УДК 004.94
М. Карпінський[(1)]**, А. Ляпандра**[(2)]
([1]Тернопільський національний технічний університет імені Івана Пулюя, [2]Тернопільський національний економічний університет)

РОЗРОБЛЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОКОМУНІКАЦІЙ НА ОСНОВІ ПЛІС

Програмовані логічні інтегральні схеми (ПЛІС) знайшли широке застосування для розв'язання ресурсомісних задач використання надійних та безпечних високошвидкісних інформаційних комунікацій. Так, на сьогоднішній день, ПЛІС компанії Xilinx (США) мають як програмні, так і апаратні рішення захисту передачі інформації, робота яких ґрунтується на використані пасивних та активних методів. Серед сімейств ПЛІС компанії Xilinx найвищий рівень захисту реалізовано у сімействі UltraScale (7 пасивних і 10 активних методів), дещо нижчий -- Zynq, ПЛІС Xilinx 7-ї серії, Virtex-6 (відповідно 5 і 8), ще нижчий – у ПЛІС сімейства Spartan-6 (4 і 4) [1].

Рішення з використанням ПЛІС характеризуються гнучкістю процесу розробки, що обумовлене простотою внесення змін при коригуванні замовником функціональної частини, а завдяки реалізації проекту на одній із мов опису обладнання суттєво спрощується перевірка відповідності технічному завданню розробленого засобу. Перевагою заміни спеціалізованих мікросхем кристалами ПЛІС є суттєве зменшення кількості та довжини провідників, рівня електромагнітного та теплового випромінювання, що в свою чергу зменшує витік інформації через канали побічних електромагнітних випромінювань і наводок.

Захищеність програмної та апаратної частин від несанкціонованого доступу до даних дає можливість розробляти функціональні вузли тестування та налаштування засобів захисту інфокомунікацій на основі ПЛІС. Принцип їх роботи полягає у подачі псевдовипадкової послідовності на вхід системи, порівнянні результуючого сигналу на виході із еталонним. Псевдовипадкову послідовність отримують на основі рекурентних ліній затримки, які проектуються на апаратуру як тригери зсуву. Зворотній зв'язок забезпечується операцією додавання за модулем два, яке реалізується елементом XOR.

Проектування засобів захисту інфокомунікацій полягає у виконанні таких етапів: 1) розроблення аналітичної моделі роботи; 2) побудова алгоритму роботи та оптимізація за критеріями часової та просторової складностей; 3) проектування алгоритму на апаратуру шляхом його опису на мові VHDL або Verilog, розроблення IP-ядер; 4) функціональне і часове моделювання, топологічне проектування логічного та комунікаційного середовища; 5) розміщення проекту на кристалі та верифікація проекту з метою виявлення впливу реальних затримок поширення сигналів; 6) завершальний етап – конфігурування ПЛІС.

Етапи 1-5 є ітераційними і вимагають верифікації проекту. У випадку складності проекту застосовують загальносистемний рівень на основі підрівнів специфікації системи, повідомлень та передач. Такий підхід дає змогу відразу проектувати як програмну, так і апаратну частини системи, узгоджувати їх між собою починаючи з початкових етапів, підготовити всю екосистему до моменту отримання прототипу.

Перелік використаних джерел

1. Design Security: [Електрон. ресурс]. - Режим доступу: http://www.xilinx.com/products/technology/design-security/index.htm

2. Маршрут проектирования «систем-на-кристалле» (СнК): [Електрон. ресурс]. - Режим доступу: http://www.ipmce.ru/custom/ekb/mp/