ES1040 – DES Core

Introduction

ES1040 core implements Data Encryption Standard (DES) cipher algorithms in hardware. DES is a block cipher, works on blocks of 64 bits of data using 64 bit long keys. However, every 8th key bit is an odd parity bit and is ignored in the DES algorithm. Hence the effective key size is 56 bits.

ES1040 core also supports Triple Data Encryption Algorithm (Triple-DES). Triple-DES is DES done three times with three different keys.

Features

- ✓ Supports both encryption and decryption
- ✓ Designed in a way to make resource sharing easier
- ✓ DES throughput – 640Mbps when clock running at 100Mhz
  - Implements 2 rounds per clock period
- ✓ Triple DES throughput – 220Mbps when clock running at 100Mhz
  - Single DES block used for Ecrypt/Decrypt/Encrypt sessions of 3DES.
  - Throughput can be increased to 640Mbps by instantiation three DES blocks
- ✓ Allows Time Division Multiplexing (TDM) of several data streams.
- ✓ Simple external interface
- ✓ Minimal gate count.
- ✓ Available in ASIC and FPGA Technologies.

Applications

- Secure corporate communications

  - Virtual Private Networks (VPN)
  - Storage Area Networks (SAN)
  - Video conferencing
  - Voice services

- Secure electronic transactions

  - Medical files
  - Financial files
  - Securities exchange
  - eCommerce
  - Point-of-Sale

- Personal mobile communications

  - Video phones
  - PDA
  - Point-to-Point Wireless

Pin Description

Name	I/O	Width	Description
clk	Input	1	Positive edge clock
rst_n	Input	1	Active low asynchronous reset
dataInVld	Input	1	Validates data and key
encryptionMode	Input	1	1: encryption; 0: decryption
tripleDesEn	Input	1	Enables triple des mode
dataIn	Input	64	Data – text
Busy	Output	1	dataInVld should be asserted only when DES block is not busy
key1In	Input	64	Key1 with parity bits
key2In	Input	64	Key2 with parity bits (used only when tripleDes is enabled)
key3In	Input	64	Key3 with parity bits (used only when tripleDes is enabled)
dataOut	Output	1	Validates dataOut
dataOutVld	Output	64	Deciphered data

Functional Description

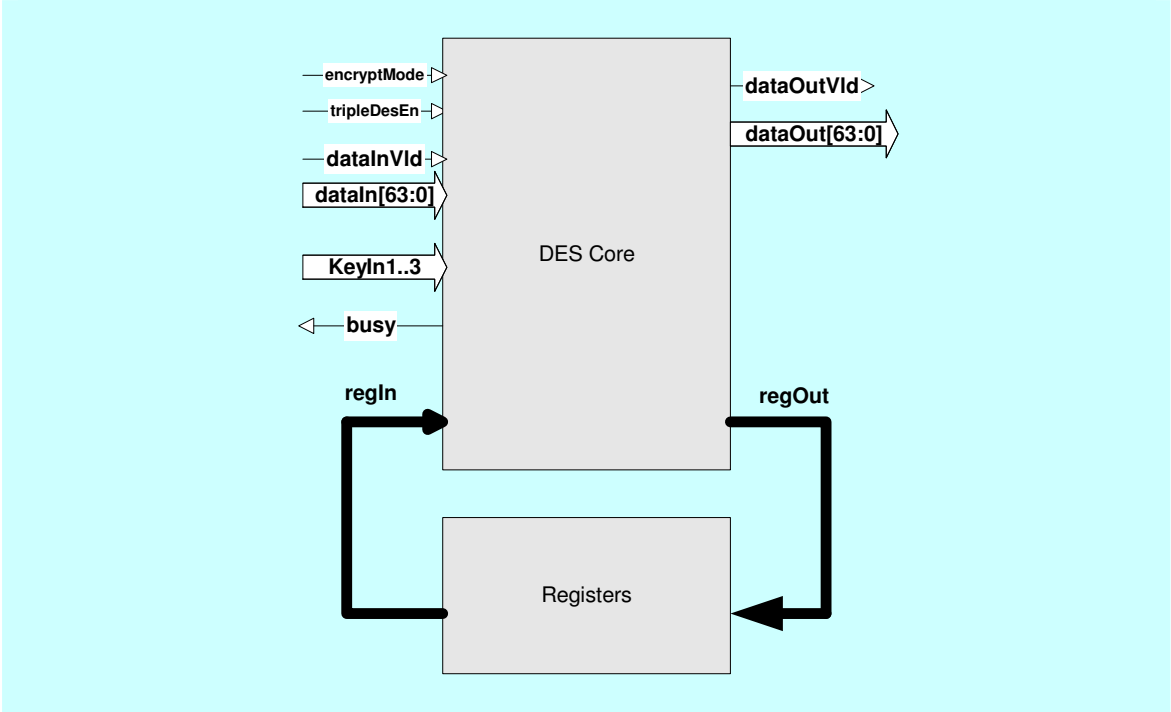

Figure 1. ES1040 Symbol

ES1040 has two modes of operation: DES mode and Triple DES mode. Both Encryption and decryption are supported in each of these modes. Figure 2 shows the interface timing diagram of ES1040. The Keys, dataIn and encryptionMode signals to the block are sampled when the dataInVld signal is asserted. Key2 and Key3 should remain valid until busy signal is deasserted.

