SM1 分组密码算法

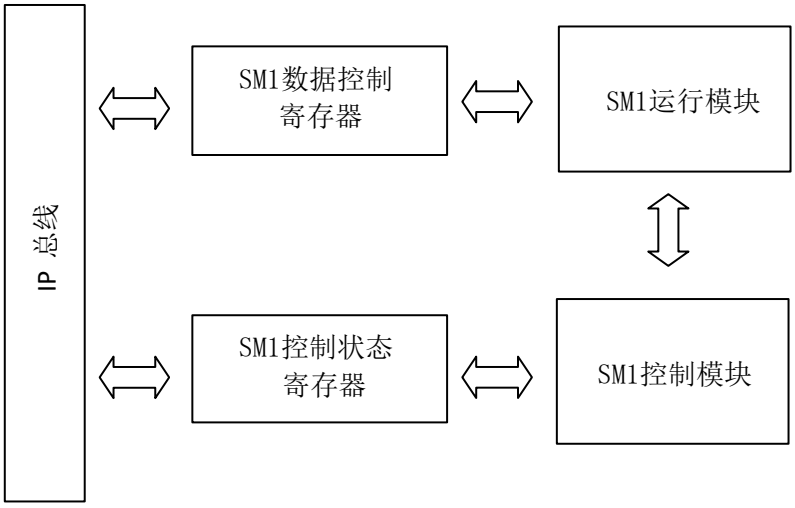
算法概述

SM1 IP 是一个硬件实现的分组密码算法模块，实现了 SM1 标准加密算法。SM1 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。采用该算法的芯片可应用于智能 IC 卡、智能密码钥匙、加密卡、加密机等安全产品，同时广泛应用于电子政务、电子商务及国民经济的各个应用领域（包括国家政务通、警务通等重要领域）。

算法特征

- 支持 SM1 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



SM1 算法框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：36.1 MBytes/s　@100MHZ
- 面积：11.2 万门