АППАРАТНАЯ РЕАЛИЗАЦИЯ ФУНКЦИИ SCRYPT НА FPGA

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

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь

Функция Scrypt [1] предназначена для формирования секретного ключа на основе секретной строки (пароля). Характерной особенностью алгоритма функции является необходимость использования значительного объема памяти и последовательный характер большей части вычислений, что усложняет оборудование для криптоанализа путем перебора возможных значений паролей или ключей (brute-force attack). Данная функция используется, в частности, при доказательстве выполненной работы (proof of works) в криптовалюте Litecoin и в системе хранения резервных копий Tarsnap.

Укрупненно алгоритм функции Scrypt применительно к криптовалюте Litecoin заключается в последовательном выполнении следующих функций: PBKDF2 (P = 80 байт, S = 80 байт, c = 1, $dkLen$ = 128) [2], ScryptROMix (r = 1, B = 128 байт, N = 1024)

и второй функции PBKDF2 (P = 80 байт, S = 128 байт, c = 1, $dkLen$ = 32 байта). Внутри функции ScryptROMix используется функция ScryptBlockMix [1]. Первое 1024-кратное выполнение функции ScryptBlockMix используется для заполнения блока памяти из 1024 128-разрядных ячеек. При втором 1024-кратном выполнении функции ScryptBlockMix содержимое этих ячеек, выбранных в псевдослучайном порядке, используется для операции xor с результатом функции ScryptBlockMix. При практической реализации алгоритма можно было обойтись без памяти, вычисляя требуемое значение переменной, соответствующее некоторой ячейке памяти, прямо внутри второй группы циклов ScryptBlockMix, однако это потребует значительного времени из-за последовательного характера вычисления значений формируемого массива (следующий элемент вычисляется на основе значения предыдущего). Внутри функции ScryptBlockMix для получения псевдослучайных чисел используется хэш-функция Salsa20/8 [3].

Исходя из анализа вычислительного процесса указанных функций выбраны следующие архитектуры для их аппаратной реализации: функция Salsa20/8 реализуется параллельно-итеративной архитектурой, ScryptBlockMix и ScryptROMix реализуются итеративной архитектурой, PBKDF2 реализуется итеративно-конвейерной архитектурой. На верхнем уровне реализации функции Script используется конвейерная архитектура. Была выполнена реализация данной системы на базе отладочной платы VC707, использующей базовый кристалл FPGA XC7VX485T-2FFG1761. Аппаратные затраты после процедуры синтеза средствами ISE 14.7: 14211 Slice Registers, 16246 Slice LUTs, 32 BRAM. Тактовая частота – 179 МГц. Выполнение PBKDF2_1 занимает 1685 тактов, ScryptROMix – 46079 тактов, PBKDF2_2 – 281 такт.

Предложенная система может использоваться в качестве ядра майнера криптовалюты Litecoin.

Список литературы

1. RFC7914. The scrypt Password-Based Key Derivation Function [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc7914. – Дата доступа: 28.04.2023.

2. RFC2898. PKCS #5: Password-Based Cryptography Specification. Version 2.0 [Электронный ресурс]. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc2898. – Дата доступа: 28.04.2023.

3. Daniel J. Bernstein. Salsa20 specification [Электронный ресурс]. – Режим доступа: http://cr.yp.to/snuffle/spec.pdf. – Дата доступа: 28.04.2023.