ZUC 流密码算法

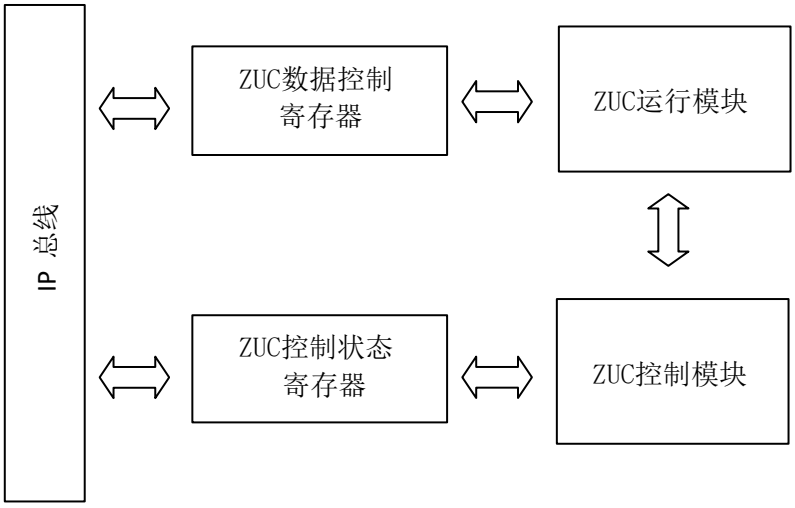
算法概述

ZUC (祖冲之序列密码算法)IP 是一个硬件实现的流密码算法模块，实现了 ZUC 标准加密算法。ZUC 算法是中国自主研究的流密码算法，是运用于移动通信 4G 网络中的国际标准密码算法，该算法包括祖冲之算法(ZUC)、加密算法(128-EEA3)和完整性算法(128-EIA3)三个部分。

算法特征

- 支持 ZUC 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



ZUC 算法框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：120 MBytes/s　@100MHZ
- 面积：4 万门