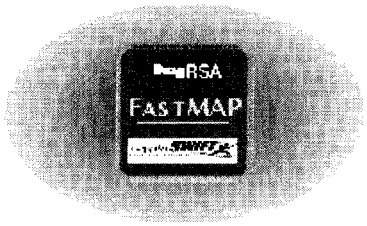
ON THIS PAGE

RAINBOW TECHNOLOGIES
Security Solutions for the Information Age



FastMAP ASIC

High Performance Public Key Processor

Able to perform a wide variety of public key algorithms with extraordinary speed, the versatile FastMAP ASIC is well-suited to supporting many emerging cryptographic protocols.

FastMAP is the ideal single chip performance solution for virtual private network (VPN), financial processing, and other security oriented hardware products. FastMAP is particularily appropriate for high volume servers or gateways based on IPSec ISAKMP, SSL, SET and other popular public key based protocols.

With twin exponentiation units and a PowerPC (PPC) 401 controller, FastMAP can perform a reference full 1024 bit RSA private key operation in under 5 ms. RSA in varying modulus sizes up to 4096 bit are supported. FastMAP also performs Diffie-Hellman (DH) and the Digital Signature Algorithm (DSA) faster than any other ASIC currently available. All algorithms are fully patent paid for any application.

FastMAP includes random number generation from a high speed dedicated generator, ensuring top quality key generation and padding. FastMAP also contains a custom cryptographic algorithm development and execution environment with full access to its twin general purpose 512 x 512 bit multipliers.

FastMAP communication takes place over a PCI-standard interface with built-in input and output FIFOs for efficient data transfer. (PCI ensures that multiple FastMAP processors can easily be used in parallel.) Internal functions are controlled by the PPC core, which acquires instructions through the ASIC's

TOP OF PAGE

external FLASH interface on boot-up. The PPC is a full-function 32-bit processor with internal and external interrupt capability and selectable data and instruction caches. Internal blocks are accessed through instruction and status registers in each functional block.

Features and Benefits

- 0.35µ technology, 3.3 V CMOS.
- IBM 401 Power PC core
- 4-bit to 4096-bit RSA accelerator
- High-grade random number generator
- Data and instruction cache
- Dual modular exponentiators (2-bit to 2048-bit)
- Dual programmable 512-bit multipliers
- Dual 512 x 64 bit RAMs
- 32-bit memory (FLASH/SRAM) interface
- 4-bit general purpose I/O

TOP OF PAGE

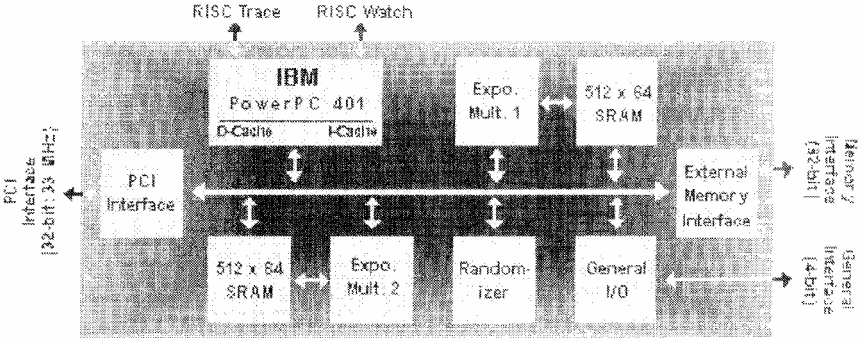
Specifications

RNG Throughput	1024-bit RSA in less than 5 ms
RNG Throughput	1mb/sec.
RISC Processor	IBM PowerPC 401
Package	208-pin PQFP
System Clock	Rate: 33 MHz Duty Cycle: 50/50 +/- 10%
Power Dissipation	~1.4 W @ 33 MHz (estimated)
Temperature Range	0 to 125° C
Operating Voltage	V_{DD} = 3.3V +/- 10%
TTL Compatibility	5V tolerant external memory data bus
PCI	3.3 or 5 V; 33 MHz compliant

TOP OF PAGE

Specifications subject to change notice

Block Level Architecture



For More

Information

RAINBOW TECHNOLOGIES
Security Solutions for the Information Age

50 Technology Drive
Irvine, CA, USA 92618

Voice: (888) 667-4728
Fax: (714) 450-7464
STU III: (310) 533-0738

E-Mail: sabbott@rainbow.com

TOP OF PAGE

Last updated February 9, 1998

FastMAP Performance

Algorithm	Bitsize	FastMAP Operation Time (ms)[1]	Pentium™ II 266 Mhz Operation Time (ms)[2]
RSA Secret Key Sign/Decrypt	1024	< 5 ms	45 ms
	2048	24.5	293
RSA Public Key Verify/Encrypt[3]	1024	0.34	1.1
	2048	1.3	3.2
DSS Sign	1024-bit modulus/160-bit exponent	7.0	24
DSS Verify	1024-bit modulus/160-bit exponent	7.0	30
DH Exponentiation	1024-bit modulus/180-bit exponent	3.9	24
	1024-bit modulus/300-bit exponent	6.4	39
	1024-bit modulus/1024-bit exponent	22	154

FastMAP for ISAKMP

Basic Handshake to establish a security association		
Algorithm	FastMAP Operation Time (ms)[4]	Pentium™ II 266 Mhz Operation Time (ms)
2 - Diffie-Hellman Operations - 180-bit exponent	3.9 x 2	24 x 2
	7.8 ms or 128 connections per second per chip	48 ms or 20 connections per second per chip
2 - Diffie-Hellman Operations - 300-bit exponent	6.4 x 2	39 x 2
	13 ms or 78 connections per second per chip	78 ms or 12 connections per second per chip
With DSS based X.509 Authentication		
2 - Diffie-Hellman Operations - 180-bit exponent	3.9 x 2	24 x 2
1 - DSS sign	7	24
2 - DSS verifies	7 x 2	30 x 2
	29 ms or 35 connections per second per chip	132 ms or 7 connections per second per chip
2 - Diffie-Hellman Operations - 300-bit exponent	6.4 x 2	39 x 2
1 - DSS sign	7	24

2 – DSS verifies	7 x 2	30 x 2
	34 ms or 30 connections per second per chip	162 ms or 6 connections per second per chip

[1]Preliminary results.
[2]Pentium™ II results from http://www.eskimo.com/~weidai/benchmarks.txt.
[3]FastMAP uses 65537 as exponent while Pentium™ II uses 17, the results are comparable.
[4]Predicted results.

Contact Shawn Abbott sabbott@rainbow.com for additional performance details.
Results subject to change. This document does not constitute an offer for sale.

Last updated February 20, 1998.