

PRP Modes Comparison

IEEE P1619.2

David McGrew
mcgrew@cisco.com

Acknowledgements

- Input and review from
 - Matt Ball
 - Shai Halevi
 - Landon Noll
 - Doug Whiting

Overview

- PRP definition
- Performance
- Security
- Properties
- References

(?) Denotes unverified data

PRP Modes

- All modes implement a tweakable pseudorandom permutation
- Inputs: secret key, plaintext, tweak
- Output: ciphertext
- Goal: *for any value of the tweak, the mode is indistinguishable from a random permutation to an attacker who doesn't know the key*

Cost of encrypting n AES blocks

	XCB	EME*	PEP†	HCTR	ABL4
#AES	$n+1$	$2n+1$	$n+5$	n	$2n$
#MUL	$2n$	0	$4n-6$	$2n (+2?)$	$2n$
Passes	2	2	3	2	3
Key Storage	1 AES, 1 hash, 48 bytes	3 AES	1 AES	2 AES, 2 hash	2 AES, 2 hash

† $\text{GF}(2^{128})$ multiplier *not* static, precomputation cannot be used

Software Summary

- XCB vs. EME*
 - XCB is faster if $\text{GF}(2^{128})$ multiply $< 1/2$ time for AES
 - Otherwise EME* is faster
- HCTR is essentially as fast as XCB
- ABL is always slower than XCB and EME*; it is never slower than half the speed of XCB
- PEP is always slower than XCB; on short messages, it may be slower than ABL (?)

Software Considerations

- $GF(2^{128})$ mult. has storage/speed tradeoff
 - 64kb per key: 1.6 times faster than AES-128* (2.3 times AES-256)
 - 8kb per key: as fast as AES-128*
- CTR mode can be faster than ECB
 - Upto 8% difference for AES-128
 - XCB, HCTR can use this benefit

*Tests on the x86 family, Brian Gladman.

Hardware Considerations

- Circuit size
 - $GF(2^{128})$ Multiplier $\sim 30\%$ AES-128
- Number of passes
 - Multiple passes avoid storing whole message at once

Security (assuming AES)

	XCB	EME*	PEP	HCTR	ABL4
Max number of bytes encrypted with a single key	$\sim 2^{68}$	$\sim 2^{68}$	$\sim 2^{68}$	$\sim 2^{47}$ (?)	$\sim 2^{68}$

Properties

	XCB	EME*	PEP	HCTR	ABL4
Bits in Plaintext	≥ 128	≥ 128	$m \times 128$ for $m \in \{1, 2, \dots\}$	≥ 128	≥ 256
Bits in Tweak	≥ 0	≥ 0	128	128	≥ 0
520 byte plaintexts	Yes	Yes	No	Yes	Yes
Encrypt / Decrypt with same circuit †	Yes	No	No	No	No
Patent Claims	Yes	Yes	No (?)	(?)	No

†Encryption equivalent to decryption with a reversed key schedule

References

- **XCB** - *The Extended Codebook (XCB) Mode of Operation*, McGrew & Fluhrer, <http://eprint.iacr.org/2004/278> & P1619 submission
- **EME*** - *EME*: extending EME to handle arbitrary-length messages with associated data*, Halevi, INDOCRYPT 2004, <http://eprint.iacr.org/2004/125>
- **PEP** - *A New Mode of Encryption Providing a Tweakeable Strong Decoude*