УДК 004.056.55

В.В. СЕЛЮТИНА*, *Л.В. ДЕРБУНОВИЧ, докт. техн. наук, профессор

Компактная и энергоэффективная система потокового шифрования

Проблема тайной передачи сообщений существует столько времени, сколько существует письменность. Для защиты информации используется, прежде всего, шифрование. При шифровании происходит преобразование данных в вид, недоступный для чтения без соответствующей информации (ключа шифрования). Задача состоит в том, чтобы обеспечить конфиденциальность, скрыв информацию от лиц, которым она не предназначена. Современные требования к криптографии накладывают жесткие рамки к скорости обработки информации. В данном ключе актуальными становятся потоковые алгоритмы шифрования.

Алгоритм шифрования RC4 – это симметричный потоковый шифр, который поддерживает различные длины ключа. RC4 допускает различную длину ключа – до 256 байт. Алгоритм RC4 строится, как и любой потоковый шифр на основе параметризованного ключом генератора псевдослучайных битов с равномерным распределением. Основные преимущества шифра — высокая скорость работы и переменный размер ключа, простой алгоритм, назначение каждого шага которого объяснимо и логично. Главные факторы, способствующие широкому применению RC4, – это простота его аппаратной и программной реализации, а также высокая скорость работы алгоритма в обоих случаях. Системы потокового шифрования на основе алгоритма RC4 могут быть использованы для систем защиты данных при передаче по беспроводным каналам связи WEP, шифрования данных в Microsoft Point-to-Point, защиты данных в документах формата PDF, протоколов обмена сообщениями Skype.

Цель работы заключается в реализации программной модели системы потокового шифрования на базе алгоритма RC4. Предложенное решение является программной моделью устройства, реализующей теоретико-числовые преобразования. Система может применяться как при синтезе устройства, так и при непосредственной проверке полученных результатов расчёта с использованием других методов.

Для выполнения поставленной цели разработана структурная схеме, по которой синтезирована компьютерная модель генератора ключевой последовательности и самого алгоритма в целом. На рисунке 1 представлена структурная схема модуля, выполняющего шифрование в соответствии с алгоритмом RC4. Схема состоит из 2-х 8-разрядных двоичный счетчиков («Счетчик i» и «Счетчик j» — накопительный счетчик-сумматор с неравномерным шагом), модуля памяти («S-блок»), сумматора по модулю 256 («Сумматор mod 256») и К-блока – выдает на выходе ключевую последовательность.

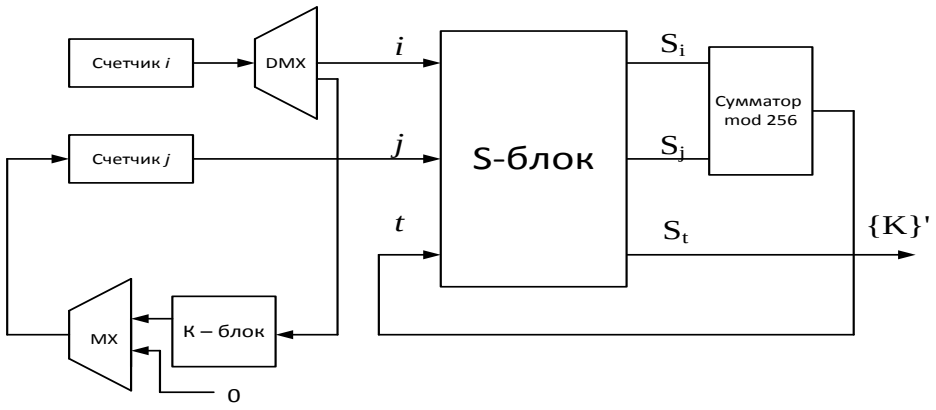

Рис. 1 – Структурная схема модуля шифрования

В среде проектирования цифровых устройств Active-HDL синтезирована многовыходная комбинационная схема потокового шифрования, реализующая структурную схему (рис. 1), и проведено исчерпывающее функциональное моделирование, результаты которого изображены на рисунке 2.

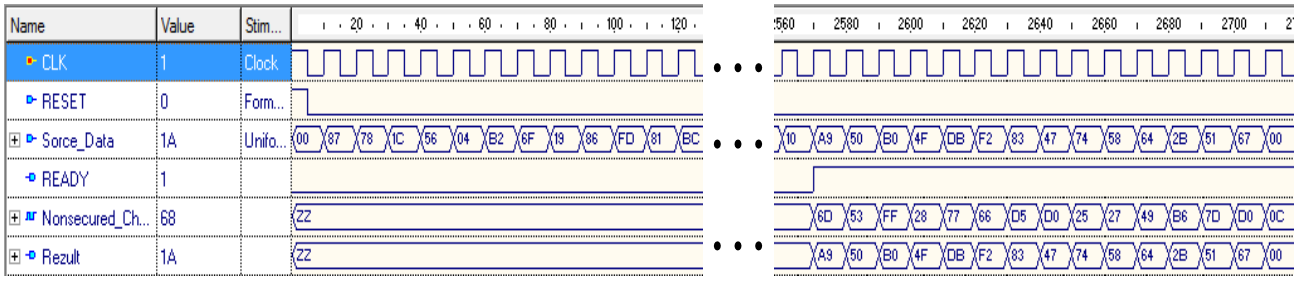

Рис. 2 – Результаты моделирования системы шифрования

Результаты моделирования показывают высокую эффективность системы. Шифрование по алгоритму RC4 примерно в 10 раз быстрее, чем шифрование DES при программной реализации. Основные преимущества шифра – высокая скорость работы и переменный размер ключа.

Список литературы:

1. Баричев С. Г, Серов Р. Е. Основы современной криптографии: Учебное пособие. – М.: Горячая линия – Телеком, 2002.

2. Ю. В. Ветров, С. Б. Макаров. Криптографические методы защиты информации в телекоммуникационных системах: Учебное пособие. – СПб.: Изд-во Политехнического университета, 2011. – 174с.

3. Сергиенко А.М. VHDL для проектирования вычислительных устройств. – К.: ЧП «Корнейчук», ООО «ТИД «ДС», 2003. – 208 с.

4. Б. Шнайер. Прикладная криптография. Второе издание – М.: Триумф, 2002. – 816 с.