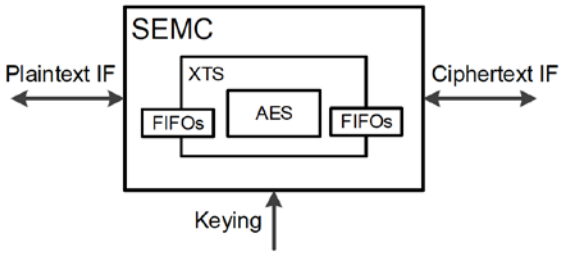
Secure External Memory Controller

The Secure External Memory Controller (SEMC) is a VHDL IP block designed to perform inline memory encryption using AES-XTS. The SEMC is highly-configurable and may be optimized for various size, throughput, and latency trade-offs. The core is device independent and is highly portable.



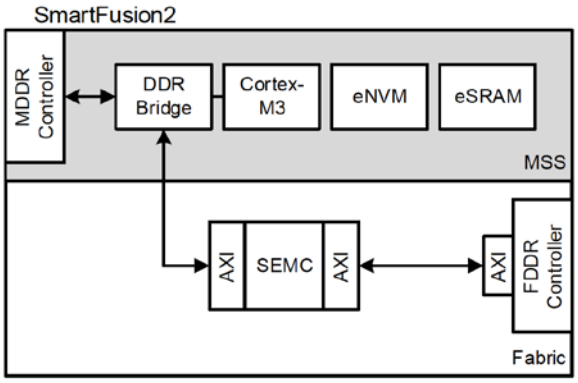
Features

- AES-XTS encryption with 128, 192, and 256 bit keys for data and tweak
  - Transparent encryption with configurable blocks-per-sector
- Modular design with internal, highly-configurable AES core
  - Internal AES supports many configurations (Area, Balanced, Throughput, Pipelined) ranging from minimal area to maximum throughput
  - When configured for pipelined AES operation the number of AES round units and pipeline registers is configurable
  - The core can support 400 MB/s of sustained throughput for high-throughput applications
- Generic keying interface providing support for both static and ephemeral keying schemes
- Single port RAM-style interface for bridging to internal bus logic
- Supports transaction queuing with multiple in-flight transactions

Application Example

Many modern FPGAs are now system on chip devices that contain an embedded processing hard-block. When data confidentiality is essential, it is necessary to protect the confidentiality of memory accesses performed by the processor. These accesses may be processor instruction fetches or general memory transactions.

Shown on the right is an example using the SEMC to protect processor memory accesses on a SmartFusion2. The ARM Cortex-M3 processor is configured to access external memory through the dedicated fabric DDR controller. The SEMC may then be integrated into this memory path with appropriate AXI bridges. When configured in this fashion, all external memory accesses through the SEMC are transparently encrypted and decrypted.



This is one example of using the SEMC to protect processor external memory accesses. More generally, the core may be used to protect any memory access bridged through the SEMC for both low latency and high-throughput applications.

Secure External Memory Controller

Representative Performance Metrics

Shown below are representative post-synthesis performance metrics for the SEMC collected from Synopsys Synplify Pro. The core is highly configurable and many of the possible area/performance trade-offs are not shown in the table. Please contact Microsemi if you have specific performance needs.

Family	Configuration					Luts	FFs	RAM	Frequency
	Key Width	Data Width	Address Width	Mode	Round Units				
Microsemi SmartFusion®2	128	32	32	T	N/A	8600	4800	28	100 MHz
	256	128	32	P	2	20000	15000	37	76 MHz
Xilinx Virtex 7	128	128	32	T	N/A	4000	5400	28	300 MHz
	256	128	32	P	15	31000	29000	24	325 MHz
Altera Cyclone V	128	32	32	T	N/A	4100	5300	16	180 MHz
	256	128	32	P	2	12700	14800	42	180 MHz

Microsemi

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,400 employees globally. Learn more at www.microsemi.com.