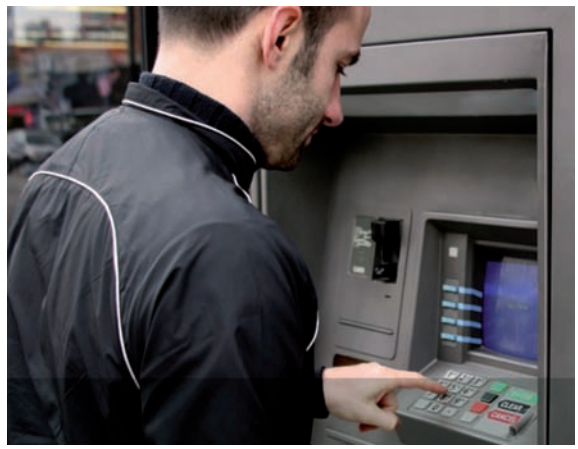
Soluciones de Seguridad de Freescale Parte III: Aceleradores Criptográficos en la familia de procesadores Coldfire

Por Luis casado de Freescale Semiconductor

Freescale Semiconductor
www.freescale.com

En esta tercera parte de la serie abordamos principalmente el estudio de los módulos CAU (Cryptographic Acceleration Unit) y RNGA (Random Number Generator Accelerator) presentes en algunos de los más recientes dispositivos de la familia Coldfire de Freescale.
Además de estos módulos CAU y RNGA podemos encontrar otros aceleradores criptográficos hardware dentro de diferentes miembros de la familia Coldfire, como RNG, MDHA y SKHA, de los que daremos una breve descripción. La integración de los módulos CAU y RNGA proporciona una solución de bajo coste y altas prestaciones y la podemos encontrar tanto en nuevos microcontroladores (MCU) y microprocesadores (MPU) de la amplia familia Coldfire.
Para más información, visite www.freescale.com/ coldfire



En esta serie de artículos, cuyo hilo conductor ha sido la implementación de funciones criptográficas y de seguridad para procesadores de Freescale, hemos introducido diferentes conceptos relacionados con estas aplicaciones, cada día mas demandadas por nuestros clientes.

En este artículo final de la serie, seguiremos introduciendo una serie de conceptos o definiciones, que nos ayuden a comprender mejor la utilización de los aceleradores hardware, que nos permitan la implementación de funciones criptográficas de una manera fácil y eficiente.

Servicios de Seguridad

En los últimos años, la implementación de protocolos de seguridad, como por ejemplo IPSec, ha sido demandada por nuestros clientes. Aplicaciones de comercio electrónico, conexión a redes por VPN son aplicaciones que necesitan seguridad en las comunicaciones, pero debemos añadir también aplicaciones industriales, donde el acceso a redes públicas puede ser totalmente necesario.

Los servicios de seguridad que un sistema criptográfico nos puede ofrecer son principalmente:

Confidencialidad

Previene de la escucha de mensajes por personas o máquinas ajenas al mismo. Debe asegurar que la información almacenada o transmitida solo es accedida y legible para partes autorizadas. Para ello se utilizarán métodos de cifrado de la información que aseguren también de la privacidad como por ejemplo DES, 3DES, AES, RC-4.

Autenticación

Previene de la suplantación de identidad. Puede ser en un solo sentido, donde un interlocutor es anónimo y el otro esta identificado o mutua, donde ambas partes conocen la identidad del otro. Asegura que el origen de la información está perfectamente identificado y que no es falsa o ha sido suplantada. La criptografía de clave pública proporciona el mecanismo para evitar la suplantación de identidad.

Integridad de los datos

Previene de la manipulación indebida de los datos (tampering). Asegura que solo partes autorizadas pueden modificar la información almacenada o transmitida. Modificación incluye escritura, cambio de estado, borrado, creación, retransmisión o reproducción de los mensajes transmitidos. Asegura que el contenido y los detalles de la información permanecen inalterados.

La integridad de los datos también se puede referir a los mecanismos de auto corrección de posibles errores en la transmisión, pero que no es parte del sistema de seguridad, si no del sistema de transmisión.

Los sistemas de Hashing pueden prevenir la manipulación indebida de los datos.

No repudio

Previene de la negación del origen del mensaje o la autoridad del mensaje. Es lo más parecido a la firma de una persona. Cuando se firma un contrato, no se puede negar (repudiar) que fuiste quien lo firmó ya que la firma es única para cada persona. En seguridad electrónica, hablaremos de firma electrónica o digital.

