Comment for EAX' Cipher Mode:

"EAX' Cipher Mode (May 2011)" [1] specification shows algorithms and four test vectors of EAX' (EAX-prime) mode. This specification seems to be made as corrections of ANSI C12.22-2008 [2] Protocol Specification [a].

TOSHIBA found some correction were made, however, some serious problems still exist in the specification [1]. There is an inconsistency between algorithms and test vectors.

TOSHIBA assume,

1. Algorithms for EAX', such as CBC', CTR' and CMAC', are correct.
2. The test vectors in the specification [1] are wrong.

Main comment:

All the documents for AES(FIPS 197)[3], AES-CTR mode (NIST SP 800-38A)[4], and CMAC(NIST SP 800-38B)[5] are wrote under a rule that Leftmost Byte is the Most Significant Byte (MSB) without no exception.

On the other hand, there are at least two procedure errors in MAC generation process in the specification [1]. The first error exists in "dbl(X)" process. In this process, Rightmost Byte is treated as Most Significant Byte. This procedure error causes fault values of D and Q in "deriveKeyDependentConstants(K)" algorithm.

The second error exists in MAC value generation process. In the specification [1], the value of test vectors derived from T[12], T[13], T[14], T[15], even though the algorithm "EAX'.Encrypt_K(N,P)" specifies that "first 32bits" of Tag value should uses as MAC value. This error is also come from construe of MSB.

Modification method:

1. In all algorithms, including algorithm dbl(X), the Leftmost Byte must treat as Most Significant Byte. For example, in 16 byte array: a[0], a[1], …, a[15], a[0] is Most Significant Byte, and a[15] is Least Significant Byte.

---

[a] In the ANSI C12.22-2008 : some algorithms of EAX' are described in Annex I.1. The sample C code for EAX' is also included in Annex I.4 - "EAX' C code example (informative)". However, an inconsistency is exists between algorithms and the sample C code.

2. Generate MAC value T by following formula:

T[0] = N[0] xor T'[0]
T[1] = N[1] xor T'[1]
T[2] = N[2] xor T'[2]
T[3] = N[3] xor T'[3].

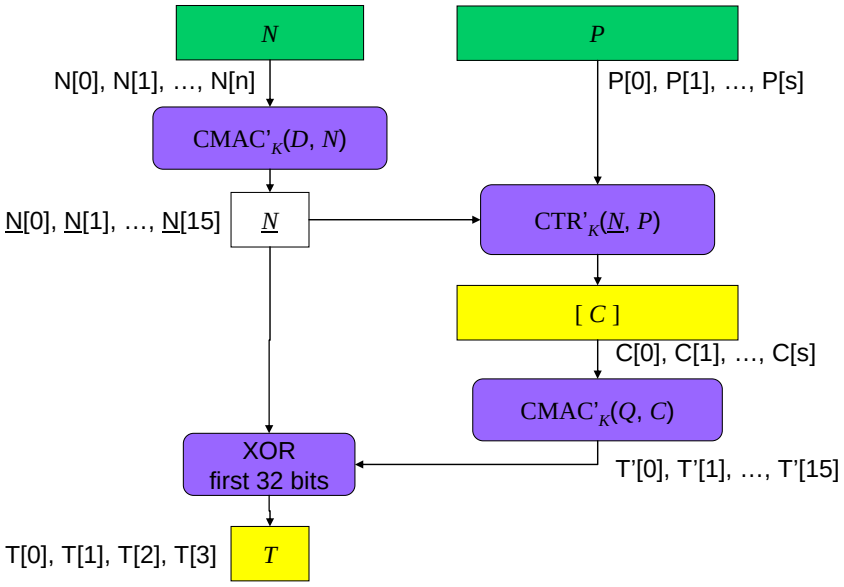

Figure : Encryption algorithm when confidentiality is selected

Test Vectors:

A. Test Vector 1

1) Inputs:

Key: (K[0], K[1], …., K[15])

01 02 03 04 05 06 07 08 01 02 03 04 05 06 07 08

Plaintext : (N[0], N[1], …, N[67])

a2 0c 06 0a 60 7c 86 f7 54 01 16 00 17 02 a7 03
02 01 04 a8 03 02 01 02 ac 0f a2 0d a0 0b a1 09
80 01 02 81 04 48 e9 93 88 be 19 28 17 81 15 9a
a6 0d 06 0b 60 7c 86 f7 54 01 16 00 17 82 11 02
48 e9 93 88

Cleartext: (P[0], P[1], …, P[15])

54 45 4d 50 0b 40 00 07 00 05 1a 00 00 02 00 e4

2) Intermediate results:

D: (D[0], D[1], …, D[15])

87 3d 27 b1 9c 89 7d ed 55 be 52 b3 fa 0c db f7

Q: (Q[0], Q[1], …, Q[15])

0e 7a 4f 63 39 12 fb da ab 7c a5 67 f4 19 b7 69

N: (N[0], N[1], …, N[15])

2e 3e bf 71 07 dd 7c f0 c7 57 21 03 6a a9 5f 19

T': (T'[0], T'[1], …, T'[15])

77 a7 4c 29 2b e7 4c 53 44 05 df 68 8f 8d e0 82

3) Outputs:

Ciphertext: (C[0], C[1], …, C[15])

fb 93 00 01 18 42 1d 30 58 80 0d c9 6f c9 82 69

MAC: (T[0], T[1], T[2], T[3])

59 99 f3 58

B. Test Vector 2

1) Inputs:

Key: (K[0], K[1], …., K[15])

