國立成功大學 電機工程學系

畢業專題實作成果報告書

AES-128 架構設計與優化

AES-128 Architecture Design and Improvement

專題組別：☑電路與系統 □電子與材料 □電腦與通訊

指導教授： 謝明得 教授

組員學號&姓名： E24086030 郭冠緯

E14071025 趙泓瑞

研究期間: 2022 年 3 月 至 2022 年 11 月底止,計 9 個月

摘要

詳閱 AES 相關論文，用 verilog 實踐 AES-128 演算法內容，必且針對 sub_byte()與 mix_column()功能優化，用 tsmc90 合成得到電路面積有幅度的減小。以我們所能實現低面積架構與管線化架構，面積為 5.62 倍。

關鍵字 Aes128 優化 加速

Abstract

Reading AES-related papers in detail, we use verilog to practice AES-128 algorithm into circuit, optimize the functions of sub_byte() and mix_column() as we can , and use tsmc90 to synthesize to obtain a significant reduction in circuit area. With the low-area architecture and pipeline architecture that we have achieved, the longest path is reduced by less than one tenth of the original, and the area is 5.62 times.

Keyword Aes128 Improvement Acceleration

目錄

一、 前言

本專題報告以 AES-128 加密系統的 verilog 實作主體，並且將系統優化與加速，並比較優化前後的差異。內容從 AES 的學術定義、詳細演算法流程至 AES 硬體系統優化的三大辦法文獻研討，從函數、架構和硬體層面都有包含，並嘗試以優化後的架構為出發點，並嘗試以過往的論文所學提升架構單位時間的工作量。

二、原理分析與系統設計

2.1 原理分析

AES 的資料區塊長度固定是 128 位元，金鑰的位元長度則可以是三種，分別為 128、192 和 256 位元。演算法進行不相同次數的加密與解 密，不同的轉換對中途結果進行操作，稱之為狀態(state)。狀態可以用長行陣列表示，特別在於陣列的「列」表敘固定為四列，則行數用 Nb 表示，等於資料區塊長度除以 32。（但因為 AES 的資料區塊長度固定，Nb 也就固定為 4。）參考[1]。

金鑰的描述也類似於 AES 的資料區塊，一樣長行陣列的「列」描述固定為四列，行數我們以 Nk 表示，等同於金鑰長度除以 32，不過不論是 AES 或是 Rijndael 加密法，金鑰的長度也有三種長度(128、192 或 256)，所以 Nk 可能為 4、6 或 8。

	明文(bits)	金鑰(bits)	Nb	Nk	Nr=6+max(Nb,Nk)
AES128	128	128	4	4	10
AES192	128	192	4	6	12
AES256	128	256	4	8	14

表: 金鑰不同長度對 AES 演算法的 Nr 影響

針對我們所作的 AES-128 的主題，我們的金鑰的位元長度為 128 bits，用 key 做 10 次 key expansion，產生 10 個 round key 用於加密。

```
KeyExpansion(byte Key[4*Nk] word W[Nb*(Nr+1)])
{
      for(i = 0; i < Nk; i++)
            W[i] = (Key[4*i],Key[4*i+1],Key[4*i+2],Key[4*i+3]);

      for(i = Nk; i < Nb * (Nr + 1); i++)
      {
            temp = W[i - 1];
            if (i % Nk == 0)
                  temp = SubByte(RotByte(temp)) ^ Rcon[i / Nk];
            W[i] = W[i - Nk] ^ temp;
      }
}
```

以上為 AES-128 key expansion 的演算法。

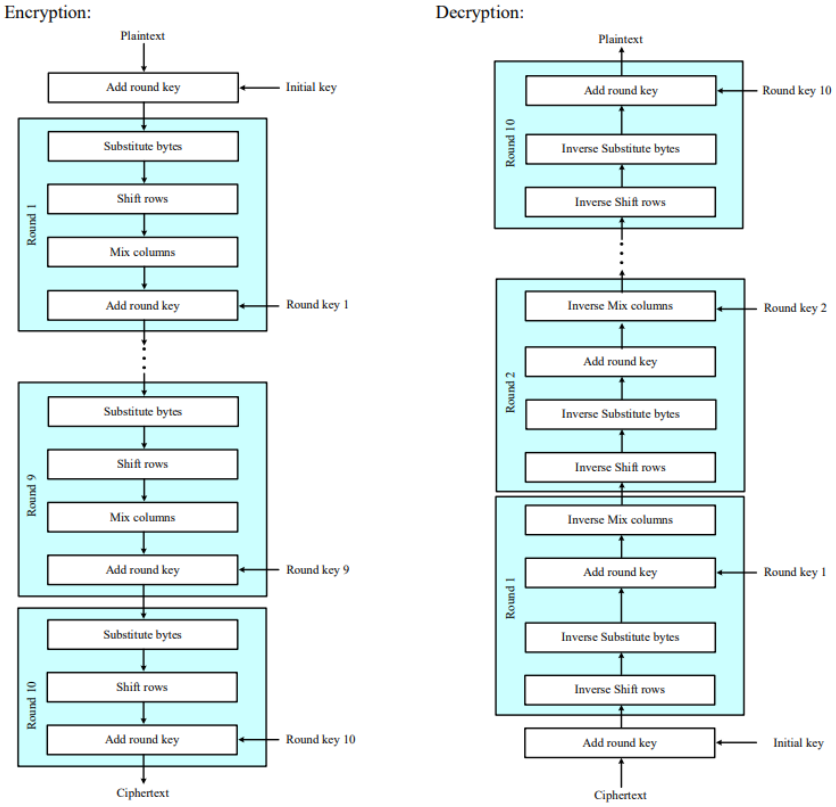


圖 1-1 AES128 演算法總流程圖

如果我們用 pseudo code 表達整體演算法的所需的函數為:

```
Round(State,RoundKey)
{
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,RoundKey);
}

FinalRound(State,RoundKey)
{
ByteSub(State) ;
ShiftRow(State) ;
AddRoundKey(State,RoundKey);
}
```

