СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ

Н.О. Карнильчик

Учреждение образования «Белорусский государственный технологический университет», Минск, Беларусь

Было проведено сравнение блочного алгоритма шифрования информации ГОСТ 28147-89 с 256-битовым ключом и 32 раундами на основе сети Фейстеля с алгоритмами защиты информации ГОСТ Р 34.10-2012 с использованием схемы Миягучи-Пренеля и ГОСТ Р 34.12-2018. С точки зрения безопасности ГОСТ 28147-89 считается чрезвычайно надежным и проверялся экспертами на протяжении многих лет. Он использует алгоритм с симметричным ключом, что означает, что один и тот же ключ используется как для шифрования, так и для дешифрования.

Был рассмотрен блочный алгоритм шифрования ГОСТ 28147-89, который был усовершенствован в алгоритме стандарта 1994 г. Описано теоретическое представление сети Фейстеля и приведена ее схема в виде графического способа описания алгоритма. Реализован блочный алгоритм шифрования с 256-битовым ключом и 32 раундами на основе сети Фейстеля для платформы «Windows», язык реализации C++20. Так же реализован алгоритм шифрования информации стандарта 1994 с использованием блочного алгоритма ГОСТ 28147-89 с 256-битовым ключом и 32 раундами на основе сети Фейстеля. Приведены различия реализаций алгоритмов шифрования информации из стандартов 2012 года с использованием схемы Миягучи–Пренеля и 2018.

Продемонстрировано применение отечественного блочного алгоритма шифрования информации и теоретической криптостойкости, и оценена скорость с разными размерами ключей и сетей Фейстеля: с 256-битовым ключом и 64 раундами на сети Фейстеля: с 256-битовым ключом и 32 раундами на сети Фейстеля, с 128-битовым ключом и 32 раундами на сети Фейстеля, с 64-битовым ключом и 32 раундами на сети Фейстеля и с 64-битовым ключом и 16 раундами на сети Фейстеля. В данной работе изучены возможности ускорения и оптимизации алгоритма шифрования ГОСТ 28147-89 [1–3].

Список литературы

1. Ищукова Е.А., Панасенко С.П., Романенко К.С. [и др.] Криптографические основы блокчейн-технологий. М.: ДМК Пресс, 2022. 302 с.

2. Рубин Ф. Криптография с секретным ключом. М. ДМК Пресс, 2022. 386 с.

3. Омассон Ж.-Ф. О криптографии всерьез. М.: ДМК Пресс, 2021. 328 с.

АППАРАТНАЯ РЕАЛИЗАЦИЯ МОДУЛЯ ПРЕОБРАЗОВАНИЯ ХЭШ-ФУНКЦИИ SHA-512 НА БАЗЕ FPGA

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

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

Криптографическая хэш-функция SHA-512 предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины. Данная функция используется для проверки целостности данных, а также в рамках других криптографических алгоритмов и протоколов в различных приложениях, связанных с защитой информации. Поскольку функция SHA-512 использует в своей работе 64-битные слова, она является самой сильной среди функций семейства SHA-2 с точки зрения устойчивости к коллизиям и взлому. Чтобы соответствовать ограничениям