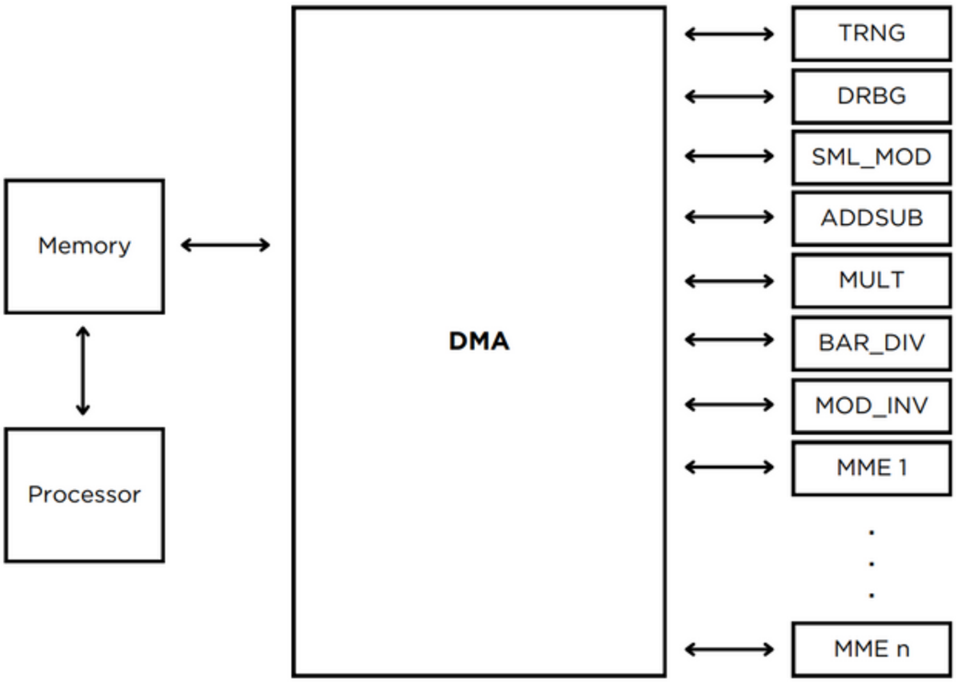
RSA Keygen IP Core
Datasheet

November 2024

OVERVIEW

RSA Keygen IP Cores perform key generation in compliance with the RSA Key Pair Generation specifications defined in 'FIPS 186'. This standard specifies methods for generating RSA key pairs. RSA Keygen IP Cores support key pair generation up to 4096 bits.

RSA Keygen IP cores consist of a cluster of IPs. VHDL is used as the Hardware Description Language of the IP Cores. The cluster includes TRNG, DRBG, SML_MOD (Small Mods), ADDSUB (Addition and substruction), MULT (Multiplication), BAR_DIV (Barrett Divider), MOD_INV (Modulo Inversion) and MME (Montgomery Modulo Exponentiation) IP Cores. MME cores are configurable and their number can be changed. The maximum supported number of MMEs is 4.



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

Technology Partner

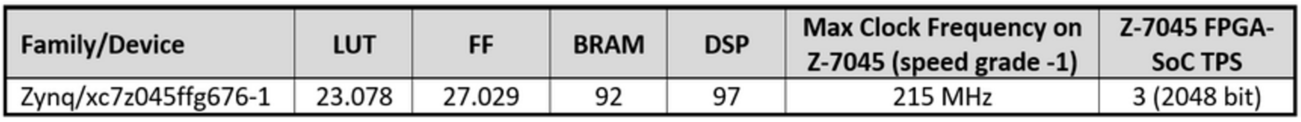
FEATURES LIST

RSA Keygen IP Core:

- supports key pair generation up to 4096 bits.
- is compliant with FIPS 186.
- is tested on Z-7015 Z-7020 Z-7045
- has fully stallable input and output interfaces.

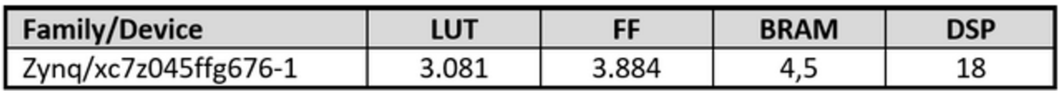
FPGA SYNTHESIS RESULTS

The FPGA resources requirements. The provided resource consumption values are for the case where each MME core uses 18 DSPs and there are 4 MME cores in the system.



Family/Device	LUT	FF	BRAM	DSP	Max Clock Frequency on Z-7045 (speed grade -1)	Z-7045 FPGA-SoC TPS
Zynq/xc7z045ffg676-1	23.078	27.029	92	97	215 MHz	3 (2048 bit)

The FPGA resource requirements for one MME core are based on a configuration that requires 18 DSPs.



Family/Device	LUT	FF	BRAM	DSP
Zynq/xc7z045ffg676-1	3.081	3.884	4,5	18

LICENSING

A one-time license fee is paid with the initial IP purchase.

- Single project license
- Multi project license

MAINTENANCE & SUPPORT

- M&S fee of 15% is mandatory for the first year.
- Telephone and email support is included under M&S contract.
- IP Core updates are included in M&S.

ORDERING

- Purchase order shall include the product number EIP-12009.

Technology Partner

procenne
DIGITAL SECURITY