СПОСОБ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Оборудование, использующее блочные алгоритмы для шифрования данных с симметричным ключом, появилось достаточно давно. Решения задач шифрования данных с использованием специализированных аппаратных систем значительно увеличивало эффективность систем безопасности по сравнению с комплексами, использующими чисто программные решения, и, не только, за счет повышения производительности системы в целом. Эволюция аппаратных комплексов шифрования определялась в первую очередь элементной базой, используемой для создания

специализированных вычислительных средств. Во вторую очередь – за счет создания более сложных алгоритмов шифрования, в условиях появления элементной базы, позволяющей выполнять аппаратную реализацию новых алгоритмов в условиях конструктивных ограничений. Первые устройства были созданы на элементах малой и средней степени интеграции и отличались относительно низкой производительностью и надежностью. Следующим этапом в эволюции подобного оборудования стало использование заказных больших интегральных схем и серийных микроконтроллеров, что позволило решить ряд задач связанных с компоновкой систем. Коренным образом подход к решению задачи изменился в связи с появлением программируемых логических устройств.

В начале такое оборудование реализовывалось в виде проектов, которые использовали декомпозицию на несколько кристаллов программируемых логических устройств. Далее, с повышением количества элементов в микросхеме те же проекты могли быть реализованы в виде одной микросхемы, и, в дальнейшем занимали только часть микросхемы. В современных условиях эта часть является весьма незначительной. То есть появляется возможность использования все более и более сложных алгоритмов, что приводит к использованию большего количества элементов кристалла и повышению криптографической стойкости, либо появляется возможность увеличения производительности за счет конвейеризации и распараллеливания операционной части аппаратных устройств. Алгоритмы блочного шифрования обычно хорошо распараллеливаются и конвейеризируются, что позволяет легко масштабировать аппаратное решения, но только для тех модификаций алгоритма, которые не используют предыдущий зашифрованных блок для обработки следующего блока.

Для решения практических задачи эффективного использования распараллеливания, путем увеличения одновременно работающих вычислительных ядер внутри кристалла, была осуществлена реализация алгоритма, позволяющая перейти к разделения параллельного потока данных на ряд битовых (последовательных) потоков. Каждый поток шифруется с использованием стандартного алгоритма блочного шифрования. Количество потоков может быть произвольным в пределах ограничения, определяемого размером блока. Сцепление блоков осуществляется в пределах каждого потока, то есть для каждого вычислительного ядра отдельно. Для увеличения криптографической сложности реализуется алгоритм случайной перестановки n потоков, которая может быть получена на базе существующего ключа фиксированного размера согласно выбранного алгоритма. Лучшее решение может быть получено при увеличения эффективной длины ключа на m дополнительных разрядов и реализующего перестановку разрядов согласно дополнительному полю ключа, что, в конечном итоге, позволяет повысить количество вариантов перебора в $n!$ раз. Предложенный способ позволяет эффективно использовать топологию программируемого логического устройства, повысить производительность устройства и увеличить криптографическую сложность алгоритма.