SILEX INSIGHT

产品手册
BA450 | BA456 | BA457

NEW! Compact Standard Premium 3 VARIANTS

FIPS VALIDATED 140-2

加密协处理器

加密协处理器是一个硬件IP核心平台，可在FPGA或ASIC上的SoC环境中加速加密操作。

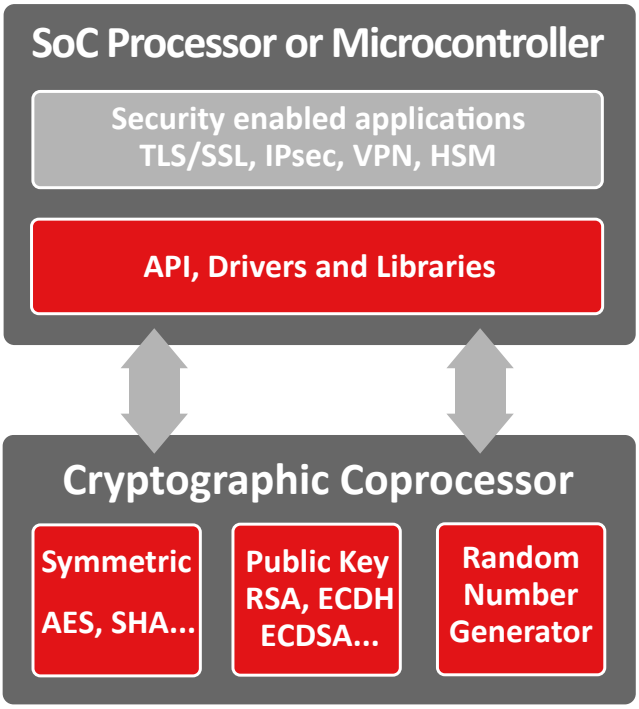
对称操作具有内置的分散/聚集DMA，可以快速卸载，协处理器适用于加速/卸载IPsec，VPN，TLS / SSL，磁盘加密或任何需要加密算法的自定义应用程序。

通用说明

协处理器平台集成了以下可选择的加密IP内核（包括我们的TRNG解决方案），附加接口、DMA和软件层，我们提供完整的解决方案。

可以选择以下加密引擎进行集成：

- 公钥密码术（RSA，ECC，ECDSA，ECDH，SM2，SM9）
- 随机数生成器（符合NIST-800-90A / B / C）
- AES（CTR，CCM，CMAC，GCM / GMAC，XTS，ECB，CBC）
- 哈希：SHA-1 / SHA-2 / SM3 / HMAC，SHA-3
- Chacha20-poly1305
- SM4
- ARIA
- 3GPP安全性（ZUC，KASMI，SNOW_3G）
- DES和3-DES



特性

- 可扩展的架构和加密引擎，可实现最佳性能/资源使用
- 可配置以实现完美的应用程序适配
- 100% CPU 卸载，低延迟和高吞吐量
- AES、PK 和 SM4 的可选 DPA 对策
- 可以使用 CPU 中隐藏的密钥（来自 PUF 或其他）
- 支持完整的软件/驱动程序
  - mbedTLS 集成
  - OpenSSL 支持
  - Linux 驱动程序（API 加密集成）
- 易于集成
  - AHB/AXI 接口
- FIPS 140-2 验证：CAVP #C742
- 低功耗

应用

- 安全通信（Tls/Ipsec/Ble/Zigbee/其他...）
- 安全启动支持
- 安全存储
- 密钥生成

软件接口

软件 API 和驱动程序与Linux操作系统的 mbedTLS和加密API进行接口，与协处理器一起提供，以便轻松得与客户的应用程序集成， 使用mbedTL、OpenSSL 或通过加密和AF_ALG与内核连接的应用程序可以直接调用硬件加速。

产品交付

- Netlist 或 RTL
- SW驱动程序（Linux）和OpenSSL
- 实现脚本
- 基于 FIPS 的 elf-check 测试平台 vectors
- 文档

市场


无线通信


联网


网联汽车


通用 MCU/MPU


数据中心 /云端

加密协处理器

从主处理器卸载繁重的任务，从而提高系统性能。

	紧凑版 专为具有严格功率要求和面积限制的设备而设计	标准版 集成所需的加密IP内核、通用接口、DMA和软件层	高级版 在标准功能的基础上构建，以支持隔离域的硬件密钥生成
可配置以实现完美的应用程序	✓	✓	✓
100%CPU卸载，低延迟和高吞吐量	✓	✓	✓
支持所有的软件/驱动程序	✓	✓	✓
通过FIPS 140–2验证：CAVP # C742	✓	✓	✓
安全通信（TLS，IPsec，BLE，Zigbee...）	✓	✓	✓
支持安全启动	✓	✓	✓
支持安全存储	✓	✓	✓
AES，PK和SM4的可选DPA对策 可以使用对CPU隐藏的密钥（来自PUF或其他密钥）	✓	✓	✓
功率/面积	极低	低	中
界面	AHB	AHB/AXI	AHB/AXI
灵活的公钥引擎配置	—	✓	✓
隐藏的非对称密钥（证明）	—	—	✓
硬件密钥生成（隐藏在CPU中）	—	—	✓
防止故障注入	—	—	✓
所有变体都提供完整的安全性功能，并且都可以包含相同的加密引擎。	产品编号 BA457	产品编号 BA450	产品编号 BA456

SILEX INSIGHT

产品手册
加密协处理器
V2.0

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