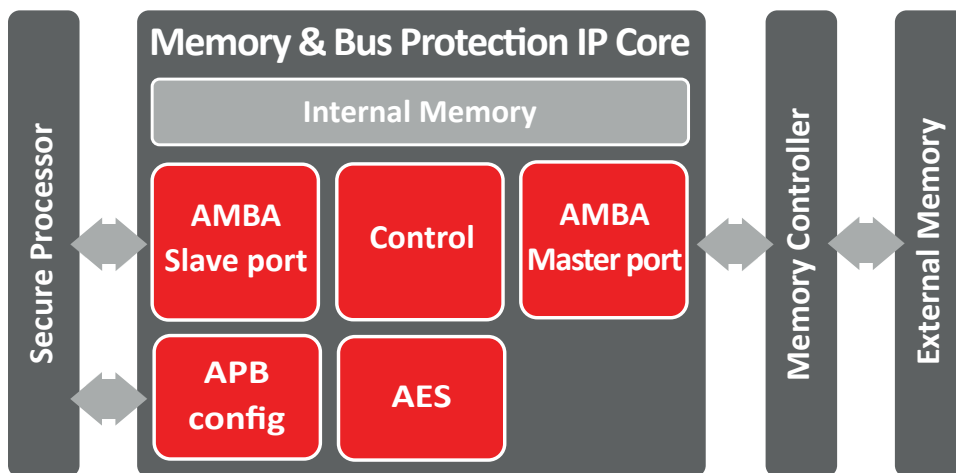


MEMORY & BUS PROTECTION IP CORE

The Memory & Bus Protection IP Core module enables on-the-fly encryption/decryption and authentication to the external memory.

It supports AHB/AXI slave/master interfaces, APB port for configuration purpose, and contains a cache. It is typically placed between the processor(s) and an external memory controller (DDRx). This IP Core improves tamper resistance by avoiding any modification, spoofing or analysis of external data.



Features

- ✓ Protect the external memory
- ✓ On-the-fly encryption/decryption and authentication
- ✓ Transparent for the processor
- ✓ Scalable data bus width (32, 64, 128 bits)
- ✓ AMBA Master/Slave interfaces
- ✓ Supports all key sizes (128/192/256 bits)
- ✓ Scalable internal Cache
- ✓ ASIC and FPGA

Applications

- ✓ Embedded security processor
- ✓ Secure payment

Implementation aspects

The processor can securely and transparently write/read data or code from external memory. It leverages the AES Core from Silex Insight. The unique architecture enables a high level of flexibility (cache size, performances) and allows it to be used by microcontroller and multi-core architectures. The features required by a specific application can be taken into account in order to select the most optimal configuration for any FPGA or ASIC technology.

Deliverables

- ✓ Netlist or RTL
- ✓ Scripts for synthesis & STA
- ✓ Self-checking RTL test-bench on referenced vectors
- ✓ Documentation

V1.1