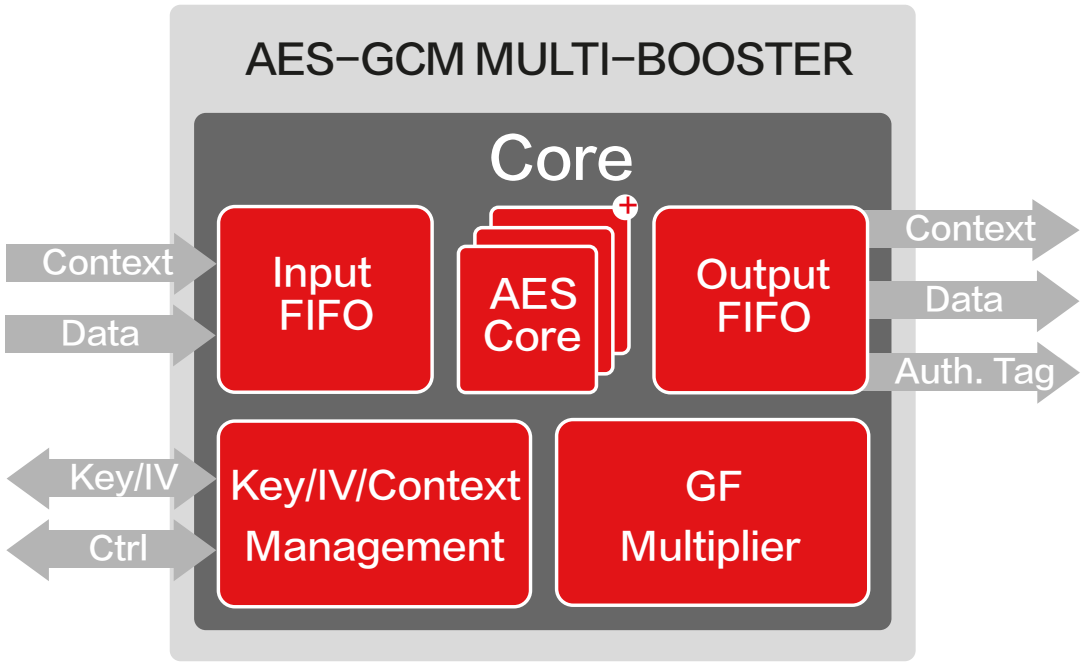
AES-GCM 多重加速器

AES-GCM 多重加速器的加密引擎实现了符合NIST SP 800-38D标准的AES-GCM算法的通用性和可扩展性，独特的产品架构可在保持最佳资源使用率的同时实现高吞吐量。

AES-GCM（Galois计数器模式）是一种经过身份验证的加密算法，它结合了用于加密的AES计数器模式和用于身份验证的Galois字段乘法器。同时实现加密和身份验证并可实现高吞吐量。像协议接口这样的数据只能对MACsec进行身份验证。

AES-GCM是NIST推荐的唯一可实现高吞吐量的身份验证加密算法。 GCM密码模式适用于保护高速通信通道，并在多个标准中被引用（例如MACsec（IEEE 802.1A），光纤通道安全协议（FC-SP），IPsec）。



特性

- ASIC 和 FPGA
- 高吞吐量:
  - ASIC: 2Tbps
  - FPGA: 100 Gbps
- 小包保证性能
- 支持128-bit / 256-bit
- 符合SP800-38D
- 可扩展的解决方案
- 可以随AXI DMA和软件一起提供
- 上下文切换和管理
- 低延迟
- 面积与性能之间的最佳平衡

直接集成到简单的FIFO

应用

- MACsec/IPsec/TLS
- 光学运输
- 宽带上网
- 支持WPA3

实施环节

独特的架构实现了高度的灵活性，可根据实际所需的吞吐量和功能要求来选择最佳配置，本产品易于植入ASIC和FPGA技术中，并可解决涉及安全性的网络应用。

AES-GCM 多重加速器的加密引擎包括密钥管理和上下文切换，经过优化的上下文切换可在单个内核中处理多个虚拟数据流，并为每个数据包选择独立密钥。 AES-GCM内核的高效流水线架构可处理小数据包，而不会影响性能。

产品交付

- Netlist 或 RTL
- Synthesis 和 STA脚本
- 可对参考向量的RTL自检平台
- 文档

有关其他AES解决方案，请参见专用产品表：AES多功能（BA411e）和AES-XTS多功能升压器（BA416）。

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