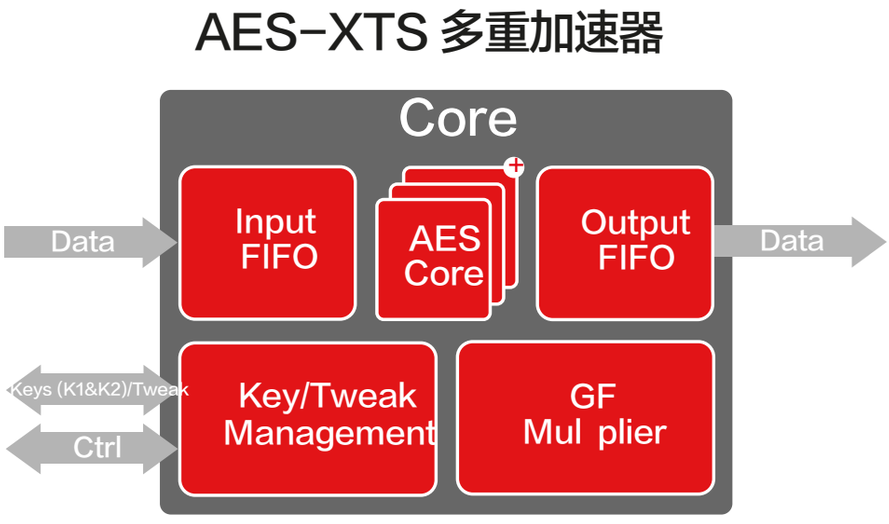
SILEX INSIGHT

产品手册
BA416

AES-XTS 多重加速器

AES-XTS多重加速器的加密引擎实现了AES算法的通用性和可扩展性，从而使该解决方案适用于各种低成本和高端应用程序(包括密钥、调整、输入和输出寄存器以及Galois领域)。

该加密引擎针对需要高吞吐量的高性能应用程序，凭借其可扩展性，可以根据客户需求对其进行定制，在性能、区域和技术之间达到最佳平衡。



特性

- ASIC 和 FPGA
- 高吞吐量:
  - ASIC: 2Tbps
  - FPGA: 100 Gbps
- 具有可扩展性的解决方案
- 支持 128-bit 和 256-bit密钥
- 符合 NIST SP800-38E
- 可以随 AXI DMA 和软件一起提供
- 可提供出色的 SPA 和 DPA防护
- 密码窃取（可选）
- 低功耗功能
- 可直接集成到简单的FIFO

应用

- 加密的磁盘/数据存储
- SATA III

实施环节

AES-XTS多重加速器的加密引擎可轻松植入ASIC和FPGA，并支持各种技术上的广泛应用，独特的架构实现了高度的灵活性。可以根据特定应用程序所需的吞吐量和功能，来选择最优的配置方案。

有关其他AES多重加速器的解决方案，请参见专用产品表：AES Multi-Purpose（BA411e）和AES-GCM多重加速器（BA415）。

产品交付

- Netlist 或RTL
- Synthesis 和 STA脚本
- 可对参考向量的RTL自检测试平台
- 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