Cipher o algoritmo de cifrado

Podemos definir Cipher como cualquier método de transformación de un mensaje para ocultar o proteger su significado. La idea consiste en crear un problema matemático no resoluble, o cuya única resolución sea el aplicar un método de fuerza bruta (Brute Force Attack), donde se debe aplicar cada posible respuesta al problema para encontrar la correcta solución. Esto significa necesitar un tiempo de ataque lo suficientemente elevado para desestimar cualquier ataque por este método.

Tipos de Ciphers en la familia Coldfire

Con la ayuda de los aceleradores hardware incluidos en los dispositivos Coldfire podremos implementar diferentes tipos de tareas criptográficas:

- Algoritmos de cifrado de clave Simétrica que proporcionan Privacidad. - AES, DES, RC-4.
- Algoritmos de cifrado Asimétrica que proporcionan Autenticación/No Repudio. – RSA.
- Algoritmos de cifrado Hashing. Proporcionan Integridad de los datos. – MD5, SHA-1, SHA-2.

Cipher/Algorithm	Type	Block Size	Key Size	Common Modes
DES	Symmetric Block Cipher	64 bit	56 bit	CBC
3DES	Symmetric Block Cipher	64 bit	168 bit	CBC
AES	Symmetric Block Cipher	128 bit	128 bit, 192 bit, 256 bit	CBC
ARC-4	Symmetric Block Cipher	8 bit	40 - 128 bit	–
RSA	Asymmetric Stream Cipher	NA	Up to 2048 and 4096	–
MD-5	Hashing Cipher	512 bit	Up to 512 bit	HMAC
SHA-1/SHA-2	Hashing Cipher	512 bit	Up to 512 bit	HMAC

Algoritmos de Cifrado o Cipher implementados en dispositivos Coldfire

Algoritmos de cifrado de clave simétrica

DES: Algoritmo de cifrado que opera sobre bloques de datos de 64 bits. Utiliza una clave de 64 bits (56 bits + 8 parity bits). Puede ser abierto por métodos de fuerza bruta en un tiempo relativamente reducido.

3DES: Utiliza el mismo algoritmo que DES, pero utilizando tres diferentes claves y tres ejecuciones del algoritmo. Se puede utilizar con dos claves, donde dos de ellas son iguales. La clave efectiva es de 192 bits en el caso de utilización de tres claves y de 128 bits es el caso del uso de dos claves. Mas seguro que DES, pero mas lento de ejecución.

AES: Proceso de los datos en bloques de 128 bits y permite el uso de claves de 128, 192 o 256 bits. Mas rápido de implementación que DES, ya que realiza menos operaciones. Actualmente considerado totalmente seguro.

ARC4: En origen desarrollado como algoritmo de cifrado para RSA. Opera con bytes individuales y soporta claves de 40 a 128 bits en incrementos de 1 byte. Es más rápido de ejecutar que los algoritmos de cifrado por bloques.

Certificados

Proporcionan una manera segura de comunicación en la que un certificado es enviado en lugar de sólo una clave pública. El certificado incluye:

- La clave pública
- Información de Identificación.
- Fecha de la emisión y caducidad del certificado.
- Firma digital de una autoridad certificadora.

Si confías en la autoridad certificadora, puedes confiar en la clave pública del certificado.

Algoritmos de cifrado Hashing

Utilizados para comprobar la integridad de los datos y que no han sido modificados en el tránsito. Utilizan el mismo concepto básico de un calculo de checksum o CRC (Cyclical redundancy check) pero con más complejidad, ya que el calculo matemático del CRC es demasiado simple. Utilizando algoritmos matemáticos más complejos y añadiendo la utilización de claves, funciones de hashing hacen imposible o muy difícil recalcular un valor Hash del mensaje modificado. Este sistema es más rápido que los métodos de encriptación de bloques. Podremos implementar:

Message Digest (MD-5): Primer sistema de cifrado hashing, usado junto a encriptación DES. Utiliza un valor hash de 128 bits.

SHA (Secure Hash Algorithm): Mejora las prestaciones de MD-5. Dos versiones, SHA-1 (160 bits) y SHA-2 (256 bits). SHA-1 es comúnmente utilizado con encriptación 3DES.

Algoritmos de cifrado de clave asimétrica o sistema de clave pública

Los algoritmos de clave simétrica utilizan dos claves, una para cifrar y otra para descifrar.

