4. Дорожное яблоко (подбрасывание в общедоступных местах организации (лифт, столовая, парковка) инфицированных носителей информации с мотивирующими к их запуску логотипами/бирками/именами файлов).

После окончания тестирования, специалистами проводится сбор и обработка данных. Часто заказчик хочет знать, кто именно попался на ту, или иную уловку теста. Однако данная информация не передается руководству компании, т.к. проводится тестирование не одного человека, а группы лиц. Соответственно, речь идет об информационной системе, как о едином целом. Исследования показывают, что «человеческий фактор» остается одной из самых распространенных угроз информационной безопасности. Для снижения рисков, связанных с этим обстоятельством, используются различные технические и административные механизмы защиты. Один из них – повышение осведомленности работников, в области информационной безопасности.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ХЭШ-ФУНКЦИИ SHA-256 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич

Криптографическая хэш-функция SHA-256 описана в документе RFC 4634 [1] и предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины. Данная функция используется в различных приложениях, связанных с защитой информации, а также в большинстве криптовалют. В указанных приложениях возникает необходимость высокопроизводительных аппаратных реализаций SHA-256. В докладе рассматривается полностью конвейерная реализация хэш-функции SHA-256 для одного блока данных (512 бит) на базе FPGA.

Характерной особенностью алгоритма SHA-256 является длинная цепочка последовательных сложений при вычислении новых значений переменных A и E. Для уменьшения числа сложений в одном такте реализации и, следовательно, повышения тактовой частоты конвейерного процессора вычисление переменных E-H на такт опережает вычисление переменных A-D. Кроме того используется предварительное вычисление сумм W_t, K_t, H и D. Одна ступень конвейерного процессора производит вычисления за один такт частоты синхронизации. Общее число ступеней конвейера с учетом 64 раундов алгоритма SHA-256 и завершающего сложения со значением вектора инициализации равно 67.

Характеристики реализации по отчету средств синтеза пакета ISE 14.7 для кристалла FPGA семейства Kintex7 XC7K160T-3: 27477 триггеров секций, 35161 просмотровая таблица (LUT), тактовая частота – 352 МГц.

При обработке сообщения, длина которого превышает один блок SHA-256 необходимо либо последовательно включить требуемое число процессорных ядер для реализации полностью конвейерного вычислителя, либо организовать итеративные вычисления на одном процессорном ядре, коммутируя с помощью мультиплексора выходные данные процессора на его вход требуемое число раз.

Литература

1. RFC 4634. US Secure Hash Algorithms (SHA and HMAC-SHA). [Электронный ресурс]. – URL: https://tools.ietf.org/pdf/rfc4634.pdf (дата обращения: 26.04.2018).

ДОСТУП К ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Р.В. Кислинский

Под информацией ограниченного распространения в Республике Беларусь понимаются государственные секреты, т. е. сведения, защищаемые государством в целях предотвращения их несанкционированного распространения и создания угрозы национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан.

Что касается перечня сведений, составляющих государственные секреты Республики Беларусь, то он определен как совокупность категорий сведений в области экономики,