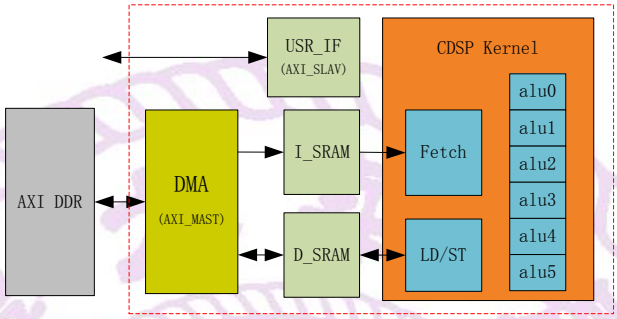
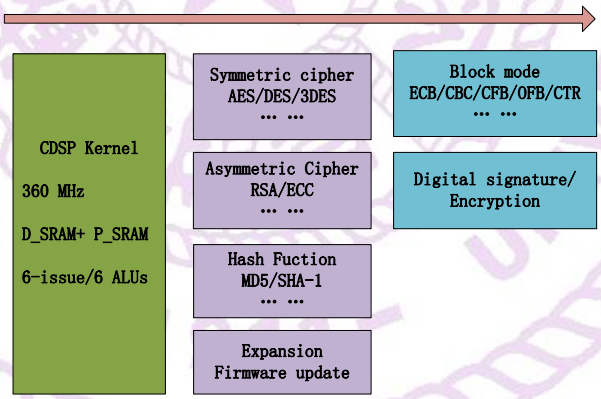
- **Overview of Crypto DSP**

The THU Crypto DSP is an IP core majored in information security, which can implement symmetric encryption (AES/ DES/ 3DES), asymmetric encryption (RSA/ ECC) and hash function (SHA1/MD5) in only one module. It supply an excellent solution that high performance and colorful algorithms can be achieved simultaneously. Due to the programmable ability, the core can be easily expanded to support more cryptographic algorithm, not limited to the ones mentioned above.



Crypto DSP Architecture

- **Feature**
  - DSP based on Harvard Architecture, separated P-RAM and D-RAM.
  - On chip P-SRAM and D-SRAM, separately used to buffer firmware and source data.
  - 9 level pipeline stages in total, 4 pipeline stages in execution units.
  - 6-issue VLIW DSP owns 6 ALUs in execution stage.
  - Powerful in calculation, and good in programmability.
  - Embedded DMA based on AXI protocol fetching source data and outputting the result.



  - AES/DES/3DES with throughput up to 300 Mbps, both encryption and decryption.
  - ECB/CBC/CFB/OFB/CTR block mode compatible to the FIPS-197.
  - SHA1/MD5 with throughput up to 560 Mbps.
  - RSA with key length from 512 bits to 2048 bits, up to 40 times per second.
  - More algorithms can be implemented by upgrading CDSP firmware.
- **Function Description**

THU Crypto DSP is a security IP supplying a high performance and flexible solution in the information security area. Block ciphers such as AES/DES/3DES are implemented, and the available block modes include ECB/CBC/CFB/OFB/CTR according to the FIPS-197, but not limited to these ones. The core can fetch the plain text in external memory and do the

encryption work using a supplied key, and write back the cipher text to external memory. The cipher algorithm and block mode used are depending on the costumer's needs.

Hash Functions such as MD5 or SHA1 can also be used to compress the original data, and extract a massage digest, both plain text and cipher text can be used in this function, depending on the configuration parameters. This massage digests are written to the external memory though the EDSP DMA too.

As the algorithm RSA is also implemented in CDSP, so after the message digest is abstracted, RSA can be used to finish the digital signature work, and the result can be sent to the external memory too. Another use of RSA is to do public key encryption work, which is very useful in asymmetric encryption. The available key length is 512 bits, 1024 bits, 2048 bits or longer and the CRT (Chinese Remainder Theorem) can be selected to accelerate the speed of RSA.

The user can choose to use only one algorithm or the combination of several algorithms in their product as their needs. The only modification is using a different version of firmware.

- **Technical Parameters & Performance**
  - DSP technical parameters

    360 MHz using TSMC 65 ns technology, 297 K gates.
  - Symmetric encryption performance(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

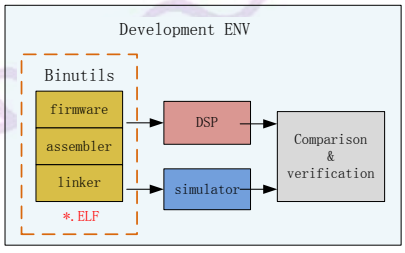
Notes: * AES128/AES192/AES256 stand for the AES key length, 128-bit/192-bit/256-bit.
**OFB/CFB, using the block length of 128 bits, other block length is also available.

  - HASH function and Asymmetric encryption performance(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.

- **Software Development Kits**
  - Instruction level simulator, used to simulator the behavior of CDSP.
  - Binutils including assembler, linker, function library, anti-assembler and so on.



- **About Tsinghua High Performance Digital Signal Processing laboratory**

  The Tsinghua High Performance Digital Signal Processor laboratory focuses on developing high level DSP and the relevant software kits. The research team can supply an excellent DSP architecture according to the customer's specific requirement. The solution has be successfully used in HD video encryption and audio codec.

For more information, please visit our website http://dsp.ime.tsinghua.edu.cn.