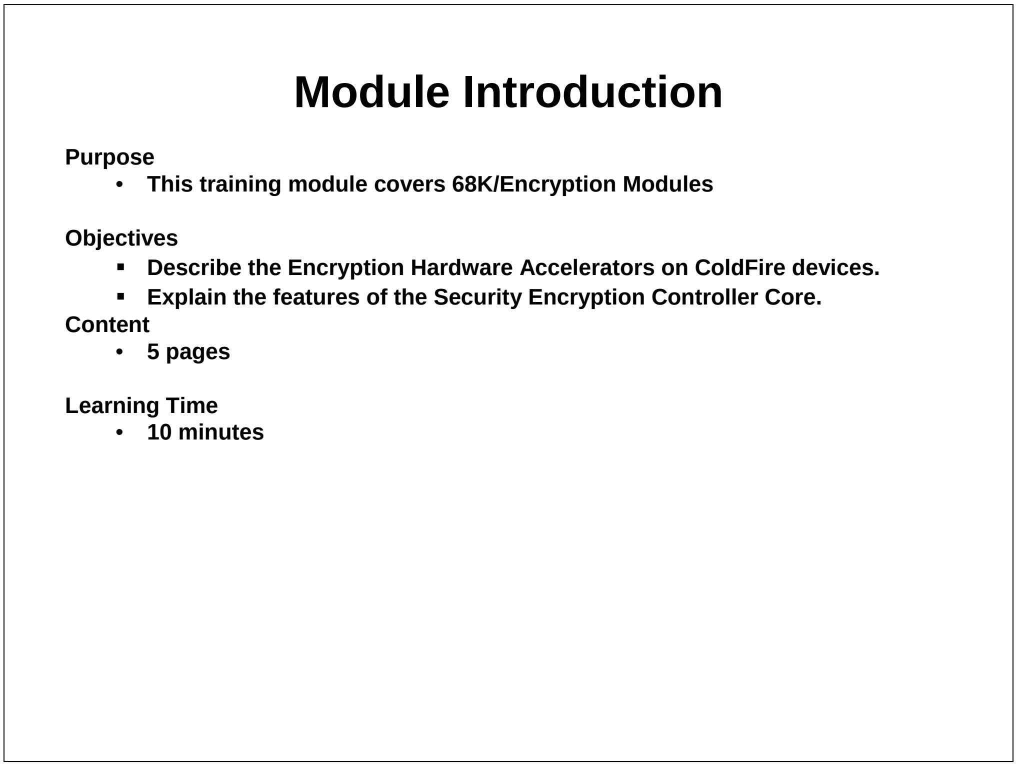


Module Introduction

Purpose

- **This training module covers 68K/Encryption Modules**

Objectives

- **Describe the Encryption Hardware Accelerators on ColdFire devices.**
- **Explain the features of the Security Encryption Controller Core.**

