256 and 512 bit PMC Block Encryption Algorithms

FACT SHEET

General Description

The 256 and 512 bit PMC Encryption Algorithms are designed for super-fast encryption/decryption and uncompromised security. Both Type 1 block ciphers have an integrated and selectable cipher feedback function.

Due to the Polymorphic nature of these ciphers, the actual encryption algorithm changes with the key. Perfect randomness, very high processing speed and immunity from every known attack result from this unique design.

Both crypto engines use the full internal state of 256/512 bit in a two-stage design with both stages compiled from the key during key-setup.

The second cipher stage is 100% intrinsically protected from Simple Power Attack (SPA), as well as from Differential Power Attack (DPA) making both ciphers the only encryption algorithms in the world which resist against every known attack.

The 256 bit PMC Block Cipher Engine is available as DLL and C++ source code. It integrates perfectly in existing and new designs live Voice-over-IP, Video-over-IP, VPN's, Network Routers, Fiber Optics Links, Satellite Channels, Disk Encryption, Encryption of the Operating System, File Encryption, License Management, DPA-proof Secure Smart Cards, etc.

The 256 bit PMC Block Cipher Engine encrypts / decrypts data 5 to 7 times faster than AES (Rijndael) while the 512 bit PMC Block Cipher Engine encrypts/decrypts data 10 times faster than AES in multi-block mode. Encrypting 512MByte and decrypting 512MByte on an AMD Athlon XP1800 processor takes only 1.6 seconds. This corresponds to an encryption speed of 5GBit/s.

Features

- 'Type 1' 256 and 512 bit block encryption
- Fully Polymorphic 2-stage design with both stages compiled from the key for optimum processing speed and data security
- DPA-proof Worker cipher stage (stage 2)
- Fastest known cipher, outperforming existing methods by factor 10
- Cipher Recompilation Mode capability for maximum protection of data streams with little entropy
- Easy integration in new and existing applications
- No known attack
- 256 and 512 bit Block PMC is the only available encryption algorithm for Secure Smart Cards
- 5GBit/s encryption speed using inexpensive general-purpose Microprocessors

Applications

- Replacement for unclassified ciphers like DES, Rijndael, and replacement for secret 'Type 1' ciphers with up to 512 key bits
- Fast VPNs with 10 times higher encryption speed
- Encryption of other server-to-server communication
- 1GBit Network Routers and (potentially) HAIPE devices
- High-speed backbones
- IP communication including encrypted Voice-over-IP, Video-on-demand, Webcasts, Video-over-IP
- Broadband Satellite Link Encryption
- Encryption of high-speed telecom links
- Broadband Military Applications
- Encryption of the Operating System for police cars, mobile military, etc.
- DPA-proof Secure Smart Cards
- Unbreakable Software License Management

Concept of PMC Encryption Algorithms

The concept of Polymorphic Encryption is based on the principle of compiled crypto code. A Crypto Compiler uses the passphrase to generate a large Pseudorandom Number Generator. This Compiled PRNG has the ability to alter the content of the Internal State in an unpredictable way.

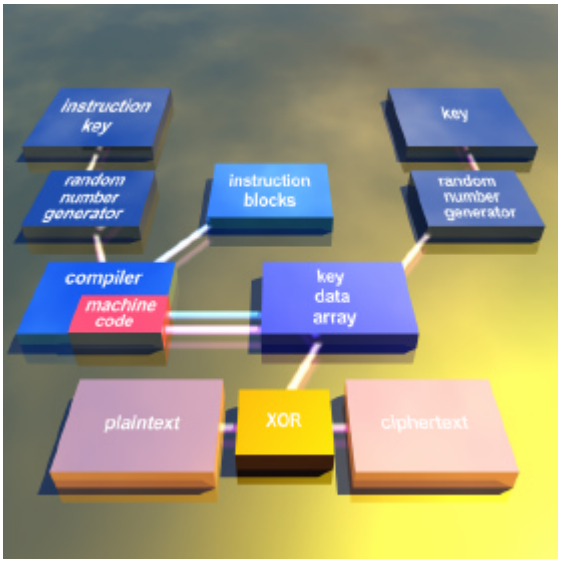

Fig. 1: Basic PMC structure

Unlike the structure shown in figure 1, which shows the simplest possible implementation of a Polymorphic Cipher, the 256 and 512 bit Block PMC Cipher Engines are two-stage implementations.

The content of the Internal State ("key data array") is used to bias an underlying fast Worker Cipher Stage. For the 256 and 512 bit Block PMC Cipher Engines, the Worker Cipher Stage is compiled as well from the passphrase.

