ECDSA IP Core
Datasheet

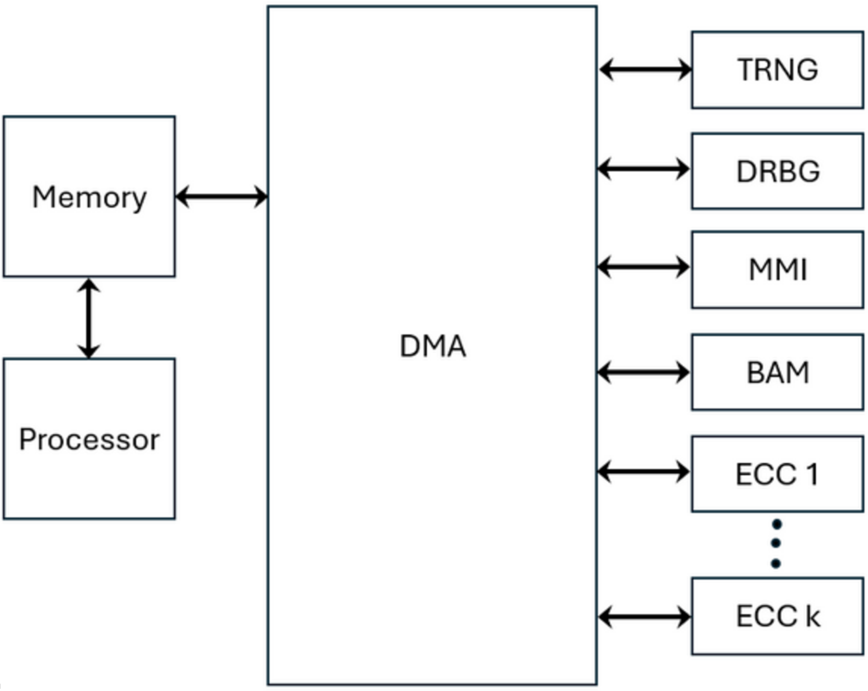
November 2024

OVERVIEW

ECDSA IP Cores perform digital signature generation and verification in compliance with the Elliptic Curve Digital Signature Algorithm (ECDSA) specifications defined in 'FIPS 186'. This standard specifies methods for digital signature generation and verification using the Elliptic Curve Digital Signature Algorithm (ECDSA).

The curves P-192, P-224, P-256, P-384, and P-521 specified in 'SP 800-186', which includes specifications for the generation of the domain parameters used during the generation and verification of digital signatures, are supported.

ECDSA 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, MMI (Montgomery Modulo Inversion), BAM (Barret Reduction, Addition-Substruction, Multiplication) and ECC (Elliptic Curve Cryptograph) IP Cores. The use of the TRNG IP Core and DRBG IP Core is recommended. ECC cores are configurable and their number can be changed.



DELIVERABLES

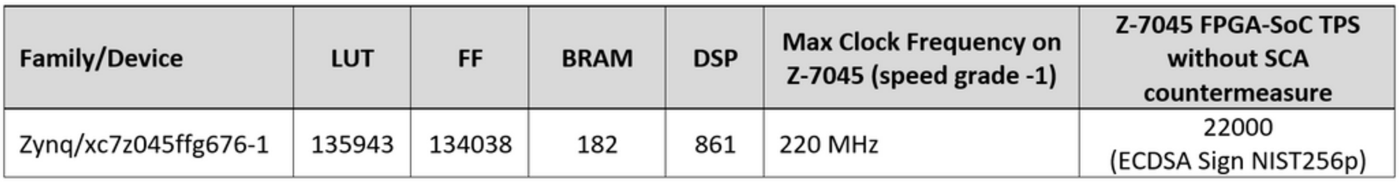
- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

Technology Partner

ECDSA IP Core

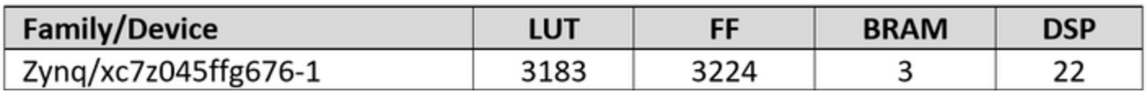
FPGA SYNTHESIS RESULTS

The FPGA resources requirements. The provided resource consumption values are for the case where each ECC core uses 22 DSPs and there are 38 ECC cores in the system.



Family/Device	LUT	FF	BRAM	DSP	Max Clock Frequency on Z-7045 (speed grade -1)	Z-7045 FPGA-SoC TPS without SCA countermeasure
Zynq/xc7z045ffg676-1	135943	134038	182	861	220 MHz	22000 (ECDSA Sign NIST256p)

The FPGA resource requirements for one ECC core are based on a configuration that requires 22 DSPs.



Family/Device	LUT	FF	BRAM	DSP
Zynq/xc7z045ffg676-1	3183	3224	3	22

FEATURES LIST

ECDSA IP Core:

- supports signature generation and verify for curves listed below:
  - *P-192*
  - *P-224*
  - *P-256*
  - *P-384*
  - *P-521*
- is compliant with FIPS 186.
- is tested on Z-7015 Z-7020 Z-7045
- has fully stallable input and output interfaces.

ORDERING

- Purchase order shall include the product number EIP-10009.

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.

Technology Partner