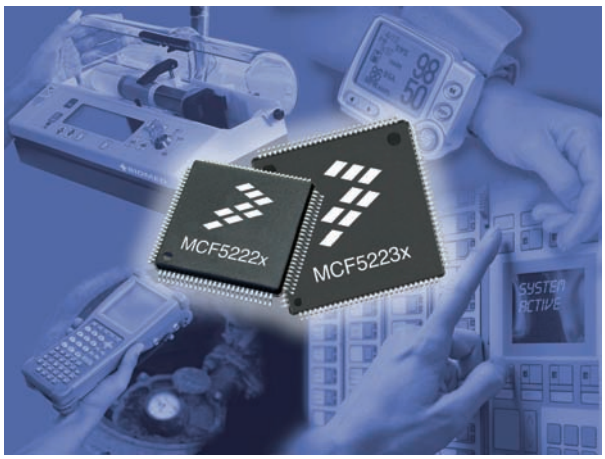
RSA es el sistema mas utilizado en sistemas de clave simétrica. Usando una clave pública para cifrar y una clave privada para descifrar permite el envío de mensajes confidencialmente. Utilizando una clave pública para descifrar y una clave privada para cifrar permite la autenticación del mensaje.

El principal problema es que necesita más tiempo de proceso que los sistemas de clave simétrica. Habitualmente se utiliza para el intercambio seguro de claves u otras variables que serán utilizadas para la transmisión segura del resto del mensaje utilizando un algoritmo de clave simétrica.

Generadores de números aleatorios

Si cerramos todas las puertas y ventanas de nuestro domicilio, ¿podemos decir que nuestra casa es segura? ¿Qué diremos si hemos dejado la llave en la cerradura de entrada? Un algoritmo de cifrado no es seguro en sí mismo, es tan seguro como lo es la clave utilizada para cifrar la información. Es el motivo por el cual debemos comenzar con una clave generada de forma aleatoria.

Los generadores de números aleatorios por software realmente son generadores de números seudo aleatorios (PRNG). Necesitan de una semilla inicial para la generación del número y el método de generación de esa semilla debe ser privado o una tercera parte será capaz de generar claves válidas para su sistema. Por lo tanto, se necesita de un generador de verdaderos números aleatorios que constituyan la semilla para el algoritmo software de generación de claves.



Seguridad en las comunicaciones

Con la familia de dispositivos Coldfire podemos implementar métodos de seguridad en las comunicaciones, a nivel de red, de transporte y de aplicación:

IPsec/IKE – Seguridad IP, proporciona confidencialidad e integridad de los datos y autenticación de los nodos dentro de una red privada. Opera en la capa de red 3.

SSL/TLS – (Secure Socket Layer/ Transport Layer Security), proporciona confidencialidad en las comunicaciones y autenticación de los nodos dentro de redes públicas, opera en la capa de red 4 y proporciona seguridad a las aplicaciones.

SSH – (Secure Shell), es un programa que permite la conexión remota con otra computadora o procesador de la red, ejecutar comandos en la máquina remota y mover archivos de una máquina a otra. Proporciona un alto nivel de seguridad de acceso y cifrado de los datos.

A continuación describiremos cada uno de los módulos disponibles en la familia de procesadores Coldfire.

CAU

El módulo CAU (Cryptographic Acceleration Unit) es un coprocesador criptográfico al que se accede por parte de la CPU por medio de instrucciones de coprocesador. El módulo CAU soporta aceleración hardware de los siguientes algoritmos criptográficos: DES, 3DES, AES, MD5 y SHA-1.

