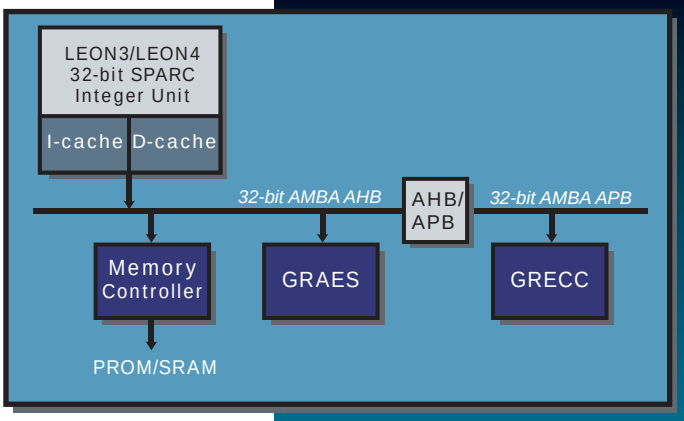
AES & ECC
Cryptography IP Cores

AEROFLEX GAISLER

Description

The Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) cores combine high throughput performance with seamless integration with the LEON3 or LEON4 32-bit SPARC processor cores.

The interfaces of the cores are based on the AMBA on-chip bus. The cores are fully integrated in the GRLIB IP library, including the plug&play interface.



Example cryptography system

Advanced Encryption Standard (AES)

The GRAES core implements the Advanced Encryption Standard (AES) symmetric encryption algorithm for high throughput application.

The implemented AES 128 and 256 algorithms are specified in the Advanced Encryption Standard (AES) - Federal Information Processing Standards (FIPS) Publication 197, established by the National Institute of Standards and Technology (NIST).

The GRAES core is accessed via a 32-bit AMBA AHB slave interface. To facilitate high throughput and low latency, the core utilizes the AMBA retry feature to indicate to the processor that an encryption/decryption is still ongoing. Alternatively, the core provides an interrupt to indicate when encryption/decryption of a block is completed.

Elliptic Curve Cryptography (ECC)

The GRECC core implements Elliptic Curve Cryptography (ECC) which is used as a public key mechanism. The GRECC core implements support for operations on an elliptic curve based on 233-bit key and point lengths. The curve is denoted as sect233r1 or B-233.

The implemented sect233r1 elliptic curve domain parameters are specified in the Standards for Efficient Cryptography (SEC) - SEC2: Recommended Elliptic Curve Domain Parameters, established by the Standards for Efficient Cryptography Group (SECG).

The implemented B-233 elliptic curve domain parameters are specified in the Digital Signature Standard (DSS), Federal Information Processing Standards (FIPS) Publication 186-2, established by the National Institute of Standards and Technology (NIST).

The GRECC core is accessed via a 32-bit AMBA APB slave interface. The core provides an interrupt to indicate when an operation on a 233-bit block is completed.

Availability

The GRAES and GRECC cores are portable and can be implemented on most FPGA and ASIC technologies. The cores are available in VHDL source code or as pre-synthesized netlist. They can be delivered for stand-alone operation or with a wrapper for the GRLIB AMBA plug&play interface.

Specifications

GRAES (AES 128 version):

- AES compatible (FIPS-197)
- AMBA AHB slave interface
- 1.4 Mbits per MHz throughput
- Speed and size:
  68 MHz, 8900 RTAX cells
  125 MHz, 5100 Virtex-2 LUTs
  14500 ASIC gates

GRECC:

- B-233 compatible (FIPS-186-2)
- sect233r1 compatible (SEC2)
- AMBA APB slave interface
- 13.9 kbits per MHz throughput
- Speed and size:
  38 MHz, 19200 RTAX cells
  93 MHz, 12900 Virtex-2 LUTs
  48500 ASIC gates

CONTACT INFORMATION

Aeroflex Gaisler AB
Kungsgatan 12
411 19 Göteborg
Sweden

Tel: +46 31 7758650
Fax: + 46 31 421407

Sales contact:
sales@gaisler.com
www.aeroflex.com/gaisler

2010 SEP