САМОПРОВЕРЯЕМЫЕАППАРАТНЫЕ КРИПТОГРАФИЧЕСКИЕМОДУЛИ

Караман Д. Г.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

При аппаратной реализации модулей криптографической защиты данных некоторые преобразования, входящие в состав алгоритмов шифрования требуют существенных аппаратных, временных затрат, или нетривиальных решений в их исполнении. К таким преобразованиям, в частности, относятся различные виды подстановок, в основе которых лежат специальным образом составленные таблицы, требующие значительного объема внутренней памяти, либо нелинейные функции, реализация которых арифметическими средствами (АЛУ) является неэффективным и аппаратно затратным. Кроме того, в последнее время особо актуальным является обеспечение тестопригодности и повышение криптоаналитической стойкости аппаратных криптографических модулей, что дополнительно усложняет их проектирование.

Подстановочный блок представляет собой устройство, на вход которого поступает n-разрядный двоичный вектор исходных данных, а на выходе формируется соответствующий ему выходной m-разрядный вектор. В зависимости от алгоритма шифрования значения m и n могут варьироваться от 4 до 128 бит.

При небольшой разрядности входных векторов (AES S-Box – 8 бит, узлы замены ГОСТ 28147-89 – 4 бита) подстановочный блок целесообразно реализовать в виде многовыходной комбинационной схемы, где каждый разряд выходного вектора формируется с помощью булевой функции n переменных. Такой способ реализации подстановочного блока позволяет исследовать возможность использования методов синтеза самопроверяемых комбинационных схем для обеспечения защиты аппаратно реализуемых криптографических средств от неисправностей, возникающих на этапе производства, в условиях эксплуатации, а также нового перспективного класса атак, основанных на искусственно вызванных сбоях.

Показано, что использование этих методов позволяет при допустимой степени увеличения аппаратной избыточности повысить степень обнаружения одиночных константных и перемежающихся неисправностей.