Implementing AES-GCM

Lab#8 Report

Pratheep Joe Siluvai (pi4810)
CMPE.661 HW SW Co-design for Crypto Apps
May 6, 2014

Instructors: Kurdziel, Michael & Lukowiak, Marcin
T.A: Skalicky, Sam

Introduction

This lab was to develop software that implements the Galois Counter Mode of Advanced Encryption Standard with 126 bit key and verify it with a set of predefined test vectors.

Procedure

1. Wrote a software that implements GF (2^128) with the following irreducible polynomial f(x) = x^128 + x^7 + x^2 + x +1.
2. Then used the baseline AES software and the multiplier that was developed to implement the simplified version of the AES GCM.
3. The Galois Counter mode was implemented by converting all the plain text, key and initialization vectors into an array of bytes into 2D blocks.
4. Then the encryption was done along with the counter mode operation, authentication and multiplication as specified in the figure.

Below are the matching results that we got for test case 3 & 4.

Results and Observations:

1. Test Case 3:

```
Val of X1 = 0 0 0 0
Val of X2 = 0 0 0 0
E(K, Y0)
   W0  W1  W2  W3
   32  3c  4d  87
   47  4f  bc  bb
   18  69  d2  b4
   4b  a4  28  18
E(K, Y1)
   W0  W1  W2  W3
   9b  d9  ee  2b
   b2  f3  2b  25
   2c  72  28  f2
   e7  c1  72  06
E(K, Y2)
   W0  W1  W2  W3
   65  39  1b  a3
   0d  36  8d  9d
   88  53  4e  2b
   7c  3a  1e  5c
E(K, Y3)
   W0  W1  W2  W3
   3d  c1  52  e5
   e9  0e  40  22
   18  9a  64  1f
```

```
   27  4f  7e  20
E(K, Y4)
   W0  W1  W2  W3
   aa  c0  87  5d
   c9  07  3b  90
   e6  4a  9b  8b
   cc  c0  a8  d0
Ciphertext1
   W0  W1  W2  W3
   42  21  4b  84
   83  77  72  d0
   1e  74  21  d4
   c2  24  b7  9c
Ciphertext2
   W0  W1  W2  W3
   e3  2c  35  29
   aa  02  c1  ac
   21  a4  7e  a1
   2f  e0  23  2e
Ciphertext3
   W0  W1  W2  W3
   21  54  7d  ac
   d5  66  8f  84
   14  93  6a  aa
   b2  1c  5a  05
Ciphertext4
   W0  W1  W2  W3
   1b  6a  3d  47
   a3  0a  58  3f
   0b  ac  e0  59
   39  97  91  85
Val of X3 = 59ed3f2b b1a0aaa0 7c9f56c6 a504647b
Val of X4= b714c904 8389afd9 f9bc5c1d 4378e052
Val of X5= 47400c65 77b1ee8d 8f40b272 1e86ff10
Val of X6= 4796cf49 464704b5 dd91f159 bb1b7f95
Val of GHASH= 7f1b32b8 1b820d02 614f8895 ac1d4eac
Val of Tag= 4d5c2af3 27cd64a6 2cf35abd 2ba6fab4
```

2. Test Case 4:

Val of X1 = ed56aaf8 a72d6704 9fdb9228 edba1322

Val of X2 = cd47221c cef0554e e4bb044c 88150352

E(K, Y0)

W0	W1	W2	W3
32	3c	4d	87
47	4f	bc	bb
18	69	d2	b4
4b	a4	28	18

E(K, Y1)

W0	W1	W2	W3
9b	d9	ee	2b
b2	f3	2b	25
2c	72	28	f2
e7	c1	72	06

E(K, Y2)

W0	W1	W2	W3
65	39	1b	a3
0d	36	8d	9d
88	53	4e	2b
7c	3a	1e	5c

E(K, Y3)

W0	W1	W2	W3
3d	c1	52	e5
e9	0e	40	22
18	9a	64	1f
27	4f	7e	20

E(K, Y4)

W0	W1	W2	W3
aa	c0	87	5d
c9	07	3b	90
e6	4a	9b	8b
cc	c0	a8	d0

Ciphertext1

W0	W1	W2	W3
42	21	4b	84
83	77	72	d0
1e	74	21	d4
c2	24	b7	9c

Ciphertext2

W0	W1	W2	W3
e3	2c	35	29
aa	02	c1	ac
21	a4	7e	a1
2f	e0	23	2e

Ciphertext3

W0	W1	W2	W3
21	54	7d	ac
d5	66	8f	84
14	93	6a	aa
b2	1c	5a	05

Ciphertext4

W0	W1	W2	W3
1b	6a	3d	00
a3	0a	58	00
0b	ac	e0	00
39	97	91	00

Val of X3 = 54f5e1b2 b5a8f952 5c239247 51a3ca51

Val of X4= 324f585c 6ffc1359 ab371565 d6c45f93

Val of X5= ca7dd446 af4aa70c c3c0cd5a bba6aa1c

Val of X6= 1590df9b 2eb67682 89e57d56 274c8570

Val of GHASH= 698e57f7 e6ecc7f d9463b72 60a9ae5f

Val of Tag= 5bc94fbc 3221a5db 94fae95a e7121a47