

General Description

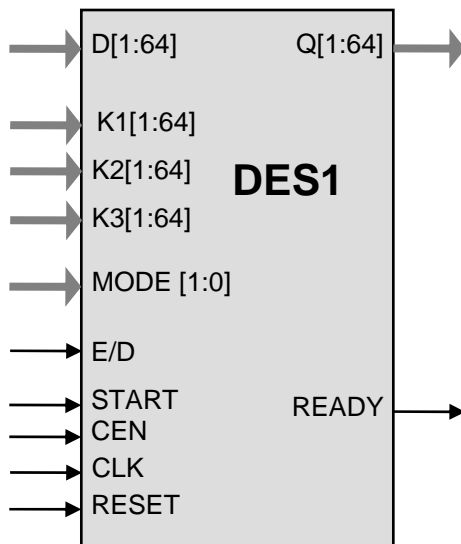
The DES1 core implements DES and triple DES encryption and decryption in compliance with the NIST Data Encryption Standard. It processes 64-bit blocks, with one, two, or three 56-bit keys.

Basic core is very small (3,000 gates). Enhanced versions are available that support various cipher modes (ECB, CBC, OFB, CFB, CTR), as well as different datapath widths for size/performance tradeoff.

The design is fully synchronous and available in both source and netlist form. Test bench includes the NIST DES test vectors.

DES Core is supplied as portable Verilog (VHDL version available) thus allowing customers to carry out an internal code review to ensure its security.

Symbol



Base Core Features

Encrypts and decrypts using the DES Block Cipher Algorithm

High throughput: up to 3 Gbps at 750 MHz in 90 nm LV technology

Small size: from 3K ASIC gates for a triple DES core

Satisfies FIPS 46-3 from the US National Institute of Standards and Technology (NIST)

Processes 64-bit data blocks

Employs one to three keys of 56 bits each

Completely self-contained: does not require external memory

Available as fully functional and synthesizable Verilog, or as a netlist for popular programmable devices and ASIC libraries

Deliverables include test benches

Applications

- Secure mobile phone communications
- Secure RFID
- Secure Smart Cards
- Secure financial transactions

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
RESET	Input	Core reset signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
START	Input	When goes HIGH, a cryptographic operation is started
E/D	Input	Encrypt (1) / Decrypt (0)
MODE[1:0]	Input	DES mode 0 – Single DES 1 – Double DES 2 – Triple DES
READY	Output	Output data ready and valid
K1[1:64]	Input	First Encryption Key
K2[1:64]	Input	Second Encryption Key (used only in Double or Triple mode)
K3[1:64]	Input	Third Encryption Key (used only in Triple mode)
D[1:64]	Input	Input Plain or Cipher Text Data
Q[1:64]	Output	Output Cipher or Plain Text Data

Function Description

An DES encryption operation transforms a 64-bit block into a block of the same size. The encryption key size is 56 bits, with one to three keys used. The block performs DES encryption as defined by NIST in FIPS 46-3.

Ultra-Compact Data Encryption Standard Core

Operation

A rising input on the START port triggers the beginning of a cryptographic operation on the data D, using the KEY as key. It then starts to process the state according to the DES algorithm.

When all the rounds are completed, the READY signal is raised and the encrypted data is available on the output.

It is possible to start a new cryptographic operation as soon as the data from the previous one is output. A cryptographic operation can be aborted at any time by lowering the START signal for at least one clock cycle.

The core is fully pipelined. Loading of the new plain/cipher text data and key can be combined with outputting cipher/plain text data from the previous operation.

New key can be used for each cryptographic operation. The absence of gaps allows sustaining the throughput of 4/2/1.33 bits per clock for DES / 2DES / 3DES correspondingly.

Implementation Details

Representative synthesis results are shown below.

Technology	Max Frequency	Area	DES Throughput	3DES Throughput
TSMC 130 nm	234 MHz	3,117 gates	936 Mbit/s	312 Mbit/s
TSMC 130 nm	512 MHz	4,482 gates	2,048 Mbit/s	684 Mbit/s
TSMC 90 nm	358 MHz	3,192 gates	1.4 Gbit/s	477 Mbit/s
TSMC 90 nm	789 MHz	5,090 gates	3.15 Gbit/s	1 Gbit/s

Export Permits

See the IP Cores, Inc. licensing basics page, http://ipcores.com/export_licensing.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Test vectors
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Test vectors
- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 814-0205
E-mail: info@ipcores.com
www.ipcores.com