SM2 公钥密码算法

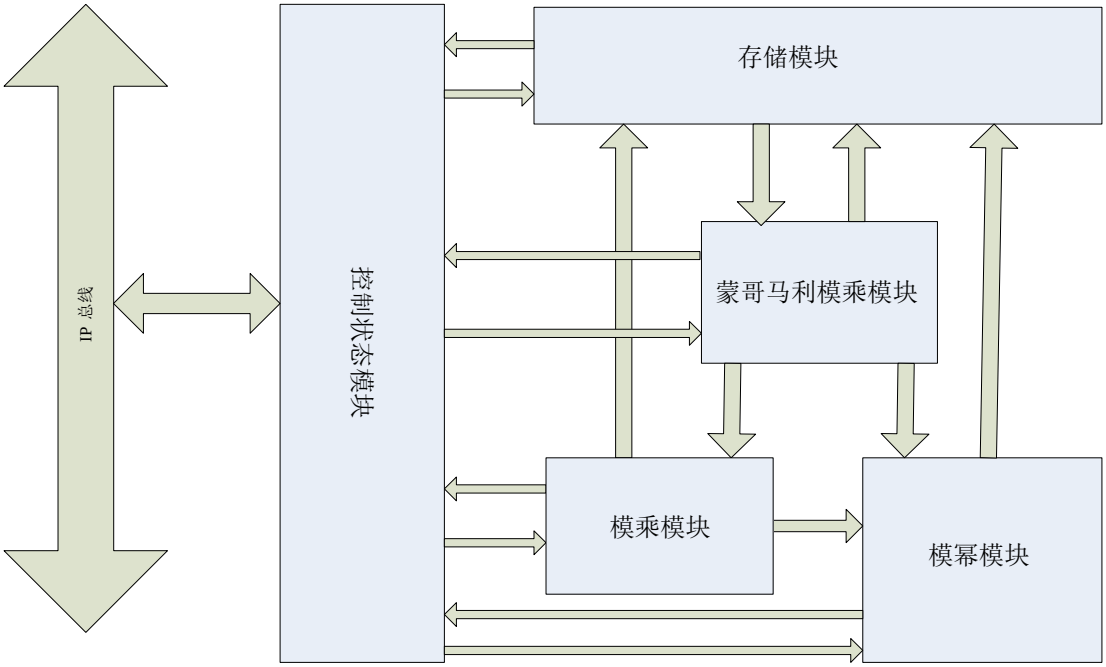
算法概述

SM2 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 SM2 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。SM2 算法是由中国政府采用的一种非对称密码算法标准，由中国国家密码管理局于 2010 年 12 月 17 日发布。

算法特征

- 支持公钥密码算法 SM2 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 512 比特素域下的椭圆曲线的点加和倍点运算；
- 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



SM2 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：240 次/s

  2）加密算法：108 次/s

  3）解密算法：216 次/s

  4）签名算法：216 次/s

  5）验证算法：108 次/s

  注：测试频率为 100MHZ
- 面积：20.4 万门