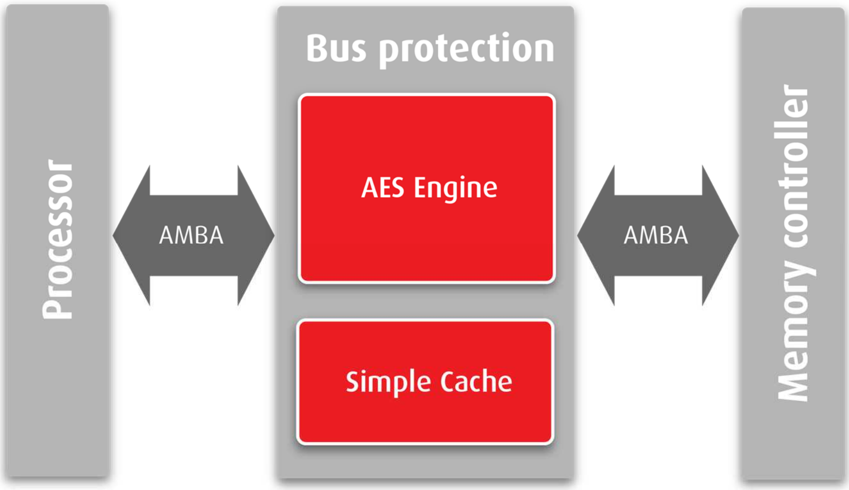
SILEX INSIGHT

Bus protection IP core

BA432b
Product sheet

The BA432b is an in-line bus protection module that implements data privacy and authentication. The bus protection module has an AHB/AXI slave port and an AHB/AXI master port, 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.



Implementation aspects

The bus protection is an in-line memory encryptor/decryptor. The processor can securely and transparently write/read data or code from external memory. The BA432b leverages the AES Core from Silex Inside. The unique architecture enables a high level of flexibility (Cache size, performances) and allows the bus protection moduke to be used by microcontroller and multi-core architectures. The IP Core can be provided with protection against SPA/DPA countermeasures. 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
- Documentation

Features

- On-the-fly encryption/decryption and authentication
- Transparent for the processor
- Scalable data bus width (32, 64, 128 bits)
- AHB/AXI Master/slave interfaces
- Supports all key sizes (128/192/256 bits)
- Easy to integrate
- Scalable internal Cache
- ASIC/FPGA SoC
- SPA/DPA countermeasures (optional)

Applications

- Embedded security processor
- Payment