IBM®

Secure Way

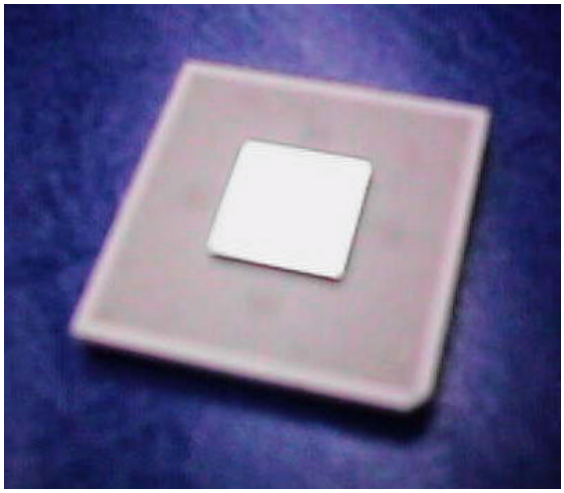
UltraCypher CRYPTOGRAPHIC ENGINE

An OEM offering from IBM

Highlights:

Technology for simplifying native cryptographic support

The IBM UltraCypher is a flexible but high performance subsystem designed to reduce the complexity of integrating fast real-time hardware-based data security into a product. UltraCypher, which employs IBM's advanced CMOS technology, leverages multiple custom cryptographic engines and other unique accelerated state-machines to provide the complex and numerically intensive operations required for ultra secure data encryption/decryption, authentication and key management. UltraCypher when incorporated into a design seamlessly off-loads the industry standard cryptographic functions of DES, Triple DES, MAC, Triple MAC, RSA, Modular Exponentiation and other Modular arithmetic functions, SHA-1 hashing and random number generation all under a common architecture contained in a single 25 mm ceramic IC package.



Hardware acceleration means performance superiority

A hardware-based data security solution exploiting IBM's UltraCypher, which off-loads the security algorithm burden from your product's main control processor, provides up to a 100X cryptographic performance improvement over traditional software based solutions. In addition by performing all security and privacy functions via hardware the vulnerability to outside attack is vastly reduced from the susceptibility afforded by software.

Excellent reliability

IBM's UltraCypher 's enhanced functionality coupled with its CBGA (ceramic ball grid array) package, low 4 watts of power dissipation and state-of-the-art .36 micron CMOS technology provides excellent inherent reliability over alternative multi-component alternatives

Functional Description:

IBM's UltraCypher consists of the following logically elements providing the functional capabilities listed:

DES Engine

Features of this engine include:

- DES, Triple DES, MAC and Triple MAC functions
- Electronic codebook (ECB) support and cipher block chain (CBC) modes of operation
- 3 internal 64-bit key registers loadable from a ISA port
- 64-bit initial vector register loadable from a ISA port
- 64-bit input & output registers readable from both a 16-bit ISA port or a 32-bit PCI add-on port via the output FIFO
- DES Engine performance of up to 53-MBytes/Sec when using the PCI Add-on bus port and the FIFO's
- Optional DES assist for data padding of data blocks which are not multiples of 64-bytes

SHA Engine

Features of this engine include:

- SHA-1 secure hash algorithm (512-bit blocks to 160 bit)
- Four 32-bit K registers with fast initialization to FIPS-180 Constants via an ISA port accessible control register
- Five 32-bit H registers with fast initialization to FIPS-180 initial values by an ISA port accessible control register. Hashing data loadable into H registers via the 16-bit ISA port or the 32-bit PCI add-on port and input FIFO. Hash results readable from five 32-bit H registers via ISA port.
- Five internal registers for SHA-1 hash results creation
- No padding of data by the hardware, data must be in complete 512-bit blocks
- SHA engine exercises FIPS 180-1 algorithm only. Digital Signature Standard FIPS PUB-186 pseudo random number creation possible by programming *K* constants and *H* initialization vector registers via the ISA bus input.
- SHA-1 engine performance of up to 25.5-MBytes/Sec

