

Features

Configurable security engine adaptable to include:

- AES-CBC mode cipher supporting 128, 192 and 256-bit key sizes.
- DES-CBC mode cipher supporting 56 and 168-bit (3DES) key sizes.
- HMAC-MD5 and HMAC-SHA-1 mode hash.
- Configurable command and status FIFOs up to 256 entries deep
 - Supports interrupt coalescence to enhance overall system throughput
- AH & ESP mode processing.
- Transport mode processing.
- Tunnel mode processing.
- Extended Sequence Numbers.
- Scatter-gather DMA based packet memory architecture.

Applications

- IPsec
- VPN Appliances
- Edge Routers

The CLP-25 engine bridges the gap between raw cryptographic offload and complete IPsec offload. The IPsec Offload Engine combines hash and cryptographic engines, a special purpose DMA engine, and ESP/AH packet processing logic to offload most of the IPsec protocol from the host processor.

The SDMA block alleviates bandwidth on the system bus through dual targeting of the hash and encryption cores. The CLP-25 engine can be tailored to achieve throughput from 40 Mbps up to 700 Mbps. The design is silicon proven in multiple technology nodes.

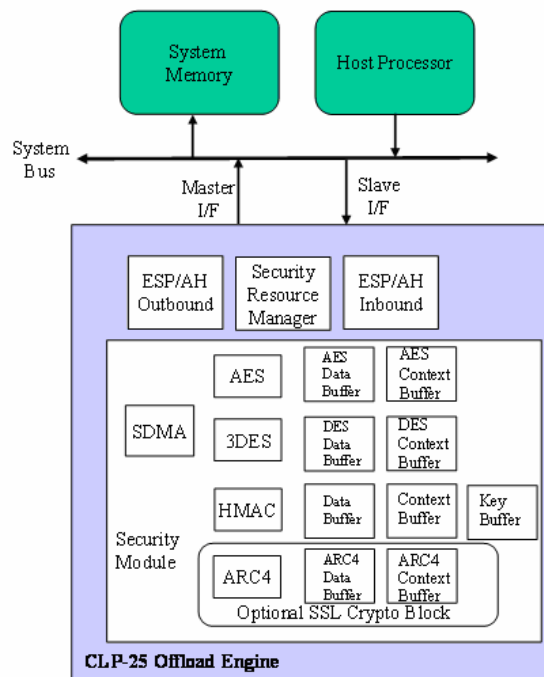
General Description

The IPsec Offload Engine is comprised of CLP hashing and crypto cores, the Security Resource Management block and inbound and outbound processing blocks. Each cipher block and the hash block have embedded memory associated with it to hold data and context values.

Depending on the system performance required, a subset of the cipher and hash modes are selected as well as the architecture desired for each cipher block implemented. These configurations are set through build-time parameters.

The figure below shows a high-level block diagram of the IPsec Offload Engine within a system.

In addition to ESP and AH mode processing, the host processor may also use the cryptographic engines and the SDMA block to perform raw cryptographic offload services. To do so, the host processor requests access to the crypto cores by writing to a register. The host either polls a register or waits for an interrupt signal before accessing crypto resources. Note that when the host is utilizing crypto resources, ESP/AH processing may slow down or stop completely. It is recommended that the host requests the minimum required accesses to crypto cores to complete a given task, and it releases the cores as soon as possible, while ESP/AH processing is in progress.



General Description cont'

Performance and Gate Count

The curves shown in graph indicate throughput for various configurations of the IPsec Offload Engine. The performance capabilities are specified with a core clock of 200 MHz which is achievable by the engine by using a high speed 0.13 micron process in combination with a high performance library and memories.

The graph illustrates that small packet performance is gated by the HMAC/SHA-1 logic and therefore the choice of cipher engine does not impact this corner of the performance curve. Given a realistic mix of traffic commonly found on networks however, the faster cipher options do provide substantial gain and may be considered for these real life traffic scenarios.

Interrupt Coalescence

The CLP-25 has recently been upgraded to implement configurable command and status FIFOs as found in the CLP-32 SPAcc. This offers software developers the ability to implement interrupt coalescence which is invaluable in small packet traffic situations. Developers can queue multiple commands in the command FIFO which will be sequentially processed by the CLP-25.

The status results for each command are pushed into the status FIFO and upon reaching a pre-determined level an interrupt is triggered. The processor can then complete the packet processing on multiple PDUs with a single context switch. The command and status FIFO depth can be configured from one to 256 entries.

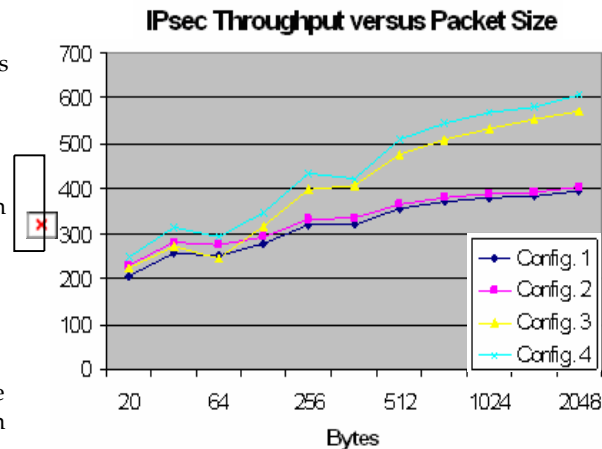
In addition, Elliptic offers a broad range of security cores including random number generators, hashing cores and public key acceleration supporting both RSA and Elliptic Curve operations that can be used for storage security and other applications such as virtual private networks, digital rights management and wireless security.

Other Products of the Family of VPN Engines

- CLP-25: Configurable IPsec (ESP/AH) Engine
- CLP-30: High Throughput Pipelined IPsec Core
- CLP-36: IPsec/SRTP (ESP/AH) Offload Engine
- CLP-46: Security Protocol Accelerator (SPAcc) Release 3.0

The configurations presented in the above graph are described in the table below:

Configuration	ASIC Gate Count	Cipher and Hashing Description
1	210 kGates	AES with 32 bit internal data path, 128-bit key and HMAC/SHA-1
2		Compact 3DES and HMAC/SHA-1
3	245 kGates	AES with 128 bit internal data path, 128 bit key and HMAC/SHA-1
4		High-performance 3DES and HMAC/SHA-1



Availability

- The CLP-25 is available in soft IP form HDL Source. The deliverables available are:

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script & constraints
- Sample simulation script
- Documentation