PRODUCT BRIEF

AHA601 / AHA602

Crypto Accelerator

FEATURES

- Optimized public key coprocessor
- Supports public key algorithms such as RSA, Diffie-Hellman and elliptic curve cryptography (ECC)
- Supports bulk encryption and hashing, including header and trailer processing for IPsec and SSL
- Supports advanced encryption standard (AES)
- Supports message digest hardware (MDH)
- NIST compliant random number generation
- Drivers and plug-ins for Apache web servers
- Linux kernel module and OpenSSL patch
- PCIe 2.0 x4 interface
- Low Profile PCIe Form Factor

APPLICATIONS

- Remote access gateways
- Network admission control appliances
- Application delivery controllers
- Internet servers using SSL/TLS

PERFORMANCE

	AHA601	AHA602
1024b Private Keys/s	29.3K	110.7K
2048b Private Keys/s	8.4K	31.7K
4096b Private Keys/s	1.7K	6.7K
Bulk Encryption	6 Gb/s	12 Gb/s

INTRODUCTION

The AHA601 and AHA602 accelerators are four-lane PCI Express Gen 2.0 plug-in cards that perform crypto coprocessing as a public key offload solution for data center and network security appliances. Public key algorithms such as RSA, Diffie-Hellman and elliptic curve cryptography (ECC) are the basis of digital signature and key exchange protocols that make electronic commerce possible.

Deprecation of 1024-bit keys by the United States National Institute of Standards and Technology in 2010 means that 2048-bit and larger keys are becoming the norm. However, the computational requirement to perform 2048-bit operations can be up to five times greater than 1024-bit. Using software on general purpose processors is impractical in systems requiring thousands of operations per second. The AHA601 and AHA602 are designed to provide the 2048-bit performance needed by users while also supporting 1024-bit and 4096-bit requirements.

FUNCTIONAL DESCRIPTION

The AHA601 and AHA602 cards accelerate cryptographic algorithms using an integrated security engine (SEC). The SEC is a modular and scalable security core optimized to process the algorithms associated with key generation, key exchange, and multiple authentication. It also supports algorithms commonly associated with SSL/TLS and IPsec bulk encryption. The AHA601 contains a single SEC, while the AHA602 contains three SECs. With the exception of performance, the number of SECs is transparent to the user. The SEC block supports the following functionalities:

Public Key Accelerators

- Modular Arithmetic (4096)
- ECC (1024) over prime field (Fp)
- ECC (1024) over binary fields (F2m)
- Miller-Rabin Prime Test
- RSA Public Key (encrypt verify)
- RSA Private Key (decrypt, sign)
- DSA Sign and Verify
- ECDSA Sign and Verify
- Diffie-Hellman and ECDH secret derivation
- Key Generation for DSA, ECDSA, DH, and ECDH
- Private Key functions are timing equalized

AES Accelerators

- Key lengths 128, 192 , and 256
- ECB, CBC, CTR, CCM, GCM, CMAC, OFB, CFB, and XTS

MDH Accelerators

- SHA-1, SHA-2 256, 384 and 512
- MD5 128 bit digest
- HMAC with all algorithms

Random Number Generator

- NIST compliant, DRBG and SHS

SOFTWARE SUPPORT

The Linux kernel module enables the coprocessor in the kernel's crypto API framework. Any kernel functions that deal with cryptography, such as IPsec or dm_crypt, will use the coprocessor. The OpenSSL patch will execute any supported OpenSSL functions using the coprocessor. OpenSSL is used by many Linux networking applications, such as OpenVPN, OpenSSH, and Apache mod_ssl to name a few.

POWER

The AHA601 and AHA602 are much more power efficient than software based crypto solutions. Power consumption at full throughput is typically 8 watts for the AHA601 and 21 watts for the AHA602. This is a significant power savings and a significant throughput increase compared to a dedicated server class processor.

ORDERING INFORMATION

Part Number	Description
AHA601A01	8.4K – 2Kb Private Key / 6 Gbps Bulk Low Profile PCIe Crypto Accelerator
AHA602A01	31.6K – 2Kb Private Key / 12 Gbps Bulk Low Profile PCIe Crypto Accelerator

ABOUT AHA

The AHA Products Group (AHA) of Comtech EF Data Corporation develops and markets superior integrated circuits, boards, and intellectual property cores for improving the efficiency of communications systems everywhere. AHA has been setting the standard in Forward Error Correction and Lossless Data Compression for many years, and now supports Crypto Acceleration, while still providing flexible and cost effective solutions for today's growing bandwidth and reliability challenges. Comtech EF Data is a wholly owned subsidiary of Comtech Telecommunications Corporation (NASDAQ: CMTL). For more information, visit: www.aha.com.

aha products group

Comtech EF Data Corporation
1126 Alturas Drive • Moscow ID 83843-8331
tel: 208.892.5600 • fax: 208.892.5601
email: sales@aha.com • www.aha.com