DES/3DES 分组密码算法

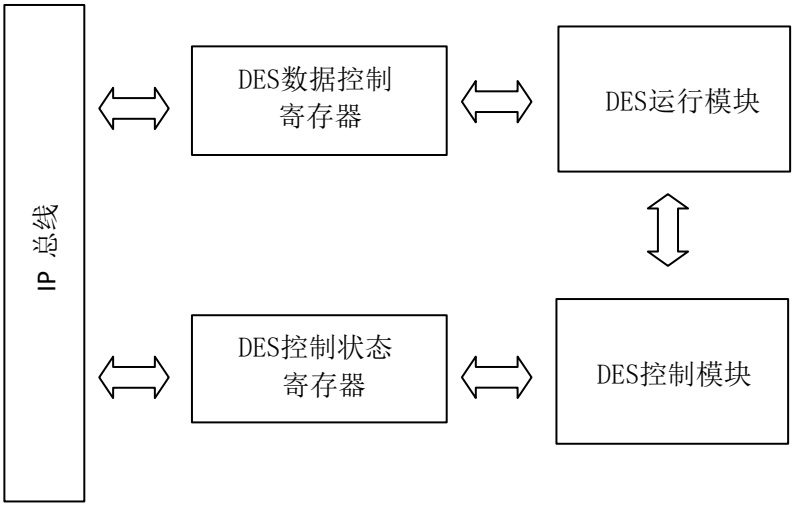
算法概述

DES(Data Encryption Standard)　IP 是一个硬件实现的分组密码算法模块，实现了 DES 标准加密算法。DES 数据加密标准算法是 1977 年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），并授权在非密级政府通信中使用。

算法特征

- 支持 DES/3DES 加密、解密算法
- 支持密钥分组长度为 64 比特的 DES
- 支持密钥分组长度为 128/192 比特的 3DES
- 支持 ECB/CBC/OFB/CFB 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



DES 算法框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：25.2 MBytes/s for DES，10.2 Mbytes/s for 3DES　@100MHZ
- 面积：2 万门