ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ФОРМИРОВАНИЯ КЛЮЧА PBKDF2 НА БАЗЕ FPGA

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

В настоящее время для разрешения доступа пользователей к электронным данным широко используются пароли. Из-за плохой случайности и произвольной длины этих паролей они не могут использоваться в качестве ключей криптографических алгоритмов шифрования. В большинстве случаев ключи получают на основе паролей с использованием криптографических хэш-функций. Функция PBKDF2 (Password Based Key Derivation Function v2) является одним из важнейших криптографических алгоритмов [1], широко используемым в различных системах, таких как WiFi Protected Access (WPA/WPA2), Microsoft .NET framework, Apple OSX Operating System, Apple iOS, Blackberry и др. Характерной особенностью данной функции является большое (несколько тысяч или десятков тысяч) число повторений использования механизма HMAC (hash-based message authentication code – код проверки подлинности сообщений, использующий хэш-функции). В результате процесс формирования ключа занимает значительное время. В докладе рассматривается подход к конвейеризации процесса вычисления ключей в процессоре PBKDF2 на основе алгоритма SHA-1, который можно использовать в различных встраиваемых системах с достаточно высокой производительностью. Так как алгоритм вычисления ключа PBKDF2 носит итерационный характер, то максимальная производительность может быть получена при полной развертке алгоритма. Однако такая развертка характеризуется большим количеством ступеней (модулей SHA-1) – порядка нескольких десятков тысяч. Реализовать такое количество ступеней в рамках FPGA не представляется возможным. Компромиссное решение заключается в конвейеризации процесса вычисления хэш-значений в алгоритме SHA-1 с сохранением итерационного процесса вычисления ключей PBKDF2. При этом процессор может вычислять не один ключ, а одновременно несколько ключей по количеству ступеней в конвейере.

Рассматриваемый в докладе подход предполагает конвейеризацию алгоритма SHA-1 на уровне раундов, т. е. на каждой ступени конвейера реализуется один раунд алгоритма и модуль SHA-1 содержит 4 ступени [2]. Так как каждый раунд состоит из 20 шагов, то каждое входное значение итерационно 20 раз прокручивается на ступени конвейера, последовательно проходя через все 4 ступени. Полный конвейер одной итерации вычисления ключа PBKDF2 строится на базе двух модулей SHA-1 и состоит из 8 ступеней. В процессор PBKDF2, построенный на базе такого модуля SHA-1, можно последовательно загрузить 8 входных значений и организовать одновременное вычисление 8 ключей. Через промежуток времени, равный времени вычисления одного ключа, на выходе процессора последовательно будут получаться 8 значений ключей.

Цикл работы процессора PBKDF2 составляет 23 такта. Через каждые 23 такта в процессор загружается 8 входных значений. Время формирования ключа составляет

920000 тактов, после чего на выход через каждые 23 такта последовательно выдаются 8 вычисленных значений ключа.

Характеристики реализации процессора PBKDF2 с использованием пакета ISE 14.7 для кристалла FPGA семейства Virtex7 XC7VX485T-1: 8493 триггеров секций, 5575 просмотровых таблиц (LUT), рабочая тактовая частота по оценкам процедуры синтеза – 253 МГц.

Литература

1. NIST SP 800-132. Recommendation for Password-Based Key Derivations. Desember 2010. [Электронный ресурс]. – Режим доступа: http://nvlpubs.nist.gov/ nistpubs/Legacy/SP/ nistspecialpublication800-132.pdf. – Дата доступа: 03.05.2021.

2. Jae-woon Kim, Hu-ung Lee, Youjip Won. Design for high throughput SHA-1 hash function on FPGA, 2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN), July.4-6 2012, Phuket, Thailand. [Электронный ресурс]. – Режим доступа: http://www.esos.hanyang.ac.kr/files/publication/conferences/international/Design_for_high_throughput_SHA-1_hash_function_on_FPGA.pdf. – Дата доступа: 03.05.2021.