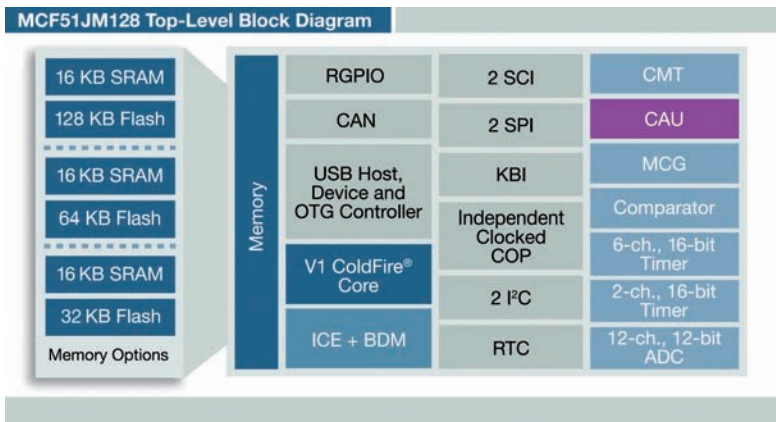
Características principales

- Solución de aceleración criptográfica de bajo coste.
- Alto soporte para seguridad de red TCP/IP
  - º SSL, IPSec
- Incremento significativo de procesado del sistema
- Soporte para todas las versiones de núcleo ColdFire, V1, V2, V3, V4e, V4m
- Solución simple y flexible

El módulo CAU realiza el coprocesado de funciones críticas en hardware y constituye una unidad opcional en los dispositivos capaces de integrarlo. Freescale proporciona una librería de criptografía que ofrece una solución completa de cifrado con unas conocidas prestaciones.

Algoritmos soportados

- Algoritmos de cifrado de bloque de clave Simétrica
  - º Data Encryption Standard (DES)
  - º Advanced Encryption Standard (AES)
    - Claves de 128, 192 y 256 bit
- Funciones Message digest
  - º Message Digest 5 (MD5)
  - º Secure Hash Algorithm (SHA-1)
- Soporta diferentes modos de operación (3DES, Cipher_block_chaining (CBC), Counter (CTR), Hash Message Authentication Code (HMAC), etc.



Arquitectura

El interfaz entre la CPU y el coprocesador criptográfico se realiza a través de dos instrucciones cp0ld y cp0st. El módulo CAU integra ocho registros de 32 bits accesibles por medio de instrucciones estándar de la CPU (load, store). No posee memoria local u otro tipo de interfaz y soporta 22 comandos de funciones de Carga, Almacenamiento, Aritmética, Lógica y Criptografía.

En la tabla de la página adjunta (arriba) podemos ver los diferentes comandos que el módulo CAU puede ejecutar y un pequeño ejemplo de cómo se realizaría la implementación en ensamblador de un bucle del algoritmo AES.

