

## Cryptographic Processor Core for the DES Algorithm IPMS\_DES

### Fraunhofer-Institut Photonische Mikrosysteme

Maria-Reiche-Str. 2  
01109 Dresden  
Phone: +49 (0) 3 51/88 23-0  
Fax: +49 (0) 3 51/88 23-266  
www.ipms.fraunhofer.de

Contact:  
Ines Schedwill  
Phone: +49 (0) 3 51/88 23-238  
ines.schedwill@ipms.fraunhofer.de

Technical questions:  
Dr. Andreas Heinig  
Phone: +49 (0) 3 51/88 23-288  
andreas.heinig@ipms.fraunhofer.de



**Quality Management**

**We are certified**

Voluntary participation in regular  
monitoring according to ISO 9001:2008

Fraunhofer IPMS reserves the right to change products and specifications without prior notice. This information does not convey any license by any implication or otherwise under patents or other right. Application circuits shown, if any, are typical examples illustrating the operation of devices. Fraunhofer IPMS cannot assume responsibility for any problems rising out of the use of these circuits.

### Overview

Cryptography has been in use since ancient times as a method to secure messages. Radio transmission, chip cards of every description, data and computer networks with large amounts of stored data require security systems.

The "Data Encryption Standard" (DES) is a description of a mathematical algorithm to encrypt and decrypt binary data sets. The DES (fig. 1) is a secret key cryptosystem. All authorized users must know this key. The coder substitutes the 64 bit wide data set  $x$  with the 64 bit data set  $y$  – the cipher. The key width is 56 bits.

Because of the high performance of modern computers a brute-force attack against the DES becomes possible due to the low key size. On the assumption that the DES forms no mathematical group it is possible to increase the key sizes with the help of multiple encryption. With a triple DES a key size of 112 bit can be gained.

The hardware realizes a flexible DES core to encrypt and decrypt data with high speed. The encryption/decryption of a 64 bit data set takes 16 clock periods. The core is completed with several interfaces.

### Characteristics

- Processor core for the Data Encryption Standard (DES) like the Federal Information Processing Standards **P**ublication **46-2**, National Institute of Standards and Technology, 1993
- VHDL model compatible with IEEE 1076-1987, usable as a macro cell in ASICs

### Usage

- High speed data encryption/decryption in parallel ISA/PCMCIA systems
- Data encryption/decryption in serial systems (RS-232 interface)

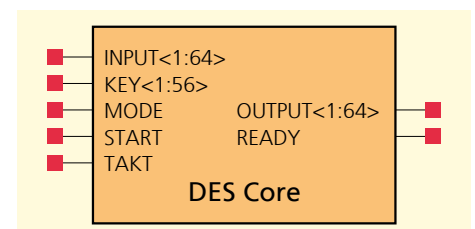


Fig. 1: Cryptographic processor core implementing the DES algorithm

Pin name	I/O	Function
INPUT	I	data input 64 bit
OUTPUT	O	data output 64 bit
KEY	I	key input 56 bit
MODE	I	select: encrypt/decrypt
START	I	start
TAKT	I	clock
READY	O	ready for encryption/decryption, encryption/decryption completed

Fig. 2: Pin description

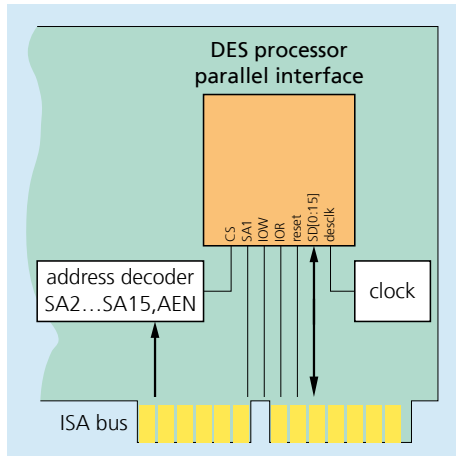


Fig. 3: Application example

### Area (NAND2 equivalent gates)

- DES core: 1922
- serial interface: 945
- parallel interface: 366

### Description

The first demonstrator (fig. 3) allows the connection of the DES core to a 16-bit width bus system, like the ISA bus or the PCMCIA bus in personal computers. The host computer can access the cryptographic processor in its memory or input/output address area.

The second example (fig. 6) combines the DES core with a serial interface like the RS-232 standard. The chip is connected in an existing serial data path. At the end of the data path another cryptographic processor decrypts the data stream.

Since the key in a symmetric-key algorithm must be kept secret, it cannot be part of the transmission. Therefore a ROM for the keys exists at every processor. A counter selects the keys, which are used likewise at the encrypting and the decrypting unit. Because of the block size of the DES the data stream is partitioned in 64 bit blocks. Data buffering enables the processing of a continuous data stream.

DES_parallel	unit	min	typ	max
Supply voltage	V	4.5	5.0	5.5
Operating current (at 10 MHz)	mA			10.0
Idle current	µA			100
Clock frequency	MHz			20

Fig. 4: Operating conditions

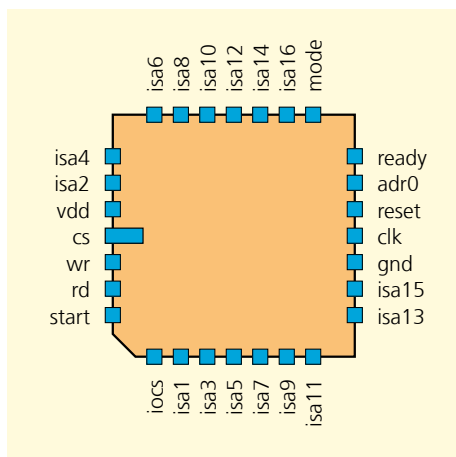


Fig. 5: Pinning of the parallel circuit

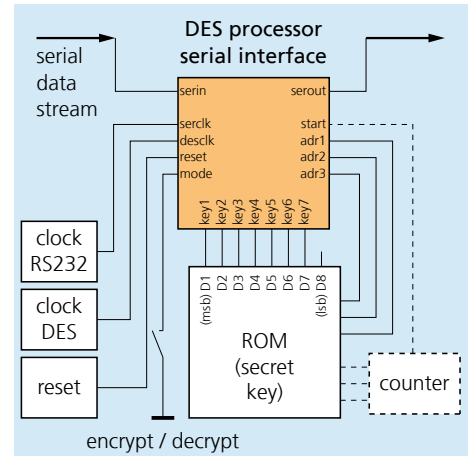


Fig. 6: Application example

DES_serial	unit	min	typ	max
Supply voltage	V	4.5	5.0	5.5
Operating current (at 10 MHz)	mA			10.0
Idle current	µA			100
Clock frequency	MHz			10

Fig. 7: Operating conditions

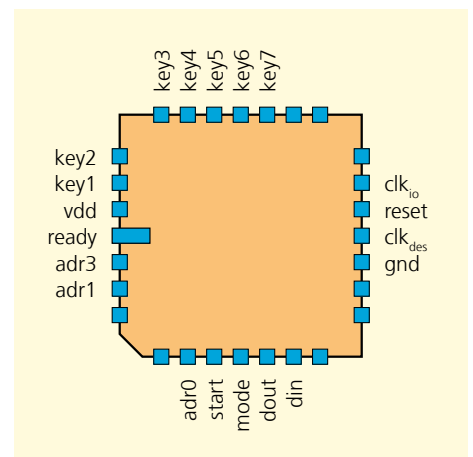


Fig. 8: Pinning of the serial circuit