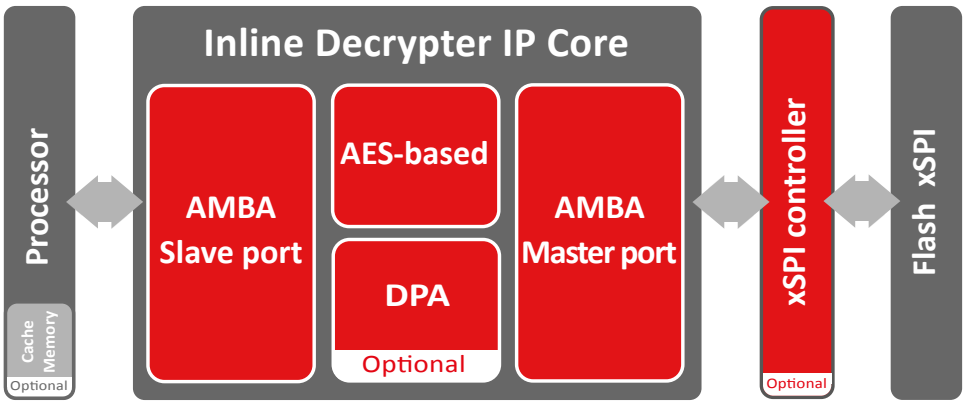
SILEX INSIGHT

Product sheet
BA432a

INLINE DECRYPTER IP CORE

The Inline Decrypter IP Core enables on-the-fly execution of encrypted code from Flash. It is often used to protect the source code from decompiling or reverse engineering.

This solution includes a highly optimized implementation of the Advanced Encryption Standard (AES) algorithm. The IP can be packaged optionally with a xSPI Controller. With the Inline Decrypter IP Core, 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. DPA countermeasures option available for applications requiring higher level of security with a very good protection against SPA (Simple Power Analysis) and DPA (Differential Power Analysis).



Features

- XIP (eXecution In Place) of encrypted code directly from Flash. (Optional xSPI controller)
- Decryption based on AES fully compliant with NIST FIPS 197
- AMBA Master/Slave interfaces
- Scalable solution (trade-off between performance vs. gate count)
- SPA/DPA countermeasures (optional)
- Supports all key sizes (128/192/256 bits)
- ASIC and FPGA

Applications

- Protects the source code from decompiling or reverse engineering (ideal for MCU's)

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 interface (AMBA AHB).

Deliverables

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

V1.2

Silex Insight
Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04
E-mail: contact@silexinsight.com
Web: www.silexinsight.com