SILEX INSIGHT

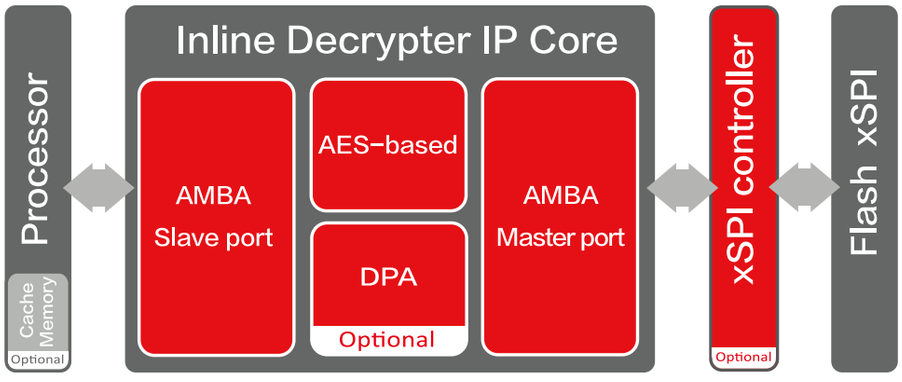
产品手册
BA432a

INLINE DECRYPTER IP Core

Inline Decrypter IP Core（内联解密IP核）支持从Flash实时执行加密代码，通常用于保护源代码免于反编译或逆向工程。

本解决方案包括了高级加密标准（AES）算法的高度优化的实现，可以选择将IP核与xSPI控制器打包在一起。借助内联解密IP核，用户可以获得我们在ASIC和FPGA设计、加密、安全应用以及可重复使用的内核和高端IP解决方案的开发、集成方面的专业知识。

DPA对策选项可用于要求更高安全级别的应用和市场，针对SPA（简单功率分析）和DPA（差分功率分析）具有非常好的保护作用。



特性

- 直接从Flash进行XIP加密代码（可选的xSPI控制器）
- 符合NIST FIPS 197的AES解密
- AMBA主/从接口
- 可扩展的解决方案（性能/门数的权衡）
- 可选的SPA/DPA对策
- 支持所有密钥大小（128/192/256位）
- ASIC和FPGA

应用

- 保护源代码免受反编译或逆向工程(非常适合MCU)

实施环节

独特的架构实现了高度的灵活性，可以选配特定应用所需的吞吐量和性能，以便为FPGA或ASIC选择最优配置，同时保障所有配置的单一RTL数据库的可靠性，基于标准接口(AMBA AHB)，易于集成。

产品交付

- Netlist 或 RTL
- Synthesis & STA 脚本
- RTL自检平台
- 文档

V1.2

Silex Insight
上海市闵行区虹许路528号
2号楼208室（201103）

Tel: +86 21 6221 0867
E-mail: contact-cn@silexinsight.com
Web: www.silexinsight.com.cn