RSA 公钥密码算法

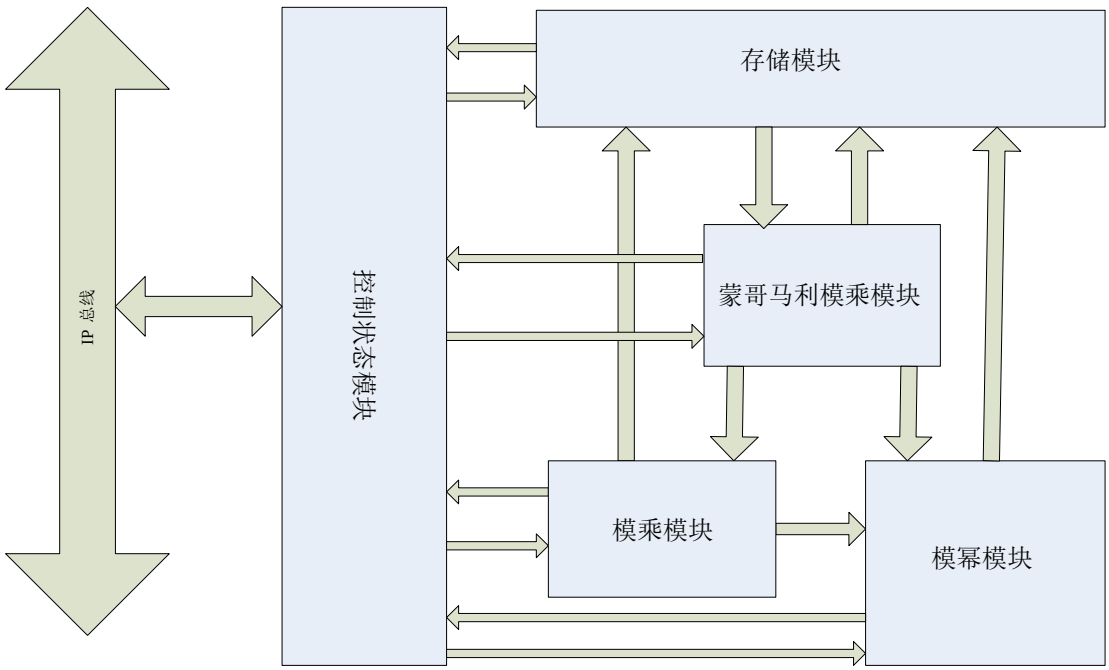
算法概述

RSA IP 是通过软件和硬件结合方式实现的的一个非对称加密算法，主要实现了 RSA 的密钥生成算法，加解密算法以及签名验签算法，密钥协商算法等。其中硬件部分主要实现了大数的模乘，模幂，蒙哥马利模乘，椭圆曲线的点乘和点加等运算。RSA 加密算法是由 MIT 三位密码学学家于 1977 年一起提出的，目前该算法广泛应用于各行各业中的数据加密领域。

算法特征

- 支持最高位宽为 2048 比特的公钥密码算法 RSA 的密钥生成算法，加密解密算法，签名验证算法，密钥协商算法
- 支持最高位宽为 2048 比特的大数模乘，模幂，蒙哥马利模乘等运算；
- 支持 RSA-CRT 和 RSA 非 CRT 模式
- 支持 AHB 接口
- 抗侧信道攻击设计
  - 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



RSA 算法硬件框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：1）密钥对生成：1.7 次/s for RSA-1024,　0.3 次/s for RSA-2048

  2）加密算法：84 次/s for RSA-1024,　9.6 次/s for RSA-2048

  3）解密算法：168 次/s for RSA-1024,　31.2 次/s for RSA-2048

  4）签名算法：168 次/s for RSA-1024,　31.2 次/s for RSA-2048

  5）验证算法：84 次/s for RSA-1024,　9.6 次/s for RSA-2048

  注：测试频率为 100MHZ
- 面积：20.4 万门