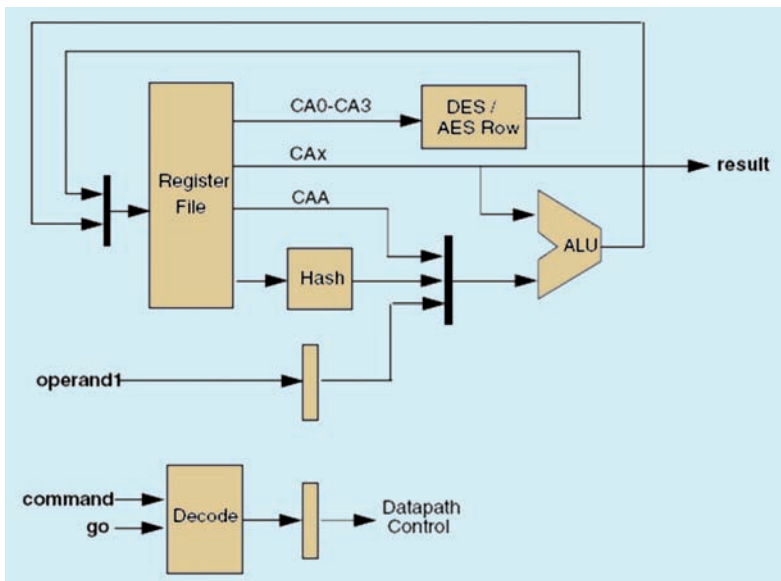


Diagrama de Bloques del Módulo CAU

Command Name	Description	CMD[8:4]	CMD[3:0]	Operation
CNOP	No Operation	0x00	0x0	---
LDR	Load Reg	0x01	CAx	Op1 -> CAx
STR	Store Reg	0x02	CAx	CAx -> Result
ADR	Add	0x03	CAx	CAx + Op1 -> CAx
RADR	Reverse and Add	0x04	CAx	CAx + ByteRev(Op1) -> CAx
ADRA	Add Reg to Acc	0x05	CAx	CAx + CAA -> CAA
XOR	Exclusive Or	0x06	CAx	CAx ^ Op1 -> CAx
ROTL	Rotate Left	0x07	CAx	CAx <<< Op1 -> CAx
MVRA	Move Reg to Acc	0x08	CAx	CAx -> CAA
MVAR	Move Acc to Reg	0x09	CAx	CAA -> CAx
AESS	AES Sub Bytes	0x0A	CAx	SubBytes(CAx) -> CAx
AESIS	AES Inv Sub Bytes	0x0B	CAx	InvSubBytes(CAx) -> CAx
AESC	AES Column Op	0x0C	CAx	MixColumns(CAx)^Op1 -> CAx
AESIC	AES Inv Column Op	0x0D	CAx	InvMixColumns(CAx^Op1) -> CAx
AESR	AES Shift Rows	0x0E	0x0	ShiftRows(CA0-CA3) -> CA0-CA3
AESIR	AES Inv Shift Rows	0x0F	0x0	InvShiftRows(CA0-CA3) -> CA0-CA3
DESR	DES Round	0x10	IP FP KS[1:0]	DES Round(CA0-CA3)->CA0-CA3
DESK	DES Key Setup	0x11	0 0 CP DC	DES Key Op(CA0-CA1)->CA0-CA1 Key Parity Error & CP -> CASR[1]
HASH	Hash Function	0x12	0 HF[2:0]	Hash Func(CA1-CA3)+CAA->CAA
SHS	Secure Hash Shift	0x13	0x0	CAA <<< 5 -> CAA, CAA->CA0, CA0->CA1, CA1 <<< 30 -> CA2, CA2->CA3, CA3->CA4
MDS	Message Digest Shift	0x14	0x0	CA3-> CAA, CAA->CA1, CA1->CA2, CA2->CA3,
ILL	Illegal Command	0x1F	0x0	0x1->CASR[0]

Comandos soportados por el módulo CAU

```
cp0ld.l  %d0,%d0,#TL,#AESS+CA0    /* sub bytes w0 */
cp0ld.l  %d0,%d0,#TL,#AESS+CA1    /* sub bytes w1 */
cp0ld.l  %d0,%d0,#TL,#AESS+CA2    /* sub bytes w2 */
cp0ld.l  %d0,%d0,#TL,#AESS+CA3    /* sub bytes w3 */
cp0ld.l  %d0,%d0,#TL,#AESR        /* shift rows */
cp0ld.l  (%a0)+,%d0,#TL,#AESC+CA0 /* mix col, add key w0 */
cp0ld.l  (%a0)+,%d0,#TL,#AESC+CA1 /* mix col, add key w1 */
cp0ld.l  (%a0)+,%d0,#TL,#AESC+CA2 /* mix col, add key w2 */
cp0ld.l  (%a0)+,%d0,#TL,#AESC+CA3 /* mix col, add key w3 */
```

Ejemplo de código para el módulo CAU

Como hemos mencionado anteriormente, Freescale proporciona una librería software por cada uno de los núcleos existentes de Coldfire para facilitar la implementación de los algoritmos de seguridad y cifrado.

Esta librería posee las siguientes características:

- Funciones criptográficas (low level) usando instrucciones del coprocesador
  - Manejo de claves, cifrado/descifrado de bloques
  - SHA-1 y MD5
- Interfaz de programación en leguaje C
- Implementación optimizada en lenguaje ensamblador de ColdFire

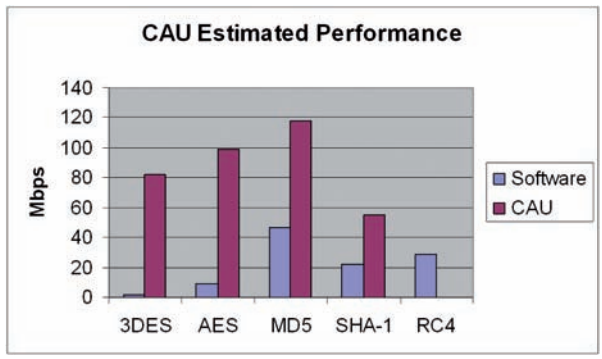
La librería posee un fichero H estándar de lenguaje C con los prototipos de todas las funciones. Estas funciones permiten cambio de contexto seguro (thread safe) si los registros del módulo CAU son salvados en un cambio de tarea.

