

PRELIMINARY EVALUATION REPORT: CENTAUR TECHNOLOGY C5P AES CORE

OCTOBER 6, 2003

Cryptography Research performed an abbreviated design and implementation review of the AES accelerator core in the Centaur Technology C5P processor.

Background

The Advanced Encryption Standard (AES) cipher is used in numerous cryptographic protocols, including TLS (SSL), SSH, and IPSEC. AES is a NIST-ratified set of operating modes for the block cipher Rijndael and is documented in FIPS-197.

Operational Summary

The C5P AES core is accessed via an unprivileged instruction. Block encryption is supported for 128-bit blocks in ECB, CBC, CFB, and OFB modes with 128, 192, and 256 bit keys. Two modes of initialization are supported: hardware-assisted (128 bit key only) and software-precalculated key expansion (required for 192 and 256 bit keys). Cryptography Research tested all supported modes and found the core to be compliant with FIPS-197 reference implementations and test vectors.

Performance

The core uses a round engine that performs a single AES block round operation in two processor clock cycles. Pipelined operation is supported for operations on independent blocks (such as ECB mode encryption), yielding a net throughput of one round per clock. Performance timings (including memory latency) yielded sustained throughput in excess of 15 Gbits/sec (ECB) on a 1.2 GHz processor. This is substantially faster than assembly-coded AES implementations on x86 platforms, which typically require at least 250 clock cycles per block.

Secure State and Process Separation

Developers must exercise caution when manipulating secrets in multi-processing environments, especially if sensitive applications may co-exist with hostile code. The C5P's key management capabilities are designed to provide security equivalent to conventional software AES implementations when the host operating system follows some common conventions.

The AES ciphertext, plaintext, and key are stored in user memory and the C5P core operates on pointers in the EAX, EBX, ECX, EDX, ESI, and EDI registers, which are saved on the user stack during context switches. AES state (including expanded key) is stored in the core and invalidated when the microcode recognizes a context switch, signified by a store to the EFLAGS register. Most common OS context switch paths save and restore EFLAGS.

Although the limited scope of this evaluation did not permit exhaustive testing of possible inter-process interactions, our evaluation did not identify any situations where the C5P would provide less security than a conventional software-only AES implementation.

Conclusion

The AES core in the Centaur C5P provides an easy to use and substantially faster substitute for existing software AES implementations. The core contains microcode support to protect key data and processing intermediates in most anticipated multi-processing environments. We expect availability of this high-performance resource to improve deployment of high-speed encryption capabilities for network security, disk encryption, and other applications.

