МЕТОД ФУНКЦИОНАЛЬНОГО ДИАГНОСТИРОВАНИЯ ПОДСТАНОВОЧНЫХ БЛОКОВ S-BOX, РЕАЛИЗОВАННЫХ В КОМПОЗИТНЫХ ПОЛЯХ

Дербунович Л. В., Караман Д. Г., Осипенко А. Н.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Высокий уровень защиты, а также высокопроизводительные аппаратные и программные реализации стандарта криптографической защиты данных AES определили первоочередность выбора алгоритма шифрования этого стандарта для многих ответственных и критически важных приложений. Тем не менее, внутренние постоянные и перемежающиеся неисправности, в том числе и намеренно вызванные злоумышленником, нацеленные на раскрытие секретного ключа, могут значительно снизить надежность этих решений.

В этой работе представлена схема оперативного обнаружения ошибок функционирования подстановочных блоков, выполняющих прямые и обратные преобразования SubBytes и InvSubBytes — единственные нелинейные операции алгоритма шифрования, описываемого стандартом AES. Предложенный метод, основанный на паритетности входных, промежуточных и выходных данных, применяется к низкозатратным реализациям подстановочных блоков S-BOX и InvS-BOX в композитных полях. Функционально эти блоки разбиваются на 3 составные части, для выходных значений которых вычисляются (предсказываются) паритетность.

Предложенная схема обнаружения неисправностей может быть подвержена субконвейеризации без добавления задержек к изначальной конвейеризированной структуре. В конвейеризированной схеме обнаружения ошибок используются модули предварительного вычисления паритетности для каждого конвейерного блока и получения флага индикации ошибки.

Схемы предварительного вычисления паритетностей могут быть использованы в конвейерных реализациях подстановочных блоков без необходимости изменения или подстройки частоты тактового сигнала. Предварительный расчет бит осуществляется в течение того же периода тактового сигнала, что и выходное значение блока подстановки. Расчет паритетности выходных данных и сравнение её с предварительно рассчитанной могут осуществляться в течение следующего такта.

Моделирование показывает, что среди подобных схем обнаружения ошибок, за исключением тех, которые построены на практически на 100% избыточности, предложенный вариант обладает лучшими характеристиками по обнаружению групповых внезапных (burst) и случайных (multiply random) неисправностей.

В результате аппаратных реализаций предложенной схемы выяснилось, что она обладает меньшими аппаратными затратами, критическими путями (задержками), энергопотреблением, чем аналоги со схожими подходами к обнаружению ошибок функционирования.