AES 分组密码算法

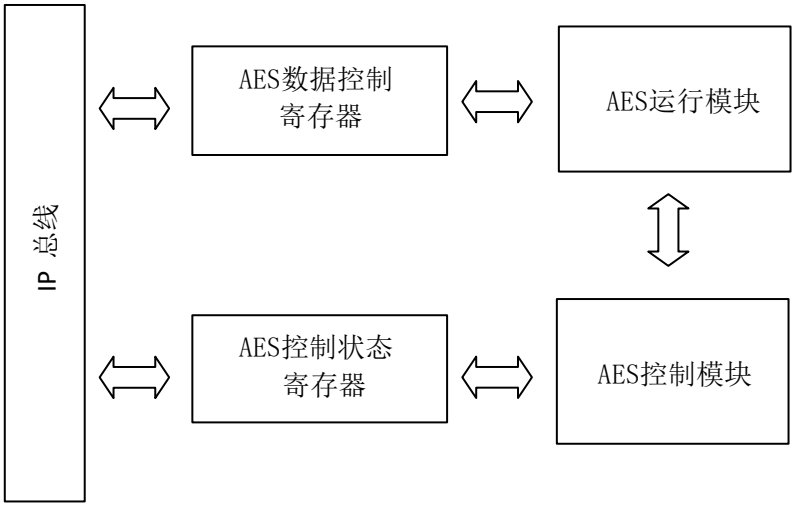
算法概述

AES(Advanced Encryption Standard) IP 是一个硬件实现的分组密码算法模块，实现了 AES 标准加密算法。AES 高级加密标准算法是 NIST(National Institute ofStandards and Technology)于 2001 年公布，用于信息安全领域的数据加解密。

算法特征

- 支持 AES 加密、解密算法
- 支持密钥分组长度为 128/192/256 比特
- 支持 ECB/CBC/OFB/CFB/CTR 工作模式
- 支持 AHB 接口
- 抗侧信道攻击设计：全掩码硬件设计
  - 抗时间攻击（TA 等）
  - 抗功耗攻击（SPA/DPA/CPA 等）
  - 抗电磁攻击（EMA/DEMA 等）
  - 抗故障攻击（FA/DFA 等）

算法架构图



AES 算法框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：35.3 MBytes/s for AES-128 @100MHZ
- 面积：8 万门