Дербунович Л.В., Караман Д.Г., Україна, Харків

СИНТЕЗ БЛОКІВ ПІДСТАНОВКИ S-BOX АЛГОРИТМУ ШИФРУВАННЯ RIJNDAEL, ЩО СИНДРОМНО ТЕСТУЮТЬСЯ

У доповіді проведено аналіз існуючих методів виявлення помилок в апаратних реалізаціях криптографічних систем у зв'язку з посиленням інтересу до використання у криптоаналітичних атаках випадкових або навмисно введених помилок. Запропоновано використання методів синдромного тестування для діагностування апаратної реалізації підстановлюючого блоку S-Box алгоритму шифрування Rijndael. Синтезовано тестоздатну модель підстановлюючого блоку мовою VHDL. Показано, що використання методів синдромного тестування дозволить скоротити апаратні витрати при проектуванні тестопридатних криптографічних модулів.

Дербунович Л.В., Караман Д.Г., Украина, Харьков

СИНТЕЗ СИНДРОМНО ТЕСТИРУЕМЫХ БЛОКОВ ПОДСТАНОВКИ S-BOX АЛГОРИТМА ШИФРОВАНИЯ RIJNDAEL

В докладе проведен анализ существующих методов обнаружения ошибок в аппаратных реализациях криптографических систем в связи с возросшим интересом к использованию в криптоаналитических атаках случайных или преднамеренно внедренных ошибок. Предложено использование методов синдромного тестирования для диагностики аппаратной реализации подстановочного блока S-Box алгоритма шифрования Rijndael. Синтезирована тестопригодная модель подстановочного блока на языке VHDL. Показано, что применение методов синдромного тестирования позволяет сократить аппаратные затраты при проектировании тестопригодных криптографических модулей.

Derbunovich L.V., Karaman D.G., Ukraine, Kharkiv

SYNDROME TESTABLE SUBSTITUTION BOX (S-BOX) DESIGN FOR ENCRYPTION ALGORITHM RIJNDAEL

In the report the analysis of existing error detection methods for hardware implementations of cryptographic systems is carried out owing to grown interest in using random or maliciously injected faults. Use of syndrome testing methods for Rijndael S-box hardware implementation diagnosis is proposed. An VHDL model for syndrome testable substitution box is synthesized. It is shown that use of syndrome testing methods allows to reduce hardware expenses in cryptographic modules design process.