SM9 公钥密码算法

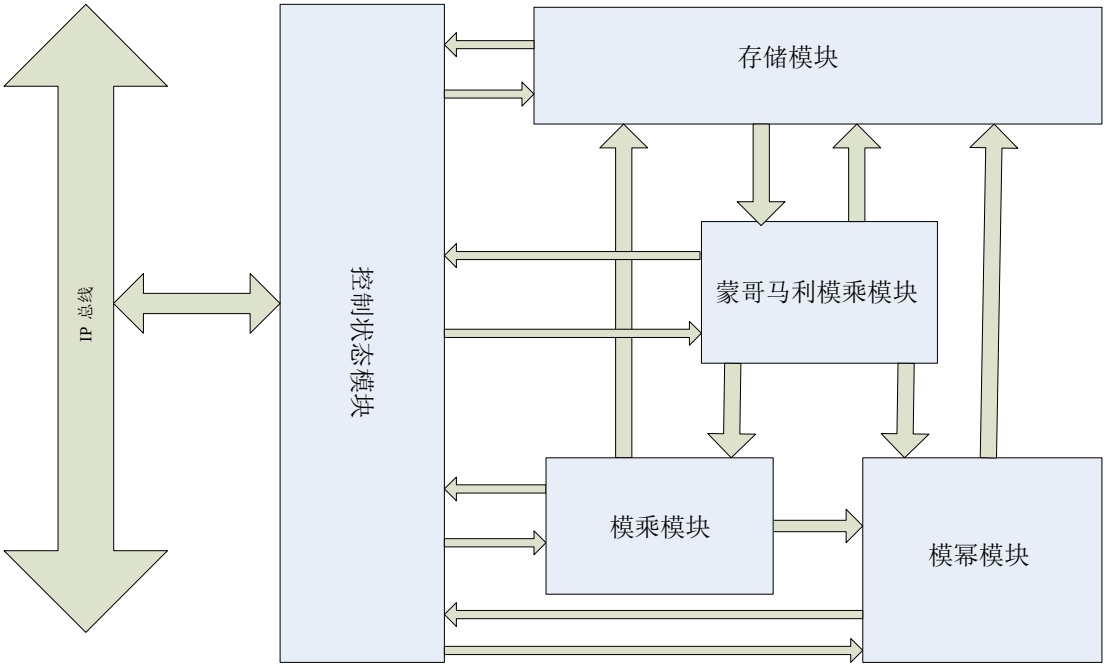
算法概述

SM9 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 SM9 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。SM9 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 2016 年 3 月 28 日发布。SM9 算法适用于互联网应用的各种新兴应用的安全保障。如基于云技术的密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等等。这些安全应用可采用手机号码或邮件地址作为公钥，实现数据加密、身份认证、通话加密、通道加密等安全应用，并具有使用方便，易于部署的特点

算法特征

- 支持公钥密码算法 SM9 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



SM9 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：1.42 s/次
  2）加密算法：724 ms/次
  3）解密算法：1.06 s/次
  4）签名算法：705 ms/次
  5）验证算法：2.12 s/次
  6）双线性对：1.06 s/次
  注：测试频率为 100MHZ
- 面积：20.4 万门