References

- For a good description of DES algorithm please refer to the book “Applied Cryptography” by Bruce Schnier, pages 271-280
- For an implementation example, refer to the electronic document titled “The DES Algorithm Illustrated” by J. Orlin Grabbe
- For a good pictorial representation of the same algorithm, refer to online version of “Handbook of Applied Cryptography” by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, chapter 7

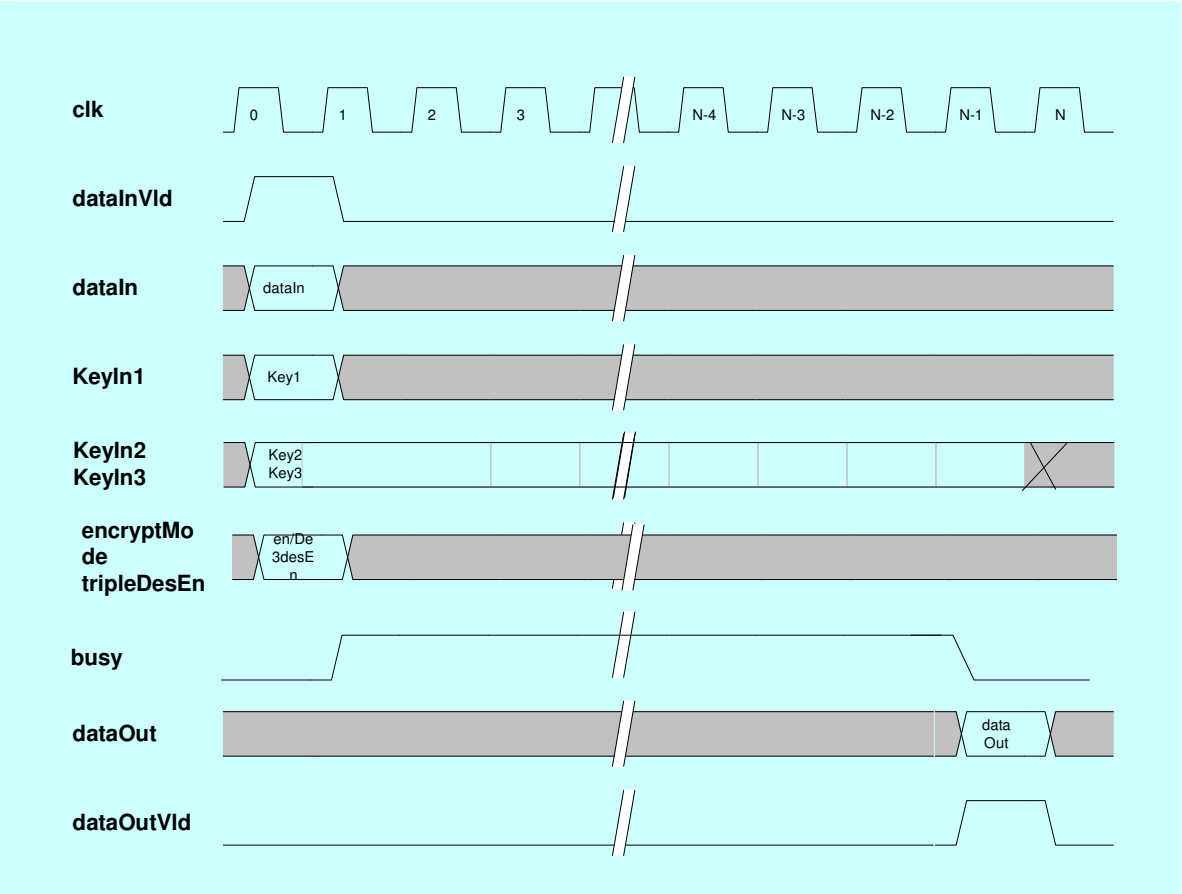

Figure 2. ES1040 Interface Timing Diagram

Deliverables

- ✓ Synthesizable Verilog RTL source code
- ✓ Simulation scripts
- ✓ Self-checking Test environment
  - ➢ Test-bench
  - ➢ Test-vectors
  - ➢ Expected results
- ✓ Synthesis scripts
- ✓ User Documentation

Sales Representatives

For pricing information:

Esencia Technologies Inc.
2041 Mission College Blvd., Suite #100
Santa Clara CA, 95054
Tel: (408) 736-8284
Web: www.esenciatech.com
E-mail: sales@esenciatech.com

About Esencia

Esencia Technologies is a leading provider of pre-verified virtual components for consumer electronics and communication markets at competitive prices.