Theoretical speed advantage of PMC

In contrast to common ciphers, which all come with the inherent speed limit $O(n^2)$ with n being the size of key k, the use of a crypto compiler has a positive effect on processing speed: There is only a linear relationship O(n) for the keysize n and the processing time.
The compiling process of the keystream generator can be generalized as block assembly with a constant number of key bits selecting the next block to be concatenated to the preceding ones. The processing time for that is O(n). The execution time for n primitive PRNGs is O(n), processing m plaintext bits with only a subset of the Internal State consumes O(m). Consequently the execution time of a Polymorphic Cipher is O(n)+ O(n)+ O(m).
The high encryption speed of Polymorphic Ciphers is unprecedented

Simplified Schematic

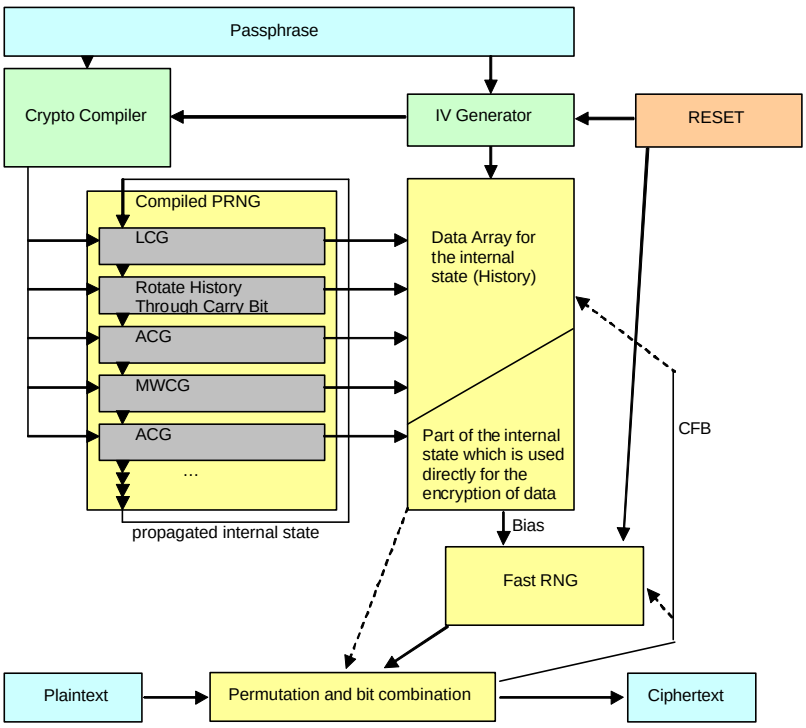

Fig. 2: Two-stage PMC structure

Encryption/Decryption speed normalized to AES test data

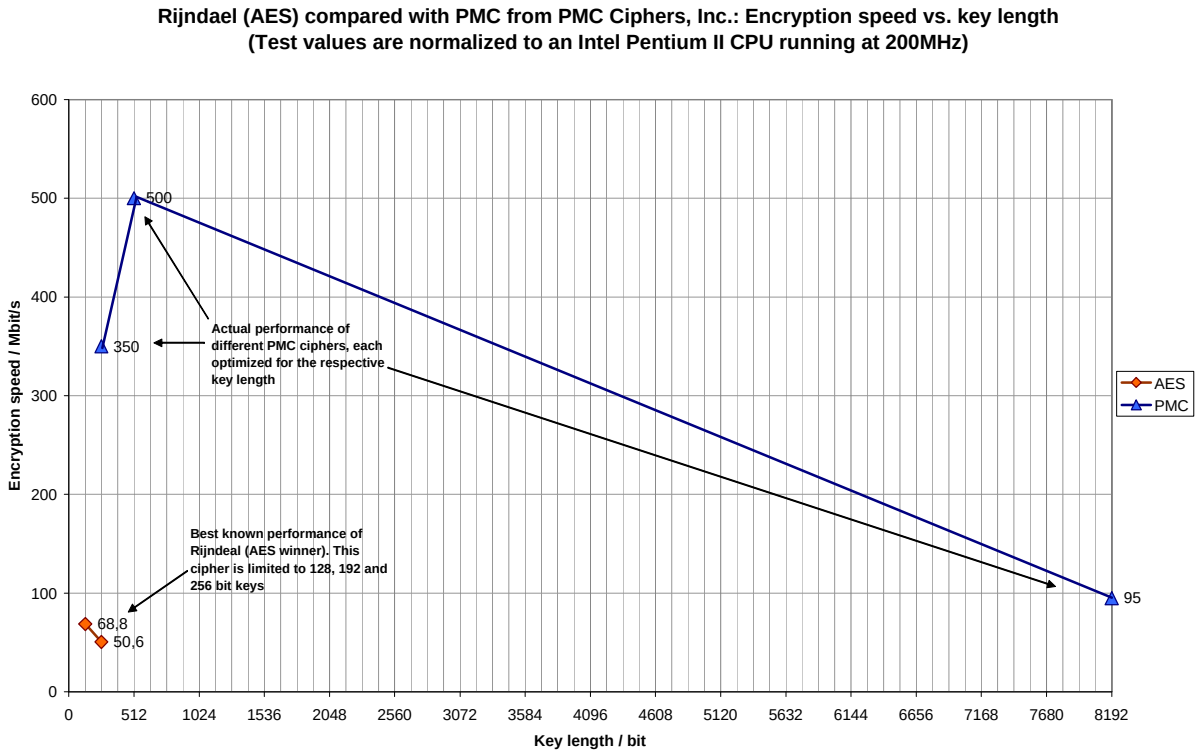

Fig. 3: Comparison of Two-stage PMC block ciphers with different key length and AES (Rijndael)