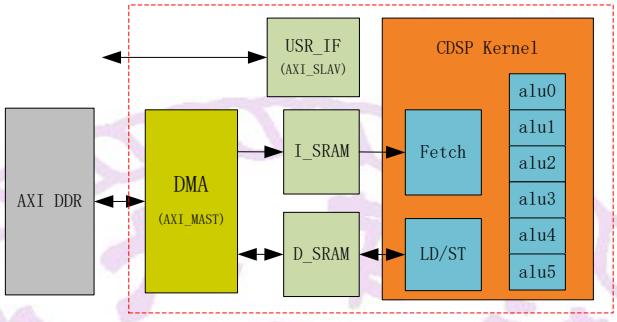
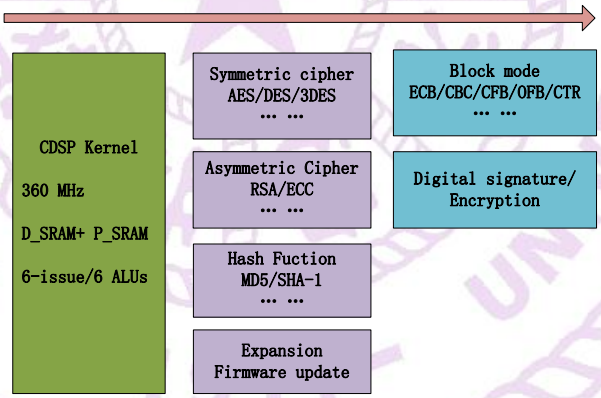
- **密码处理器简介**

清华大学密码处理器 IP 主要面向信息安全应用。该密码处理器 IP 实现了目前国际上主流的密码算法，主要包括对称密码算法 (AES/ DES/ 3DES)，非对称密码算法 (RSA/ ECC)和哈希算法 (SHA1/MD5) 。该密码处理器最大特点是支持多种密码算法的同时还能够保持高性能。同时由于密码处理器是基于清华大学先进的 DSP 技术设计，可以通过软件方式不断扩展密码处理器支持的密码算法。



密码处理器架构图

- **特点**
  - 基于哈弗结构的 DSP 处理器，拥有独立的指令和数据存储单元；
  - 在片数据和指令存储器，分别存储数据和指令；
  - 总共十一级流水线，四级执行级流水线；
  - 6 发射 VLIW DSP，6 个数据处理单元；
  - 超强的计算性能和良好的编程能力；
  - 嵌入式的具有 AXI 结构的 DMA；



  - AES/DES/3DES 加密解密吞吐率均超过 300 Mbps；
  - ECB/CBC/CFB/OFB/CTR 模式与 FIPS-197 兼容；
  - SHA1/MD5 吞吐率超过 560Mbps；
  - RSA 支持 512 位，1024 位和 2048 位秘钥，每秒超过 40 次；
  - 通过升级固件，就可以实现新的更多密码算法。
- 功能描述

清华大学密码处理器是一个面向信息安全的 IP。由于基于高性能 DSP 技术设计而成，使得该密码处理器不但性能高，同时具备灵活性。密码处理器通过通用总线从外部存储器获取明文进行加密，然后把密文保存到外部存储器。算法和模式都可以由用户自由选择。密码处理器还支持用哈希函数对原始数据进行压缩，提取特征数据。RSA 算法同样在密码处理器上得到了实现。RSA 的主要工作时完成对特征数据进行数字签名。

由于 RSA 是公钥密码算法，可以用于非对称加密场合。支持的 RSA 算法支持多种秘钥长度。采用中国剩余定理优化的 RSA 算法可以满足绝大多数场合应用要求。

用户可以通过选择不同的固件来实现各种不同的数据安全处理要求。使用极为方便。

- **技术参数和性能**
  - DSP 技术参数

    360 MHz 使用 TSMC 65 nm 工艺, 297 K 等效逻辑门（包括数据和指令存储器）。
  - 对称密码算法性能(Mbps)

Algorithm	DES	3DES	AES128 *	AES192	AES256	IDEA
ECB	1124	632	732	633	557	668
CBC	536	307	443	384	339	325
CFB**	536	307	443	384	339	325
OFB	536	307	443	384	339	325
CTR	NA	NA	705	612	541	NA

Notes: * AES128/AES192/AES256 stand for the AES key length, 128-bit/192-bit/256-bit.

**OFB/CFB, using the block length of 128 bits, other block length is also available.

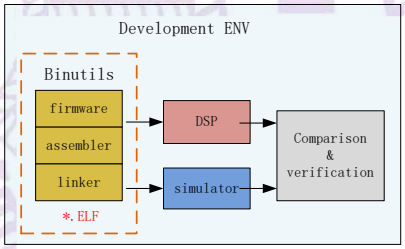
  - 哈希函数和非对称密码算法性能(Mbps)

Algorithm	SHA1	MD5	RSA1024	1024CRT*	RSA2048	2048CRT
Available	✓	✓	✓	✓	✓	✓
Performance	583	567	65 Tps**	251 Tps	14 Tps	46 Tps

Notes: *CRT, RSA using Chinese Remainder Theorem.

**Tps, times per second.

- **软件开发工具**
  - 指令级软件模拟器，可以仿真和调试密码处理器.
  - 基于 GNU 的二进制工具集 Binutils。支持汇编级的程序开发。



- **流片结果**

密码处理器 IP 在中星微 VC0718 芯片中得到量产。该芯片是面向国家《安全防范监控数字视音频编解码技术标准》(简称 SVAC，Surveillance Video and Audio Coding)的第一款 SoC 芯片。