La librería incluye las siguientes funciones:

- *cau_aes_set_key*
  Ejecuta una expansión de clave AES.
- *cau_aes_encrypt*
  Cifra un bloque de datos de 16 bytes utilizando AES
- *cau_aes_decrypt*
  Descifra un bloque de datos de 16 bytes utilizando AES
- *cau_des_chk_parity*
  Comprueba paridad de clave DES
- *cau_des_encrypt*
  Cifra un bloque de datos de 8 bytes utilizando DES
- *cau_des_decrypt*
  Descifra un bloque de datos de 8 bytes utilizando DES
- *cau_md5_update*
  Actualiza cálculo MD5 para uno o varios bloques de mensajes
- *cau_sha1_update*
  Actualiza cálculo SHA-1 para uno o varios bloques de mensajes

Prestaciones

En el gráfico adjunto se puede comprobar la diferencia de prestaciones que obtenemos en el procesado de datos utilizando el módulo CAU frente a la misma implementación por software del algoritmo.



150/75 MHz CF V2, software routines from OpenSSL

RNGA y RNG

Los módulos RNG (Random number generator) RNGA (Random Number Generator Accelerator) son capaces de generar números aleatorios de 32 bits. Diseñados para cumplir el estándar FIPS-140. El número aleatorio es generado a través de registros de desplazamiento digital cuyos relojes están derivados de osciladores en anillo. La configuración de los registros de desplazamiento asegura la generación de números aleatorios con la requerida entropía y distribución estadística. Freescale recomienda la utilización de estos números aleatorios como semilla (seed) de algoritmos de generación de números aleatorios basado en DES, SHA-1, RSA o BSS para incrementar la seguridad en la generación.

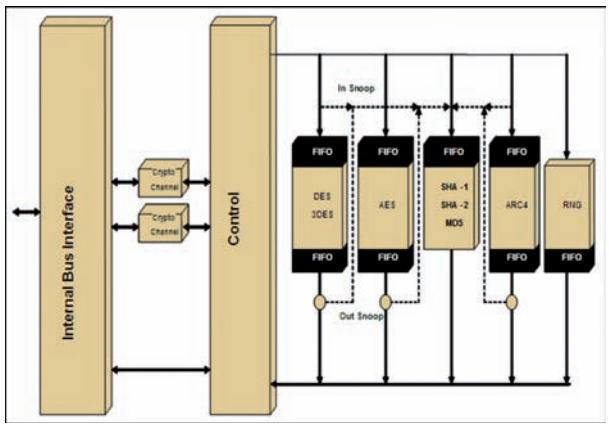


Diagrama de Bloques del módulo Crypto SEC

Dispositivos Coldfire con módulos aceleradores de Cifrado

MDHA (Message Digest Hardware Accelerator)

El módulo MDHA implementa mediante hardware dos de las más populares funciones Hash: SHA-1 y MD5. Ambas funciones son críticas en implementaciones del protocolo IPSec. También incluye el hardware necesario para la generación de HMAC (Hashed Message Authentication Code) especificado en RFC 2104 y EH-MAC (Enhanced Hashed Message Authentication Code), utilizando el algoritmo SHA-1.

Características principales del módulo MDHA

- MD5 128-bit hash (RFC 1321)
- SHA-1 160-bit hash (ANSI X9.30-2 y FIPS 180-1)

Producto	Módulos Criptográficos	Interna Flash(KByte)	Núcleo	Nº pines
MCF51JMX	CAU, RNGA	128,64	ColdFire V1	80,64,44
MCF5223X	CAU, RNGA	256,128	ColdFire V2	112,121,80,64
MCF5225x	CAU, RNG	512,256	ColdFire V2	100,144
MCF527X	MDHA,SKHA, RNG	-	ColdFire V2	196,160,256
MCF532X	MDHA,SKHA, RNG	-	ColdFire V3	256,196
MCF537X	MDHA,SKHA, RNG	-	ColdFire V3	256,196
MCF547X	SEC	-	ColdFire V4e	388
MCF548X	SEC	-	ColdFire V4e	388
MCF5444x	CAU, RNG	-	ColdFire V4m	256,36

SKHA (Symmetric Key Hardware Accelerator)

El modulo SKHA es un coprocesador criptográfico diseñado para la implementación dos de los dos algoritmos de cifrado de clave simétrica mas ampliamente utilizados, AES (Advanced Encryption Standard) y DES (Data Encryption Standard).

Características principales del módulo SKHA

- AES - clave de 128 bit
- DES – clave 64 bit (con paridad)
- 3DES - 2 claves y 3 claves (128-bits y 192-bits con paridad)

Información Adicional

Más información de los procesadores Coldfire, en la dirección web: www.freescale.com/coldfire