УДК 004.056.55

Д.Р. ПРИХОДЬКО*, *Д.Г. КАРАМАН, ассистент

Аппаратный модуль защиты данных на базе стандартизированного симметричного криптографического алгоритма

Применение криптографии является надежным способом для идентификации объектов, защиты и обеспечения целостности данных. Для безопасной передачи данных используют аппаратные и программные средства.

Не смотря на то, что криптографические методы защиты информации постоянно развиваются и усложняются, не теряют актуальность и популярность алгоритмы, изобретенные ранее. Ярким примером таких решений является симметричный блочный криптографический алгоритм DES. Благодаря своей простоте реализации, высокому быстродействию и своей лицензионной свободе алгоритм DES получил широкое распространение в областях, для которых уровень его криптографической надежности и крипто аналитической стойкости является приемлемым. Задача разработки универсального недорогого масштабируемого модуля защиты данных на базе криптографического алгоритма DES является актуальной и востребованной.

Для решения этой задачи был выполнен анализ современной элементной базы и современных методов проектирования цифровых устройств и их компонентов, который позволил выбрать наиболее экономически и технологически эффективный способ реализации модуля защиты информации. Также была разработана структурная и принципиальная схема устройства.

DES осуществляет шифрование 64-битовых блоков данных с помощью 56-битового ключа. Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, обратной перестановке битов. На рисунке 1 представлена структурная схема модуля шифрования.

По приведённой структурной схеме разработаны принципиальные схемы устройства, а также проработаны алгоритмы его функционирования. В среде проектирования цифровых устройств Active-HDL синтезирована функциональная модель системы шифрования в виде многовыходной комбинационной схемы и управляющего автомата. После этого был проведён анализ и выбор наиболее подходящей элементной базы и проведено функциональное моделирование системы шифрования.

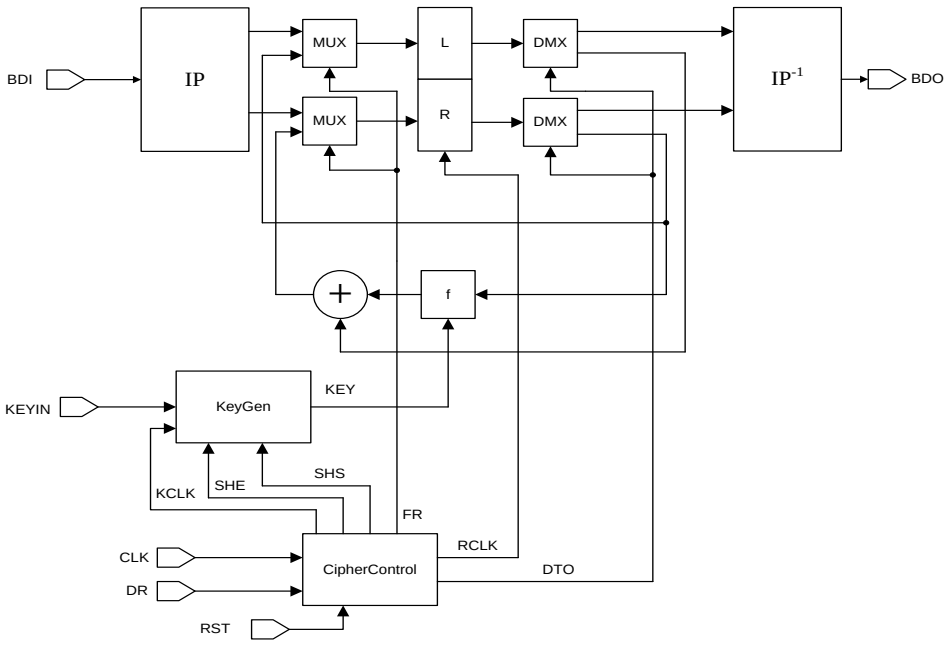

Рис. 1 – Схема шифрования метода DES

Результаты функционального моделирования, которые были получены в процессе выполнения эксперимента, изображены на рисунке 2.

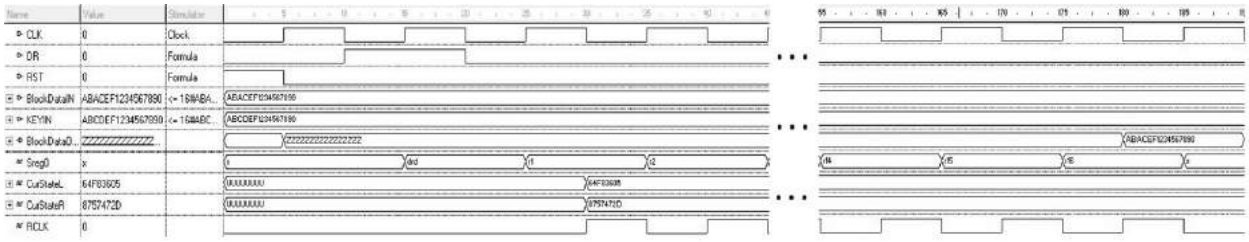

Рис. 2 – Результаты моделирования системы шифрования

Результаты проведенного моделирования и функционального анализа показывают, что разработанная модель не уступает аналогам по функциональности, быстродействию, занимаемым аппаратным ресурсам. Представленное решение может быть реализовано как индивидуальное самостоятельное устройство, такое как криптопроцессор, либо структурный компонент в составе более сложного цифрового устройства.

Список литературы:

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

2. Аппаратные и программные реализации DES [Электронный ресурс] // Режим доступа: http://r3al.ru/kripto_2/apparatnye_i_programmnye_realiza.htm.

3. Data encryption standard (DES) // Federal information processing standards publication (FIPS) – 1999.