях FPGA, які часто використовуються у критичних застосунках, таких як мережеве забезпечення, медична техніка та автономні системи.

Перш за все, ми розглянемо метод захисту бітового потоку шифрування оскільки існує ще інший метод це аутентифікація. Шифрування дозволяє захистити конфігураційні дані від несанкціонованого доступу шляхом застосування різних криптографічних алгоритмів, таких як Advanced Encryption Standard (AES). Дешифрування дозволяє забезпечити інтегритет та автентичність бітового потоку, перевіряючи його цілісність за допомогою підпису або хеш-функції.

Одним з ключових аспектів безпеки є запобігання зворотному читанню, що включає в себе захист від реверс-інженерії [1]. Для цього можна використовувати різні рівні захисту, такі як рівень 1 і рівень 2, які вимикають повторне читання та повторне налаштування відповідно. Наступним важливим пунктом є розгляд інтегрованих методів шифрування і дешифрування в FPGA. На прикладі пристроїв Artix серії 7 виявляється, що вони мають вбудовану логіку дешифрування AES, яка забезпечує високий рівень безпеки. Ключовий момент полягає в тому, що без знання ключа шифрування потенційні зловмисники не зможуть аналізувати зовнішні перехоплені бітові потоки.

Процес завантаження ключа шифрування на пристрій серії 7 FPGA відбувається через інтерфейс JTAG. Інструменти, такі як iMPACT або програматор пристрою Vivado, приймають файл NKY як вхідні дані та програмують його на пристрої з ключем через JTAG, використовуючи кабель програмування AMD.

Для програмування ключа, пристрій переходить у спеціальний режим доступу до ключа за допомогою інструкції XSC_PROGRAM_KEY. У цьому режимі вся пам'ять FPGA, включаючи ключ шифрування та конфігураційну пам'ять, очищається. Після програмування ключа і виходу з режиму доступу до ключа, його не можна зчитати з пристрою і неможливо перепрограмувати без повного очищення пристрою. Режим доступу до ключа є прозорим для більшості користувачів.

Під час завантаження ключа в біти eFUSE користувач може прочитати ключ для перевірки. Після цього користувач повинен запрограмувати регістр FUSE_CNTL, щоб вимкнути читання та запис ключа AES.

Розглянемо процес завантаження зашифрованих бітових потоків на пристрій FPGA серії 7 після програмування його за допомогою відповідного ключа шифрування. Після конфігурації із зашифрованим бітовим потоком неможливо прочитати конфігураційну пам'ять через інтерфейси JTAG або SelectMAP, незалежно від самого бітового потоку.

Хоча пристрій має ключ шифрування, для налаштування можна використовувати незашифрований бітовий потік лише після очищення конфігураційної пам'яті за допомогою сигналів POR або PROGRAM_B, в такому випадку ключ ігнорується. Після конфігурації з незашифрованим бітовим потоком можливе повторне зчитування (якщо це дозволено параметрами безпеки BitGen). Проте ключ шифрування все ще залишається недоступним для зчитування з пристрою, що запобігає використанню бітових потоків троянського коня для руйнування схеми шифрування FPGA серії 7.

Зашифрований бітовий потік може бути доставлений через різні інтерфейси конфігурації, такі як JTAG, послідовний, SPI, BPI, SelectMAP і ICAPE2. Проте, існують обмеження часу для деяких методів конфігурації, зокрема для інтерфейсів, що приймають зашифровані бітові потоки через шину даних x8 або x16. Наприклад, швидкість CCLK сповільнюється для шини x16, коли використовується ExtMasterCCLK_en, що може вплинути на швидкість передачі даних [2].

Цей процес завантаження зашифрованих бітових потоків є ключовим аспектом забезпечення безпеки конфігурації FPGA та захисту від потенційних атак. У підсумку, забезпечення безпеки бітового потоку в FPGA є важливою задачею для забезпечення цілісності та захисту конфігураційних даних у критичних застосунках.

Список використаних джерел:

1. Білоцерківець О.Г., Воргуль О.В. Стандартизація крипто безпеки задля потреб та викликів сьогодення // Об’єднані наукою: перспективи міждисциплінарних досліджень Київ. – 2020. – С. 171–173.

2. Xilinx.com: [Інтернет-портал]. URL: https://docs.xilinx.com/v/u/en-US/ug470_7Series_Config (дата звернення: 01.02.2024).