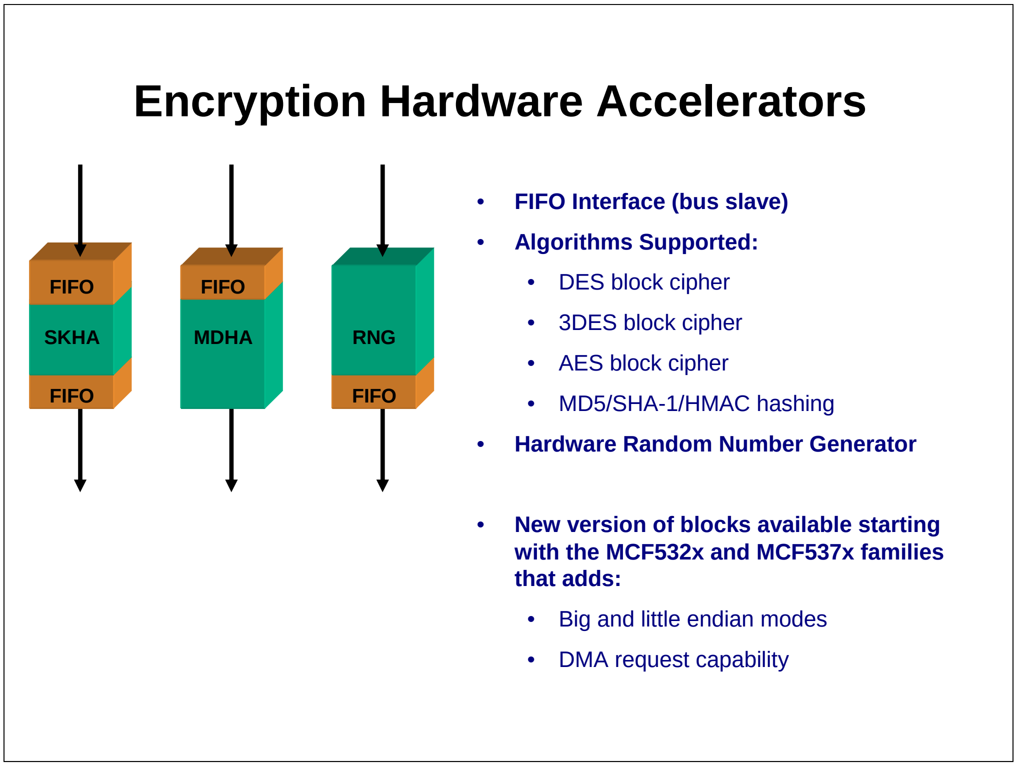
Content

- **5 pages**

Learning Time

- **10 minutes**

This module introduces you to the features of the encryption modules used on ColdFire family devices. These include the encryption hardware accelerators (HAs) and the security encryption controller (SEC).



Encryption Hardware Accelerators

- **FIFO Interface (bus slave)**
- **Algorithms Supported:**
  - DES block cipher
  - 3DES block cipher
  - AES block cipher
  - MD5/SHA-1/HMAC hashing
- **Hardware Random Number Generator**

- **New version of blocks available starting with the MCF532x and MCF537x families that adds:**
  - Big and little endian modes
  - DMA request capability

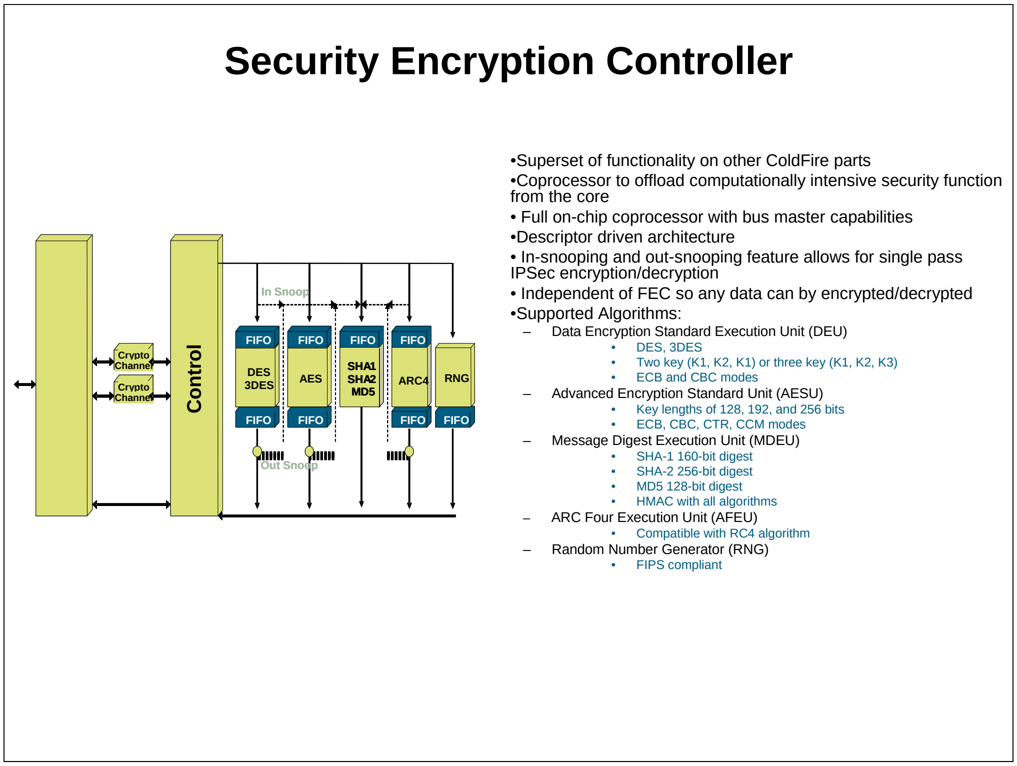
There are several different variations of encryption modules available on ColdFire devices. One version uses individual encryption hardware accelerators or (HAs). The HAs are actually three completely independent modules—the symmetric key hardware accelerator (SKHA), the message digest hardware accelerator (MDHA), and the hardware random number generator (RNG).

The SKHA supports the DES, triple DES, and AES block cipher algorithms.

The MDHA implements hashing algorithms—MD5 and SHA-1. Both hash algorithms can be used in HMAC or non-HMAC mode.