01 02 03 04 05 06 07 08 01 02 03 04 05 06 07 08

Plaintext : (N[0], N[1], …, N[67])

a2 0c 06 0a 60 7c 86 f7 54 01 16 00 7b 02 a7 03

02 01 04 a8 03 02 01 02 ac 0f a2 0d a0 0b a1 09

80 01 02 81 04 48 f3 d2 f8 be 19 28 17 81 15 9a

a6 0d 06 0b 60 7c 86 f7 54 01 16 00 7b 82 11 02

48 f3 d2 f8

Cleartext: (P[0], P[1], …, P[15])

54 45 4d 50 0b 40 00 07 00 05 1a 00 00 02 00 e4

2) Intermediate results:

D: (D[0], D[1], …, D[15])

87 3d 27 b1 9c 89 7d ed 55 be 52 b3 fa 0c db f7

Q: (Q[0], Q[1], …, Q[15])

0e 7a 4f 63 39 12 fb da ab 7c a5 67 f4 19 b7 69

N: (N[0], N[1], …, N[15])

cc 58 80 03 17 13 c3 88 ff 33 3f de 67 82 19 0a

T': (T'[0], T'[1], …, T'[15])

e6 d5 d6 b4 54 86 44 ea db c3 b9 04 1a d9 44 1f

3) Outputs:

Ciphertext: (C[0], C[1], …, C[15])

82 ba ff f2 c1 ae ee 15 ac ad ae 0b 72 bf ab cf

MAC: (T[0], T[1], T[2], T[3])

2a 8d 56 b7

C. Test Vector 3

1) Inputs:

Key: (K[0], K[1], …., K[15])

10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0 00

Plaintext : (N[0], N[1], …, N[64])

a2 0e 06 0c 60 86 48 01 86 fc 2f 81 1c aa 4e 01
a8 06 02 04 39 a0 0e bb ac 0f a2 0d a0 0b a1 09
80 01 00 81 04 4b ce e2 c3 be 25 28 23 81 21 88
a6 0a 06 08 2b 06 01 04 01 82 85 63 00 4b ce e2
c3

Cleartext: (P[0], P[1], …, P[27])

17 51 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 00 00 03 30 00 01

2) Intermediate results:

D: (D[0], D[1], …, D[15])

15 c8 8e 3a 97 5c e2 0b 25 9c 1d 2e b4 bc 38 3a

Q: (Q[0], Q[1], …, Q[15])

2b 91 1c 75 2e b9 c4 16 4b 38 3a 5d 69 78 70 74

N: (N[0], N[1], …, N[15])

ac a6 ae de 3a a4 b0 5b 2f 1b 78 09 10 10 c2 76

T': (T'[0], T'[1], …, T'[15])

e7 c0 41 5b c3 fa 4e f5 78 59 06 58 20 C3 4e 3d

3) Outputs:

Ciphertext: (C[0], C[1], …, C[27])

d3 34 3d 8a f1 e1 70 ed c5 11 06 0a 9e 1f 4c aa

17 8b 4e 3f be 21 d8 36 04 07 4b 2f

MAC: (T[0], T[1], T[2], T[3])

4b 66 ef 85

D. Test Vector 4

1) Inputs:

Key: (K[0], K[1], …., K[15])

66 24 c7 e2 30 34 e4 03 6f e5 cb 3a 8b 5d ab 44

Plaintext : (N[0], N[1], …, N[66])

a2 11 06 0f 2b 06 01 04 01 82 85 63 8e 7f 85 f1

c2 4e 01 a8 06 02 04 2b c8 1a a1 ac 0f a2 0d a0

0b a1 09 80 01 00 81 04 4b 97 d2 cc be 39 28 37

81 35 88 a6 09 06 07 2b 06 01 04 82 85 63 00 4b

97 d2 cc

Cleartext: (P[0], P[1], …, P[47])

17 51 30 30 30 30 30 30 30 30 30 30 30 30 30 30

30 30 30 30 30 30 00 00 03 30 00 01 03 30 00 78

03 30 00 79 03 30 00 7a 03 30 00 7b 03 30 00 7d

2) Intermediate results:

D: (D[0], D[1], …, D[15])

d1 83 32 b9 83 5d 5c ab 95 1d c2 70 7a 6f 68 11

Q: (Q[0], Q[1], …, Q[15])

a3 06 65 73 06 ba b9 57 2a 3b 84 e0 f4 de d0 a5

N: (N[0], N[1], …, N[15])

3c 2b 23 5e 5b 2a d3 8a 89 f9 c7 41 e5 a5 4c d4

T': (T'[0], T'[1], …, T'[15])

eb a9 53 5f d6 56 60 1c 71 8c 8a bb 26 92 82 95

3) Outputs:

Ciphertext: (C[0], C[1], …, C[47])

a8 2c 8d 5b cc 7d 7b f3 1f e4 fa 92 e0 5b a5 B5

54 d5 c8 96 79 5a e0 3b db 65 08 dd d5 d3 c8 32
e4 3d 07 a1 b2 cf 3d cf 2d 42 e5 24 ea 9a 01 c0

MAC: (T[0], T[1], T[2], T[3])

d7 82 70 01

References:

[1] "EAX' Cipher Mode (May 2011)", available from http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/eax-prime/eax-prime-spec.pdf

[2] "American National Standard Protocol Specification For Interfacing to Data Communication Networks", ANSI C12.22-2008 / IEEE P1703 / MC1222: Annex I, "EAX' description"

[3] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS Publication 197, available from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] National Institute of Standards and Technology (NIST), Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38A, available from http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[5] National Institute of Standards and Technology (NIST), Cipher-based Message Authentication Code (CMAC), NIST Special Publication 800-38B, available from http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf