The VIA PadLock™ Data Encryption Engine



Introducing the VIA PadLock™ Data Encryption Engine that is used on JRex-VE

The PadLock™ Data Encryption Engine embedded into the new seventh generation 'Nehemiah' core VIA C3 processor features an advanced, hardware-based Random Number Generator (RNG) that provides a simple yet effective method of obtaining high quality randomness without the use of separate software drivers, providing an inherently more secure solution than combined hardware/software RNG solutions.

The unprecedented increase in PC networking and Internet-based commerce has led to growing concerns about corporate and personal data security. Data is kept secure through encryption by means of a key; an attacker must decipher the key to compromise the data security of any computer or network. Such keys are created by Random Number Generators, and the more random a number is, the more secure that key or password becomes.

Greater Security and Assurance

The new generation VIA C3 is ideally suited to security appliances such as firewalls, VPNs, etc, and to other embedded applications, as these systems can benefit from the VIA C3 low power consumption and cost effectiveness, as well as the security features. The hardware RNG of the PadLock Data Encryption Engine is particularly important for embedded systems, as it does not rely on the seed data such as keystroke timing, mouse events or other less random methods typically used to seed software-based RNGs (called pseudorandom number generators).

The PadLock Data Encryption Engine provides greater assurance to end-users, as VIA has integrated the random number generator directly onto the die of the microprocessor, making it much more difficult for an attacker to probe or influence.

PadLock RNG: How It Works

The PadLock Data Encryption Engine RNG uses random electrical noise on the chip as its source of randomness ('entropy'), to securely produce random number values. Logic within the processor core collects entropy from this physical process, pre-processes the data, and queues up to 32 bytes for immediate access by the processor. By collecting the data from physical sources in this way, the RNG produces output that is unpredictable and not influenced by outside sources.

Featuring a direct application level interface through an extended x86 instruction that reads the entropy source, the PadLock Data Encryption Engine RNG includes several operating modes, offering performance from 750K bits per second to as high as 6 million bits per second. Partitioning enables multiple applications to safely share the random number generator.

PadLock Data Encryption Engine: Work and Play Safe

Computers normally operate in a completely deterministic fashion, but deterministic processes cannot create truly random numbers. Hardware random number generators, on the other hand, do make it possible to create true random numbers.

The PadLock Data Encryption Engine provides the hardware necessary to allow developers to directly obtain true high-quality randomness without having to use separate software drivers, providing greater inherent security than other methods of generating randomness.

Note:
The PadLock Data Encryption Engine is currently undergoing comprehensive testing by leading data security firm, Cryptography Research, Inc.; preliminary results show high quality output.

Courtesy by VIA Technologies Inc., Taiwan, 2003