АНАЛІЗ ЕФЕКТИВНОСТІ ВБУДОВАНОЇ СИСТЕМИ СИНДРОМНОГО ТЕСТУВАННЯ ПІДСТАНОВЛЮВАЛЬНОГО БЛОКУ

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

Тема діагностування апаратних реалізацій криптографічних систем останнім часом активно розглядається в зарубіжних публікаціях. Однак значна частина уваги приділена тільки функціональному діагностуванню — основні зусилля дослідників спрямовані на запобігання атакам по вторинним каналах, таких як атака з впровадженням помилки або атака маніпуляціями в ланцюгах живлення, які виконуються під час функціонування цільового пристрою.

Сучасні апаратні рішення в області криптографії не поступаються за складністю електронним пристроям середнього і високого ступеня інтеграції, таким як вбудовані модулі, процесори, плати розширення. Більш того, до криптографічних модулів пред'являються більш жорсткі вимоги по надійності і відмовостійкості. Отже, зростає необхідність використання напрацювань в області тестового діагностування для підвищення тестопригодності апаратних криптосистем.

Основним механізмом синдромного тестування є подання до схеми, що перевіряється, повного тривіального вичерпного тесту і підрахунок контрольної суми реакцій на виходах схеми — синдрому, як характеристики внутрішнього стану схеми, що перевіряється. Для визначення справності схеми отриманий синдром порівнюється з еталонним значенням або синдромом дублюючої схеми.

Перевагою методу є простота реалізації діагностичного експерименту, в якому використовуються двійкові лічильники і схеми порівняння, а також виключення дорогої процедури машинного синтезу перевіряючих тестів. Однак платою за простоту процедури діагностування є або невисока достовірність результатів діагностування для довільної КС, або необхідність застосування спеціальних методів аналізу схеми і її подальшої модифікації, що забезпечує покриття обумовленого класу несправностей для даного методу тестування.

У доповіді розглянута схема модуля системи шифрування на базі алгоритму ГОСТ 27148-89, що синдромно тестується. Розглянутий модуль складається з восьми 4-входових підстановлювальних блоків і реалізує підстановлювальне перетворення алгоритму шифрування. Для цього модуля розроблена і реалізована модель на мові опису апаратури VHDL з вбудованою схемою діагностування, а також розроблена і реалізована модель системи впровадження/імітації помилки для проведення автоматизованих випробувань. На базі розроблених моделей проведено випробування з вичерпною генерацією тестів і повним перебором помилок.