The RNG is a FIPS 140 compliant hardware random number generator.

In order to help increase performance some new features have been added to the HAs. These changes are available starting with the MCF532x and MCF537x family devices. The updated modules are programmable for big or little endian modes, where the original HA implementations only supported little endian data. Programmable DMA request capability has also been added to the SKHA and MDHA blocks.



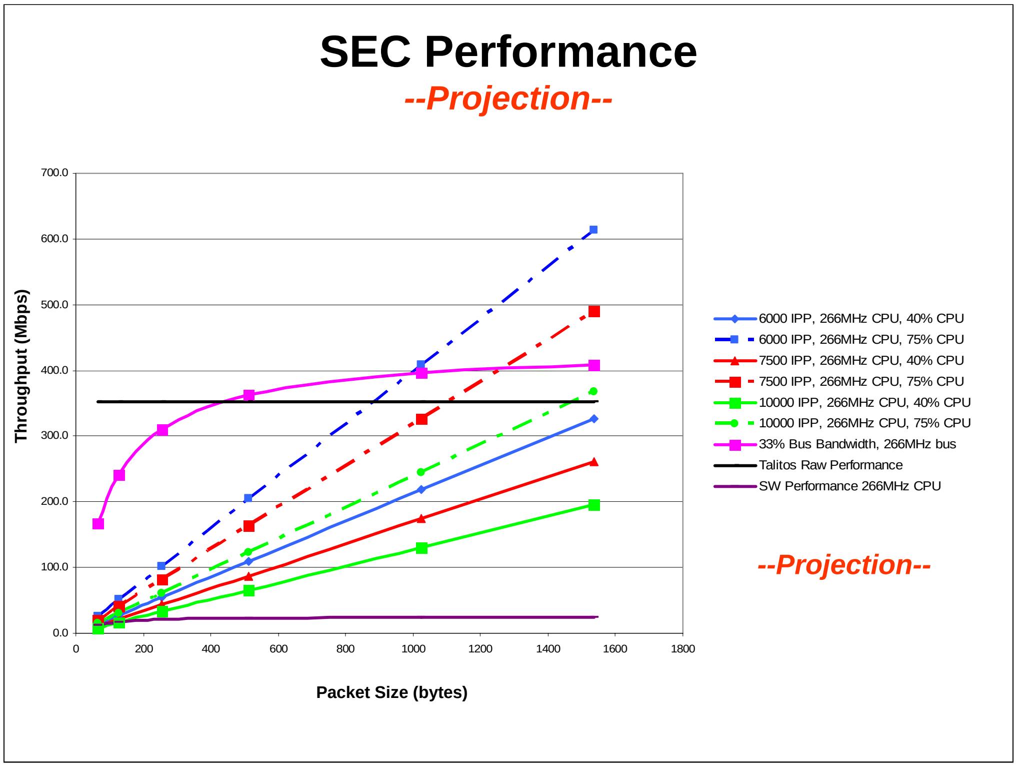
Security Encryption Controller

- •Superset of functionality on other ColdFire parts
- •Coprocessor to offload computationally intensive security function from the core
- • Full on-chip coprocessor with bus master capabilities
- •Descriptor driven architecture
- • In-snooping and out-snooping feature allows for single pass IPSec encryption/decryption
- • Independent of FEC so any data can by encrypted/decrypted
- •Supported Algorithms:
  - Data Encryption Standard Execution Unit (DEU)
    - DES, 3DES
    - Two key (K1, K2, K1) or three key (K1, K2, K3)
    - ECB and CBC modes
  - Advanced Encryption Standard Unit (AESU)
    - Key lengths of 128, 192, and 256 bits
    - ECB, CBC, CTR, CCM modes
  - Message Digest Execution Unit (MDEU)
    - SHA-1 160-bit digest
    - SHA-2 256-bit digest
    - MD5 128-bit digest
    - HMAC with all algorithms
  - ARC Four Execution Unit (AFEU)
    - Compatible with RC4 algorithm
  - Random Number Generator (RNG)
    - FIPS compliant

The security encryption controller (SEC) is a superset of the functionality provided by the HAs. The HAs are slave modules while the SEC is a full co-processor with bus mastering capabilities. The SEC uses a descriptor driven architecture. The SEC will read in descriptor data structures stored in system memory that describe the location and length of data, keys, and other information as well as the algorithm that should be used to process the data. The descriptors allow for the calculation of a block cipher in conjunction with a hashing algorithm in a single descriptor.

The SEC is a coprocessor that operates independently of the other modules. It is not tied directly to the FEC module, so it can process incoming or outgoing data from any of the communications modules on a device, or it can be used to encrypt and decrypt bulk data stored in external memory.

