SM7 分组密码算法

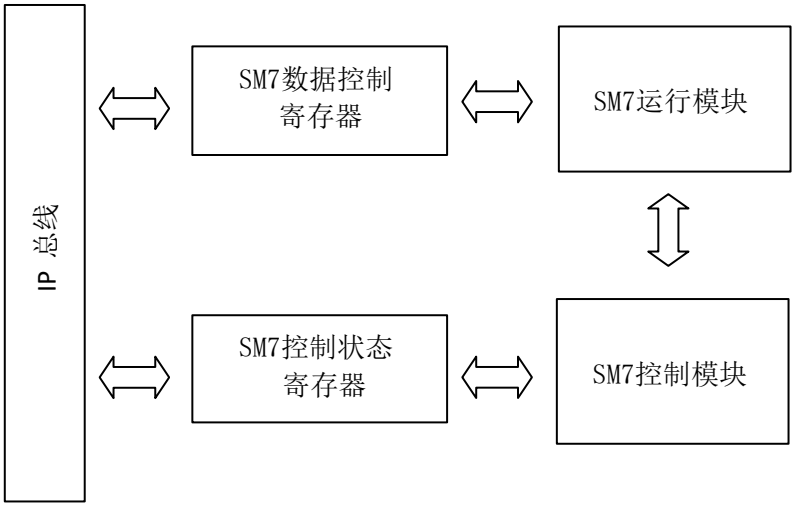
算法概述

SM7 IP 是一个硬件实现的分组密码算法模块，实现了 SM7 标准加密算法。SM7 算法是由中国国家密码管理局编制的一种商用密码分组标准对称算法。该算法不公开，仅以 IP 核的形式存在于芯片中。SM7 算法适用于非接触式 IC 卡，应用包括身份识别类应用(门禁卡、工作证、参赛证)，票务类应用(大型赛事门票、展会门票)，支付与通卡类应用（积分消费卡、校园一卡通、企业一卡通等）。

算法特征

- 支持 SM7 加密、解密算法
- 支持密钥分组长度为 128 比特
- 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



SM7 算法框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：50 MBytes/s @100MHZ
- 面积：0.5 万门