HMAC 杂凑密码算法

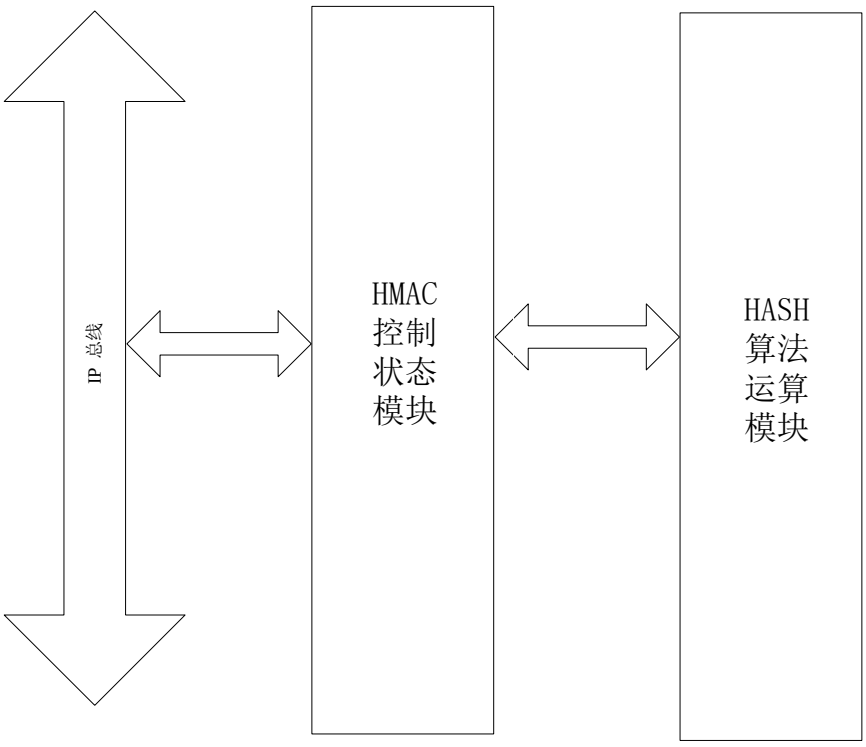
算法概述

HMAC IP 是一个全硬件实现的杂凑密码模块，实现了 HMAC-MD5/ HMAC-SHA0/ HMAC-SHA1/ HMAC-SHA224/ HMAC-SHA256/ HMAC-SHA384/ HMAC-SHA512/ HMAC-SM3 等标准的杂凑密码算法。HMAC 是密钥相关的哈希运算消息认证码（Hash-based Message Authentication Code）。HMAC 于 1997 年作为 RFC2104 被公布，并在 IPSec 和其他网络协议（如 SSL）中得以广泛应用，现在已经成为 Internet 安全标准。

算法特征

- 支持 HMAC-SM3 杂凑密码算法
- 支持 HMAC-MD5/ HMAC-SHA0/ HMAC-SHA1 杂凑密码算法
- 支持 HMAC-SHA224/ HMAC-SHA256/ HMAC-SHA384/ HMAC-SHA512 杂凑密码算法
- 支持 HMAC-SM3/ HMAC-MD5/ HMAC-SHA0/ HMAC-SHA1/ HMAC-SHA224/ HMAC-SHA256/ HMAC-SHA384/ HMAC-SHA512 杂凑密码算法的 HMAC 分段运算
- 支持 AHB 接口

算法架构图



HMAC 算法硬件框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：1）HMAC-SHA0/ HMAC-SHA1：43.2 MBytes/s

  2）HMAC-SHA224/ HMAC-SHA256：54.5 MBytes/s

  3）HMAC-SHA384/ HMAC-SHA512: 60.1 MBytes/s

  4）HMAC-MD5：52.6 MBytes/s

  5）HMAC-SM3 ：49.6 MBytes/s

  注：测试频率为 100MHZ
- 面积：14.8 万门