The SEC uses five execution units (EUs) that act as the math engines to perform the various algorithms. The DEU supports DES and triple DES. The AESU performs the AES cipher. The MDEU supports MD5, SHA-1, and SHA-2 hashing algorithms. The AFEU performs a cipher compatible with the RC4 algorithm. The RNG generates FIPS compliant 32-bit random numbers.



The primary advantage of using hardware encryption acceleration is the performance gain. Encryption can be implemented in software; however, the algorithms can be complex and time-consuming. Using a hardware encryption accelerator allows for faster encryption calculations. Plus offloading the CPU core from performing the encryption allows for more CPU bandwidth available for handling other tasks. This graph shows the range of performance expected on the SEC for the MCF547X and MCF548X silicon for 3DES, HMAC, SHA-1, which is the basic set of accelerators required to do IPSEC.

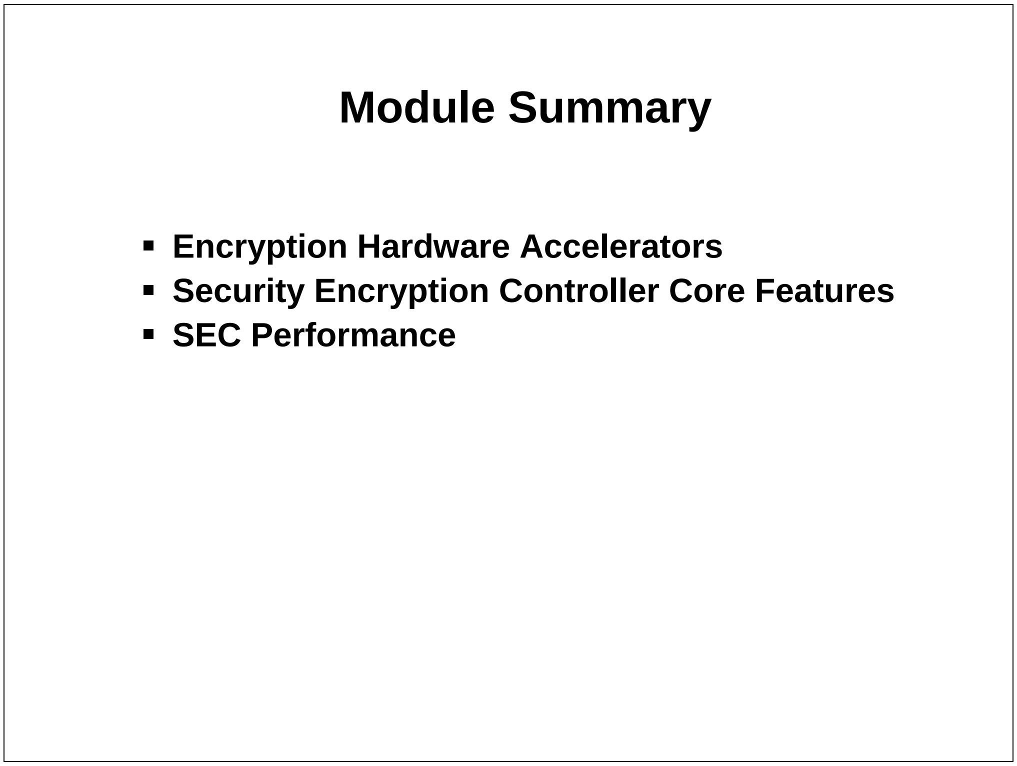
The purple line on the bottom indicates the data throughput expected for software implementation of 3DES-HMAC-SHA-1.

It is clear from this diagram that the only time software is a reasonable solution from a performance perspective is with very small packet sizes, less than 100 bits.

The black line on the graph shows that the theoretical maximum throughput of the Encryption accelerator on the silicon is approximately 350Mbps, assuming no internal bus or I/O limitations.

The remaining colored lines show reasonable combinations of processor activity, bus utilization, and Instructions Per Packet (IPP) that will typically bound the performance for the encryption accelerator.

Thus, for a packet size of 800 bits, it is reasonable to expect that the overall IPSEC throughput will be somewhere between 100Mbps (solid green line) and 300Mbps (dashed blue line) depending upon the availability of the internal bus and the instructions done per packet by the CPU.



Module Summary

- Encryption Hardware Accelerators
- Security Encryption Controller Core Features
- SEC Performance

In this module, you learned about he features of the encryption hardware accelerators and the security encryption controller.

You also learned how using hardware acceleration for encryption operations can help to increase both encrypted data throughput and overall system performance.