SM4 分组密码算法

算法概述

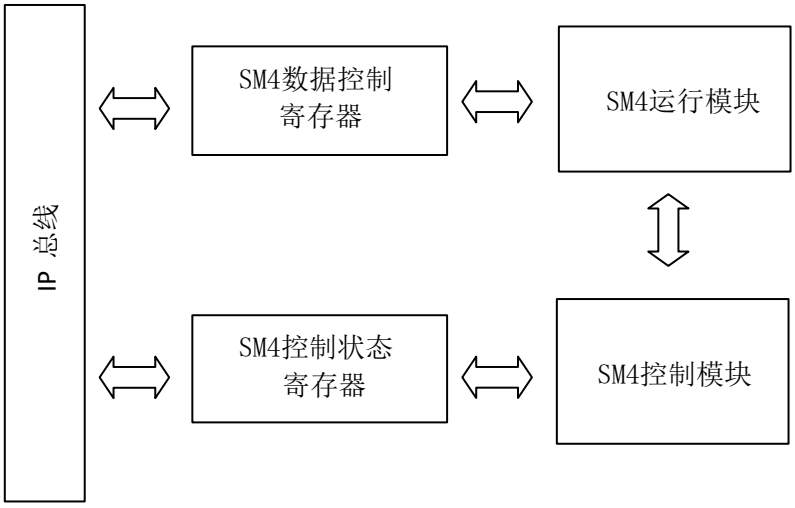
SM4(原名 SMS4) IP 是一个硬件实现的分组密码算法模块，实现了 SM4 标准加密算法。

SM4 分组加密算法是中国政府采用的一种分组密码标准，同时也是中国无线局域网标准的分组数据算法，由中国国家密码管理局于 2012 年 3 月 21 日发布。

算法特征

- 支持 SM4 加密、解密算法
- 支持密钥分组长度为 128 比特
- 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



SM4 算法框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：22.1 MBytes/s　@100MHZ
- 面积：3.9 万门