RSA Engine

The RSA engine performs the following modular arithmetic and exponentiation functions for very high speed RSA encryption:

Modular Exponentiation with CRT (chinese remainder theorem)	$R=A^{(Bp,Bq)}\text{mod}(N_p,N_q)$
Modular exponentiation	$R=A^B \text{ mod } N$
Modular multiplication	R=(A*B)mod N
Modular addition	R=(A+B) mod N
Addition	R=(A+B)
Subtraction	R=(A-B)
2's complement	R=~A+1
Signature	$R=A^B$mod N;if(2R>=N)R=N-R
Verify	$R=A^B$ mod N;if(R mod16!=6) R=N-R

The RSA engine is a 2048-bit engine with the following registers:

Operand Register	Length (bits)	Contents
A	2048	Data
B	2048	Exponent
B_p	1088	CRT Mod Expo. only
B_q	1024	CRT Mod Expo. only
N	2048	Module
N_q	1088	CRT Mod Expo. only
N_p	1024	CRT Mod Expo. only
U	1088 (CRT only)	Multiplicative inverse for CRT
R	2048	Results

- Registers B, B_p, B_q, N, N_p, N_q and U are write only from the ISA port of the UltraCypher module.
- Register R (results) is read only from the ISA port of the UltraCypher module
- Chinese Remainder (CRT) Operands
  - A = data
  - B_p= the largest of two odd primes so $N=N_p*N_q$
  - B_q= the smallest of two odd primes so $N=N_p*N_q$
  - N_p= B mod(N_p-1)
  - N_q= B mod(N_q-1)
  - U = Multiplicative inverse: $N_q^{-1} \text{mod } N_p$

Exponentiation performance can be enhanced by enabling the built-in Chinese Remainder Theorem (CRT) algorithm. Performance is 50 Exponentiations/Sec for 2048-bit operations, and 200 Exponentiations/Sec for 1024-bit operations using CRT.

Control and Status Registers

There are ten 16-bit Control, Setup, and Status registers which are written and read via the ISA bus. Some are read only and some are write only from outside of the UltraCypher module. These registers control the data paths and various engines inside of the UltraCypher and provide information as to the status of the engines and FIFO's.

Random Number Generation - (up to 64-Kb/sec)

A 64-bit shift register is provided for the collecting of Random data bits generated from outside the UltraCypher module. The external 1-bit input (usually a random noise source) is sampled and loaded into bit-0 of the shift register. The sampling rate is controlled from control register bits which are loaded via the ISA bus. The collected data bits are shifted after each new sampling of data. When the shift register is full of new data an interrupt is generated and the shift register contents may be read from the ISA data port.

FIFO Data Buffering

A 128x32-bit Input FIFO and a similar Output FIFO is provided on the UltraCypher module to buffer the PCI Add-on bus.

INPUT FIFO Inputs	INPUT FIFO Outputs	OUTPUT FIFO Inputs	OUTPUT FIFO Outputs
PCI add-on bus	DES engine	DES engine	PCI add-on bus
ISA bus	SHA-1 engine	ISA bus	ISA bus
	OUTPUT FIFO	INPUT FIFO	
	ISA bus		

Physical Description

I/O

A multipurpose 16-bit data interface supports ISA 16-bit cycles at 8 MHz. This same multipurpose interface can run up to 33 MHz.. Addressing of the UltraCypher's internal registers is via the 18-bit ISA address bus. The 32-bit PCI Add-on bus was designed to interface with the AMCC 32-bit PCI bridge chip and to support PCI bus master.

There are 8 IRQ interrupt outputs, reset, other control lines, clock I/O, and test I/O comprising the remaining 214 total chip I/O.

Technology and Power

The UltraCypher consists of a 9mm CMOS chip mounted on an enhanced 25 mm CBGA (ceramic ball grid array) substrate which contains 360 I/O balls.

Power

Voltage	3.3 volts
Max. Power	4 watts

IBM Corporation
S/390 OEM Business Unit
Mail Stop P339
522 South Road
Poughkeepsie NY 12602-5400
1-800-IBMS OEM