

Cryptography process core according to AES standard IPMS_AES

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 against unauthorized access.

The "Advanced Encryption Standard" (AES), original Rijndael, includes the description of a mathematical algorithm for ciphering binary coded data. Since November 2001 it has been standardized as Standard FIPS Pub 197. It is based on a secret key that has to be known by every user.

In this polygraphic substitution cipher a data block x is replaced by a data block y . The block size is defined in the standard as 128 bit. The key width can constitute 128, 192 or 256 bit. The encryption and decryption are different operations. The IPMS_AES supports both.

The IPMS_AES has been developed as an all-purpose macro cell in a synthesizable hardware description and therefore it can be employed in FPGAs, but it is also easy to integrate in an ASIC.

The AES core is completed with three different interface devices, tested in silicon and can be employed as a cryptography processor circuit. By implementation of a special hardware solution a high velocity is achieved, the algorithm is temper-proof and can be implemented with small mechanical dimensions.

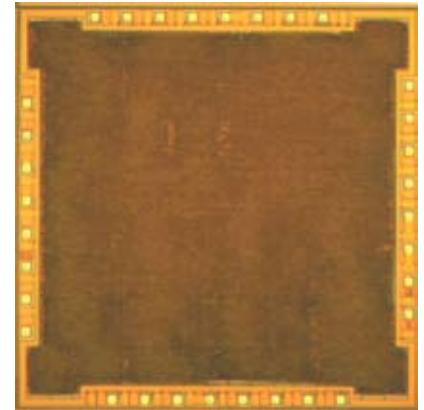


Fig. 1: Chip microphotograph of the IPMS_AES.

Features

- Hardware implementation of Advanced Encryption Standard (AES) after Federal Information Processing Standards **P**ublication **197**, National Institute of Standards and Technology, 2001.
- Synthesizable VHDL model after IEEE standard 1076-1987 for the employment as macro cell in ASICs.
- High processing speed of 100 Mbit/s (128 bit key, 25 MHz). Same speed for coding and decoding.
- Key widths of 128, 192 and 256 bit are implemented
- Dimensions with interface are 16 mm² in a 0.5 μ m CMOS technology. The AES core itself enfolds 120 kGates.

IPMS_AES	in	min	typ	max
Supply voltage	V	3.0	3.3	3.6
Operating current (at 25 MHz)	mA		10	20
Idle current	μ A		1	100
Clock frequency	MHz			25

Fig. 2: Operating conditions

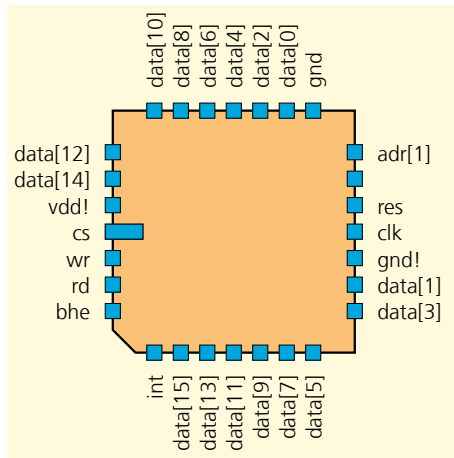


Fig. 3: Pinning of IPMS_AES in parallel mode, LCC28 package.

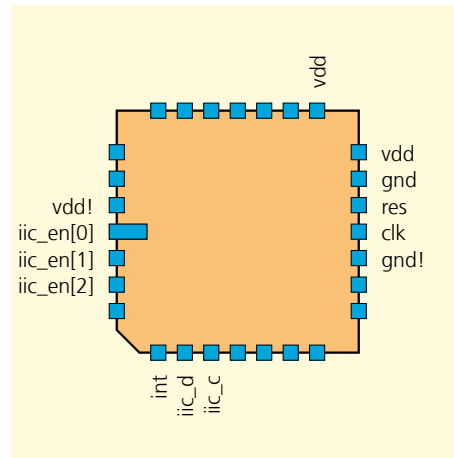


Fig. 5: Pinning of IPMS_AES in I2C mode, LCC28 package.

