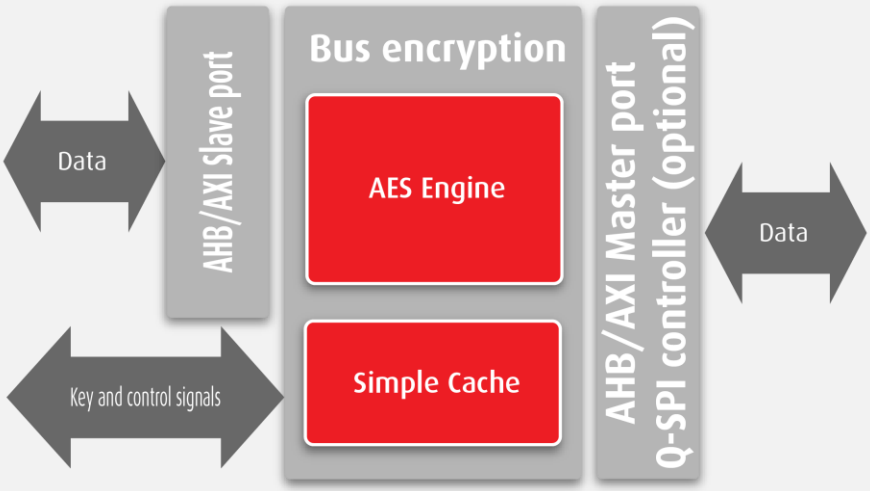
Bus encryption IP core

BA432a
Product sheet

The BA432a is an in-line decryption IP Core enabling on- the-fly execution of encrypted code from Flash. It has a simple AHB/AXI Slave port and AHB/AXI Master port. This solution includes a highly optimized implementation of the Advanced Encryption Standard (AES) algorithm. The key can be made invisible from the processor. The IP can be packaged optionally with a Q-SPI Controller. With the BA432a, our customers can take advantage of our expertise in ASIC and FPGA design, cryptography & security applications and the development & integration of re-usable cores & high-level IP solutions.



Features

- On-the-fly decryption
- In-place execution of encrypted code
- Decryption based on AES fully compliant with NIST FIPS 197
- Supports all key sizes (128/192/256 bits)
- Asynchronous core clock vs external clock
- AHB/AXI Master/slave interfaces
- Can be provided with Q-SPI Controller (optional)

Applications

- On-the-fly execution of encrypted code.

Implementation aspects

The unique architecture enables a high level of flexibility. The throughput and 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. The single RTL database for all configurations is a guarantee of liability and integration is made very easy due to standard interfaces (AHB/AXI).

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking RTL test-bench
- Documentation