HASH 杂凑算法

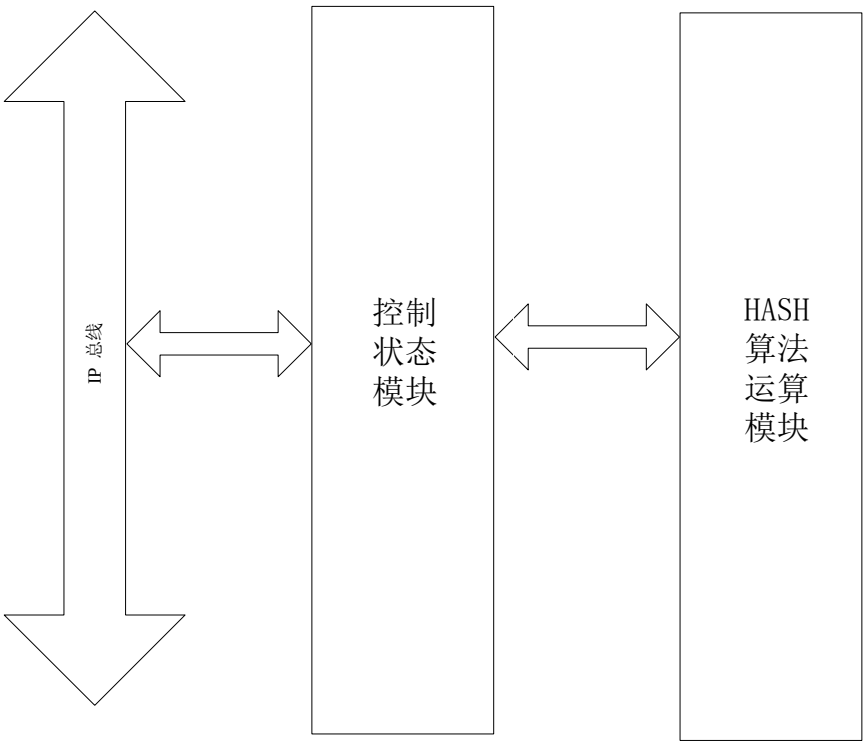
算法概述

HASH IP 是一个全硬件实现的杂凑密码模块，实现了MD5/SHA0/SHA1/SHA224/SHA256/SHA384/SHA256/SM3 等标准的杂凑密码算法。MD5 信息摘要算法（MD5 Message-Digest Algorithm）于 1992 年公开，用以取代 MD4 算法，可以产生出一个 128 位的散列值，用于确保信息传输完整一致。SHA (Security Hash Algorithm) 是美国的 NIST 和 NSA 设计的一种标准的 Hash 算法，SHA 用于数字签名的标准算法的 DSS 中，也是安全性很高的一种 Hash 算法。SHA0/SHA1 是第一代 SHA 算法标准，SHA224/SHA256/SHA384/SHA512 是第二代 SHA 算法标准，统称为 SHA-2。SM3 算法是由中华人民共和国政府采用的一种杂凑密码算法标准，由中国国家密码管理局于 2010 年 12 月 17 日发布。在商用密码体系中，SM3 主要用于数字签名及验证、消息认证码生成及验证、随机数生成等。

算法特征

- 支持 SM3 杂凑算法
- 支持 MD5/SHA0/SHA1 杂凑算法
- 支持 SHA224/SHA256/SHA384/SHA512 杂凑算法
- 支持 SM3/MD5/SHA0/SHA1/SHA224/SHA256/SHA384/SHA512 杂凑算法的分段运算
- 支持 AHB 接口

算法架构图



HASH 算法硬件框架图

算法性能

- 工艺：TSMC 40nm ULP EFLASH
- 频率：100MHZ
- 性能：1）SHA0/SHA1：48.1 MBytes/s

  2）SHA224/SHA256：60.1 MBytes/s

  3）SHA384/SHA512: 67.2 MBytes/s

  4）MD5：58.5 MBytes/s

  5）SM3 ：55.2 MBytes/s

  注：测试频率为 100MHZ
- 面积：7.2 万门