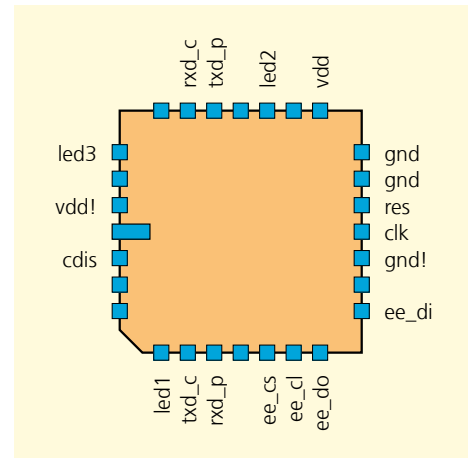


Fig. 7: Pinning of IPMS_AES in serial mode, LCC28 package.

IPMS_AES: parallel interface

The module of the AES cluster in connection with the parallel interface enables to make an AES hardware coding available to a host system (processor, DSP, micro controller).

The data and key exchange as well as the control occurs over a 8 or 16 bit wide parallel bus. The module of the AES cluster with the parallel interface combines the high security by cryptography with a high data throughput.

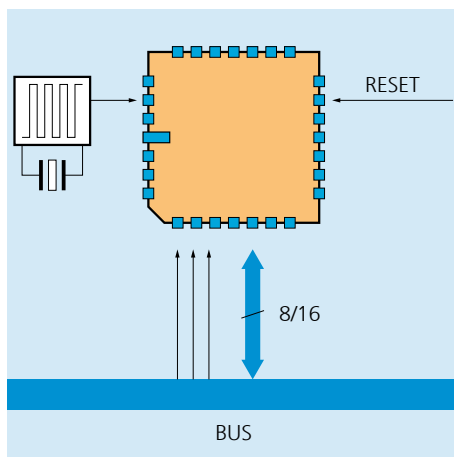


Fig. 4: Parallel system with IPMS_AES.

IPMS_AES: I2C interface

The module of the AES cluster in connection with the PC interface makes hardware encryption/decryption available to a host system (processor, DSP, micro controller).

The data and key exchange as well as the control occurs in this case via an I2C bus. The module of the AES cluster with the I2C interface combines the high security by cryptography with a minimum amount of wiring.

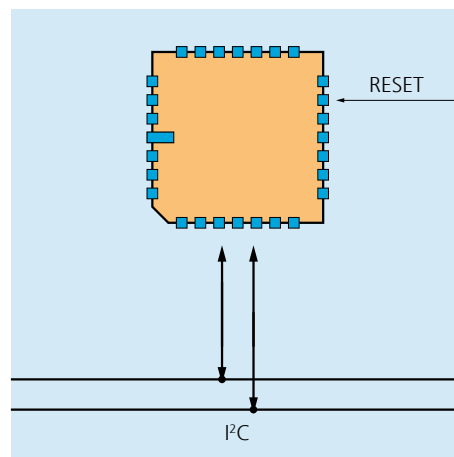


Fig. 6: I2C system with IPMS_AES.

IPMS_AES: serial interface

The module of the AES cluster in connection with the serial interface enables an autonomous encryption/decryption of a bidirectional serial data stream.

The module includes separate channels for data encryption/decryption. Existing serial transmission networks can be enhanced with a single module at each the beginning and end of the area to protect with small effort and without modifications in the existing system.

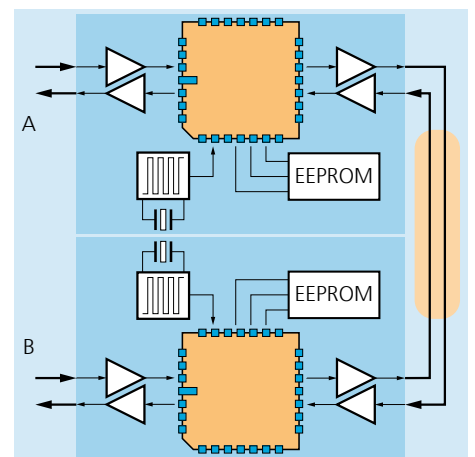


Fig. 8: Serial system with IPMS_AES.