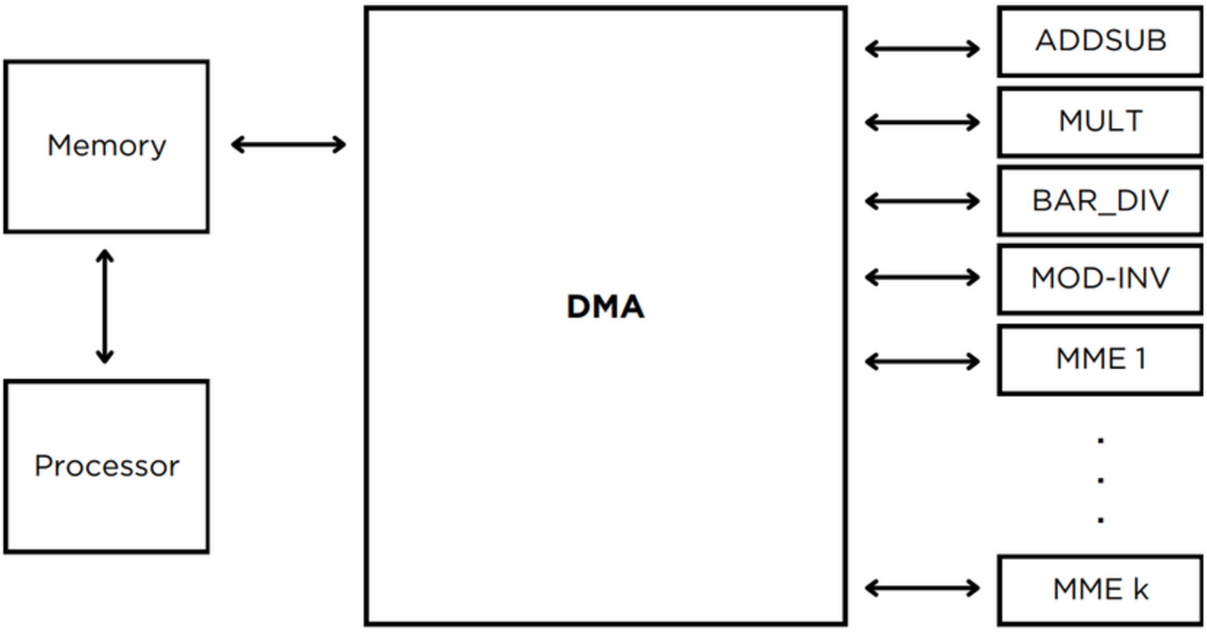
RSA IP Core
Datasheet

November 2024

OVERVIEW

RSA IP Cores perform digital signature generation and verification in compliance with the RSA (Rivest-Shamir-Adleman) Digital Signature Algorithm specifications defined in 'FIPS 186'. This standard specifies methods for digital signature generation and verification using the RSA Digital Signature Algorithm. RSA IP cores support bit lengths from 256 to 4096.

RSA IP cores consist of a cluster of IPs. VHDL is used as the Hardware Description Language of the IP Cores. The cluster includes 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.



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

FEATURES LIST

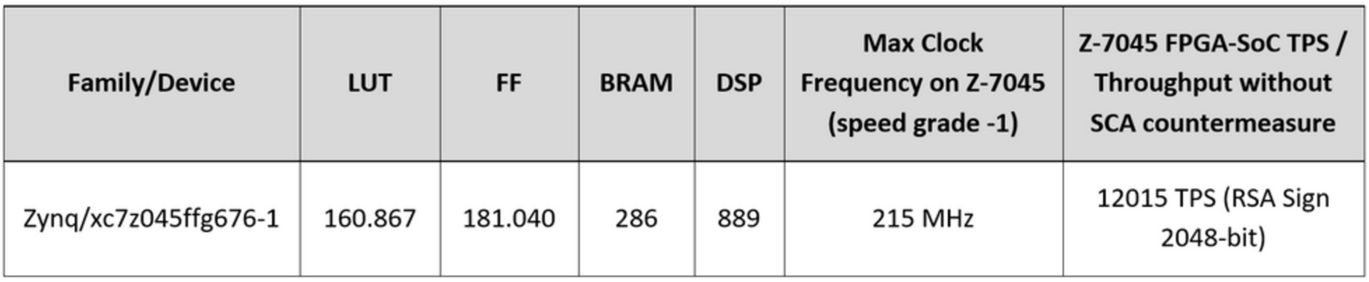
RSA IP Core:

- supports signature generation and verify for bit lengths from 256 to 4096.
- is compliant with FIPS 186.
- is tested Z-7015 Z-7020 Z-7045
- has fully stallable input and output interfaces.

Technology Partner

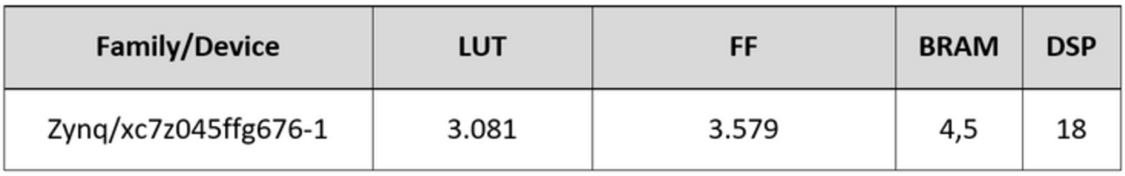
FPGA SYNTHESIS RESULTS

The FPGA resources requirements. The provided resource consumption values are for the case where each MME core uses 18 DSPs and there are 48 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 / Throughput without SCA countermeasure
Zynq/xc7z045ffg676-1	160.867	181.040	286	889	215 MHz	12015 TPS (RSA Sign 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	3.579	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-11009.

Technology Partner

procenne DIGITAL SECURITY