АППАРАТНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ШИФРОВАНИЯ DES НА БАЗЕ FPGA

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

Уваров Н.С.

Качинский М.В.–к.т.н., доцент

Аннотация – В современном мире не обойтись без сохранения данных, алгоритмы шифрования присутствуют везде. В данной работе был поставлена задача реализация DESшифрования на базе FPGAс использованием конвейера.

DES (Data Encryption Standard) — симметричный алгоритм шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт (FIPS 46-3). DES имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для DES рекомендовано несколько режимов.

На рисунке 1 приведена структурнаясхема, реализующая алгоритм шифрования DES:

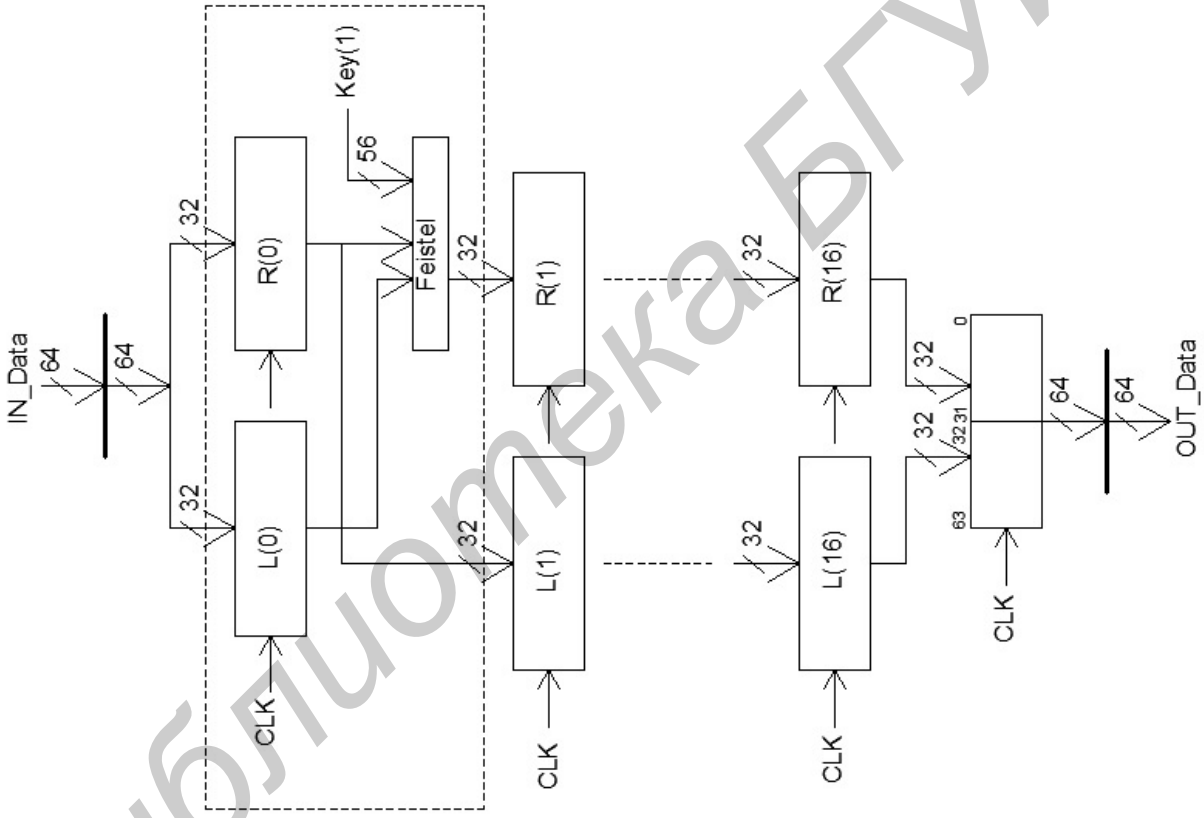

Рис. 1 – Структурная схема быстрого алгоритма шифрования DES

В ходе проведённой работы был спроектирован алгоритм шифрования DES на базе конвейера.

DES был национальным стандартом США в 1977—1980 гг., но в настоящее время DES используется (с ключом длины 56 бит) только для устаревших систем, чаще всего используют его более криптоустойчивый вид (3DES, DESX). 3DES является простой эффективной заменой DES, и сейчас он рассмотрен как стандарт.Алгоритм DES широко применяется для защиты финансовой информации: так, модуль THALES (Racal) HSM RG7000 полностью поддерживает операции TripleDES для эмиссии и обработки кредитных карт VISA, EuroPay и проч. Канальные шифраторы THALES (Racal) DataDryptor 2000 используют TripleDES для прозрачного шифрования потоков информации. Также алгоритм DES используется во многих других устройствах и решениях THALES-eSECURITY.

Список использованных источников:

1. Панасенко С.П., “Алгоритмы шифрования. Специальный справочник”СПб.:БВХ- Петербург, 2009.
2. Бибило П.Н., “Основы языка VHDL”, Изд. 3-е доп., -М.: Издательство ЛКИ, 2007.