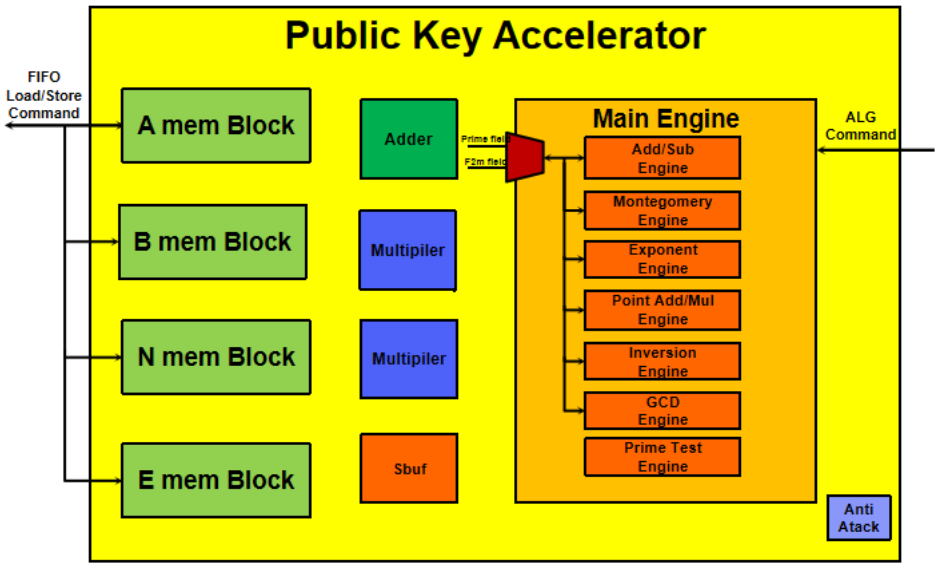
公钥算法加速引擎

概述

Pkha（Public Key Hardware Accelerator）模块用于在公钥算法中计算各种大数运算的模块，包括基本的一些模运算，如模加，模乘，模幂等，也能进行椭圆曲线的点加，点乘点倍的操作，上述操作都能在素域和二元域上进行操作。模幂和点成操、作带有运算时间等长的功能，可以防止进行时间攻击和旁路攻击。pkha 还带有一个拉宾米勒素数检测的运算算子，用来检测大素数。



框架图

算法特征

- 高效支持所有主流公钥算法（RSA/ECC/SM2/SM9)
- 支持最高 4096 位模运算
- 支持椭圆曲线 1024 位运算（素域/二元域）
- 支持 Miller-Rabin 素数测试算法
- 支持加解密/签名验证/秘密推导
- 支持秘钥生成（DSA/ECDSA/DH/ECDH 等）
- 防侧信道攻击

公钥算法性能指标							
配置选择	PKHA 综合面积 (SMIC40LL)	功耗 （预估）	RSA-2048位 签名 （无CRT） (次/秒)	SM2-256位 签名 (次/秒)	SM2-256位 验签 (次/秒)	SM9-256位 签名 (次/秒)	SM9-256位 验签 (次/秒)
单核PKHA 128乘法器	0.8mm2	140mw	480 @400MHz	3182 @400MHz	1814 @400MHz	230 @400MHz	107 @400MHz
4核PKHA 128位乘法器	3.2mm2	560mw	1920 @400MHz	12728 @400MHz	7256 @400MHz	920 @400MHz	428 @400MHz