РЕАЛИЗАЦИЯ И ИССЛЕДОВАНИЕ АЛГОРИТМОВ КРИПТОГРАФИЧЕСКОГО ХЕШИРОВАНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сыроваткин М.И.

Клюс В.Б.- к.т.н., доцент

В информационном мире поток данных, передаваемых тем или иным способом, обладает огромными объемами. Во многих случаях для сравнения данных используется хеширование – преобразование входного массива данных произвольной длины в выходную строку фиксированной длины. В идеальном случае каждому массиву данных будет соответствовать уникальный хеш. Очевидна уязвимость незащищенных систем связи, в том числе вычислительных сетей. Так среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые, в том числе, и в криптографии. Криптографическое хеширование является одним из методов защиты информации.

Структура Меркла-Дамгарда — метод построения криптографических хеш-функций. Криптографическая хеш-функция должна преобразовывать входное сообщение произвольной длины в выходное сообщение фиксированной длины. Этого можно достичь путём разбиения входного сообщение на блоки одинакового размера и их последовательной обработки односторонней функцией сжатия, которая преобразовывает входное сообщение фиксированной длины в более короткое выходное сообщение фиксированной длины.

Популярность структуры Меркла-Дамгарда обусловлена тем, что, как было доказано, если односторонняя функция сжатия устойчива к коллизиям, то и хеш-функция, построенная на ее основе, будет также устойчива к коллизиям.

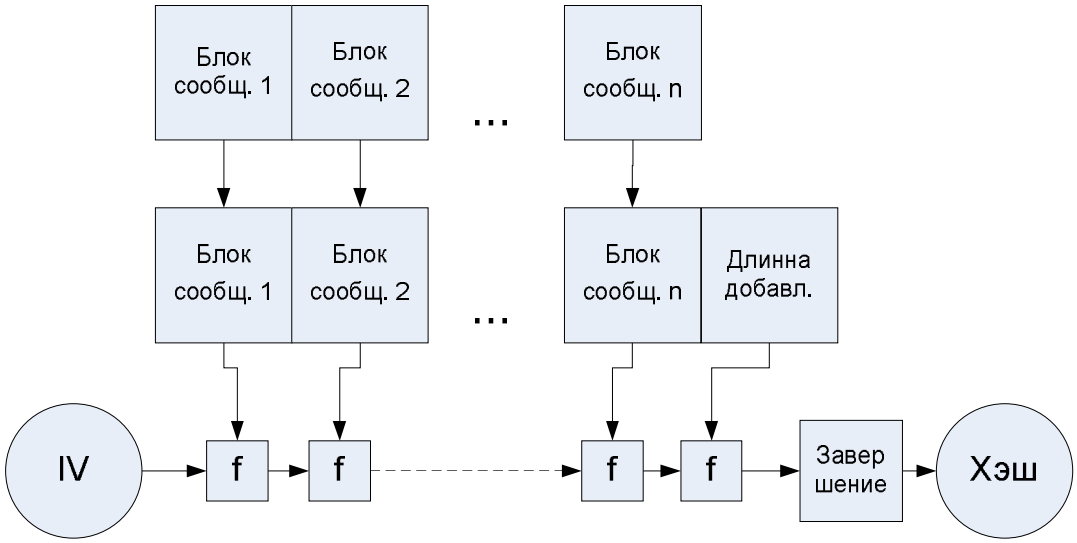

Рис. 1 – Конструкция кодирования хеш-функции согласно структуре Меркла-Дамгарда

Одной из реализованных функций, использующую данную структуру стало семейство алгоритмов Secure Hash Algorithm Version 2. Разработка и описание модели производилось на языке VHDL. Реализация на ПЛИС в программном комплексе Xilinx.

Список использованных источников:

1. Secure Hash Standart [Электронный ресурс]. – Электронные данные. – Режим доступа : http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

2. Лапонина, О. Криптографические основы безопасноти / О. Лапонина // М.: ИНТУИТ, 2004. – 320 с.

3. McEvoy, R. Optimisation of the SHA-2 Family of Hash Function on FPGAs / R. McEvoy, C. Murphy // ISVLC. – 2006. Vol. 2779. – pp. 319 – 333