

## Cryptographic Processor Core for Public Key En- cryption IPMS\_RSA

### Overview

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

Asynchronous cryptographic algorithms use a private and a public key – thus enabling a good key management in the system. Many of these asynchronous algorithms involve exponentiation modulo a number  $n$ , the most known algorithm is the RSA (Rivest-Shamir-Adleman cryptosystem).

To reach a good security long key sizes are necessary, a typical key size is 1024 bit. The hardware realization (fig. 1) IPMS\_RSA calculates  $C=E*D \bmod N$  and  $C=E**D \bmod N$  with a very high data rate.

The modules are cascadable, therefore the bit size of the calculation can be optimized and the IPMS\_RSA is “ready” for future requirements in security.

The interface to the circuit is a 8/16 bit wide bus. The module is available as a VHDL synthesizable behavioral description – this makes it possible to transfer it into other technologies and optimize it for various requirements.

The pin description is provided in fig. 2.

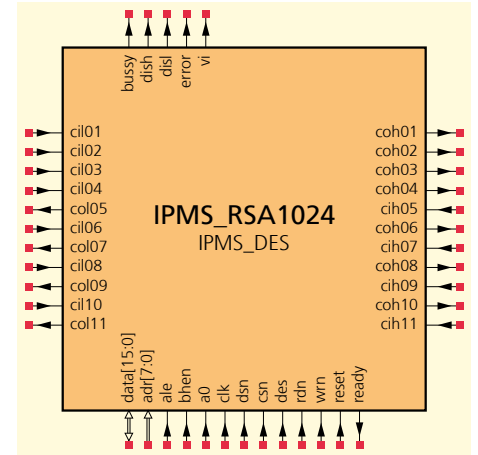


Fig. 1: RSA processor core

Pin name	I/O	Function
data	IO	8/16 bit data bus
adr	I	addresses
ale	I	address latch enable
bhen	I	bus high enable
a0	I	address at 8 bit mode
clk	I	system clock
dsn	I	device select
csn	I	chip select (RSA)
des	I	chip select (DES)
rdn	I	read enable
wrn	I	write enable
reset	I	system reset
ready	O	interrupt
cil01, cil02, cil03, cil04, cil06, cil08, cil10 cil05, cil07 cil09, cil11	IO	to the next IPMS_RSA* (lower significant bits)
coh05, coh07, coh09 coh11, coh01, coh02, coh03, coh04, coh06, coh08, coh10	IO	to the next IPMS_RSA* (higher significant bits)
bussy, dish, disl, error, vi	O	for test purposes
		*) optional

Fig. 2: Pin description

### 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



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.

## Characteristics

- processor core for modulo  $n$  multiplication and exponentiation (RSA) with high speed and high bit sizes
- Data rates (for a 1024 bit system at 25 MHz clock frequency)
  - 1024 bit RSA up to 10 kbit/s
  - 512 bit RSA up to 32 kbit/s
- VHDL model compatible with IEEE 1076-1987, usable as a macro cell in ASICs

## Applications

- public-key cryptosystems
- asynchronous coding and authentication systems
- RSA encryption/decryption

## Area (NAND2 equivalent gates)

- RSA-core: 117.600 per 1024 bit

## Description

The demonstrator includes a  $C = E \cdot D \bmod N$  and a  $C = E^* \cdot D \bmod N$  calculation for up to 1024 bit size. The bit size or the data rate can be increased when two or more devices are cascaded (fig. 4).

The 16 bit wide parallel interface allows to include the IPMS\_RSA in different host systems, for example ISA or PCMCIA systems. The 8 bit mode makes it possible to connect the IPMS\_RSA directly to microcontrollers.

Additionally the circuit includes a modified DES processor core IPMS\_DES (please refer to the IPMS\_DES information sheet). This core is optimized to work together with the IPMS\_RSA and allows high speed data encryption with the synchronous DES algorithm (Triple-DES, 5-fold-DES, 7-fold-DES) – the best solution for cryptographic systems transferring a session key with an asynchronous algorithm, but using the high speed of the synchronous algorithm for the data.

IPMS_RSA	in	min	typ	max
Supply voltage	V	3,0	3,3	3,6
Operating current (at 10 MHz)	mA			100
Idle current	μA			1
Clock frequency	MHz		8	

Fig. 3: Operating conditions

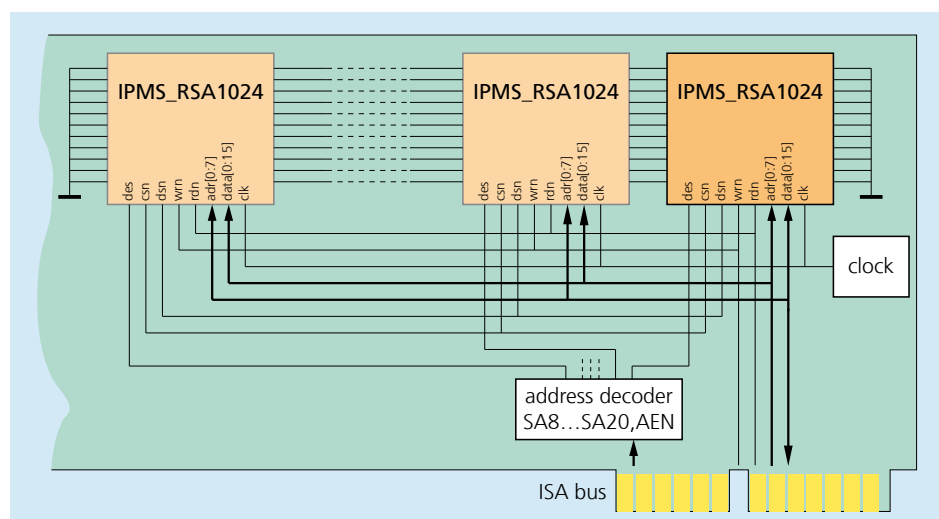


Fig. 4: Application example