從比較中發現，Round 跟 Final_Round 的差別為 Mix_Column 子函數被移除。子函數功能分別討論。

ByteSub( )是將明文透過 Substitution Table (or S-box)查表替換，Substitution Table 是經過可逆性替換運算(找出 Galois Field 的乘法反元素，再由 Affine transformation)整理得到，有可逆性和一對一的特徵。

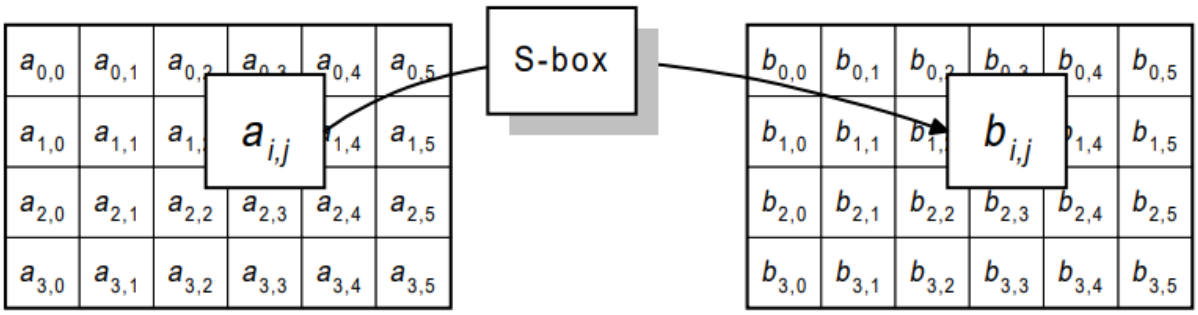


圖 1-2 ByteSub( )對每一 byte 的替換經過

Inverse_ByteSub( )使用 Affine transformation 的逆運算表對密文做替換運算，最後找出 GF(2^8) 的乘法反元素。

- 詳細 ByteSub( )參考[2]的詳細原理，將一個 byte 的資料(暫時稱呼為 a)做 mapping 運算後產生$a_h x + a_l$，乘法的 inverse 後得(a_h ・ d)x + ($a_h \oplus a_l$)・d。其中 d = ((a_h^2・{e})⊕(a_h・a_l) ⊕ a_l^2)^-1。最後做 mapping inverse 及 affine 即對 a 完成 ByteSub( )的運算。

ShiftRow( )以密文的每 4 個 bytes 為一列，則第 x 列向左位移 x 位，所以舉例來說第 0 列不移動，而第 1 列向左位移 1 位。

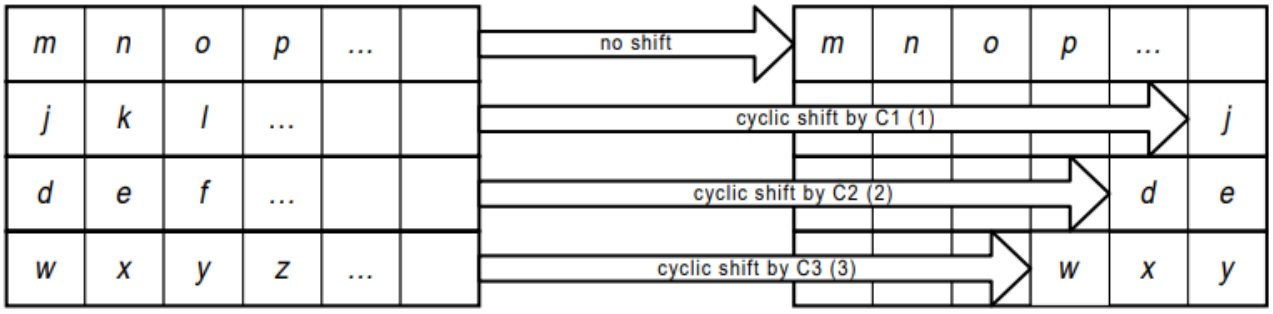


圖 1-3 ShiftRow( )對列的轉換過程

Inverse_ShiftRows( )則以密文每 4 個 bytes 為一列，第 x 列向右位移 x 位，例如第 3 列向右位移 3 位，位置的數學運算公式為(j+Nb-x)。

在 AES 中，因資料長度固定，所以 **ShiftRow ()**和 **Inverse_ShiftRows()**運算為上述規則，在 Rijndael 加密法中若為 256bits，則不適用。

Mix_column( ) 將狀態的直行視作 GF(2^8)多項式，並且對 x+1 的固定多項式做 Inverse_ShiftRows( )運算後的矩陣，將密文每單一行乘以一個那固定矩陣的過程稱為 Mix column。

Inverse_MixColumn( )將密文每單一行乘以另一固定矩陣。

若使用脈動陣列於實現 mix column 的架構和 AES 分組密碼算法的

Inverse_MixColumn。使用 mix column 的脈動方法提供更好的更好的 through- put 實現，所以若嘗試使用脈動陣列，可以對 AES 的演算法 MixColumn()加速。

AddRoundKey( ) 通過 XOR 按位置運算後，從金鑰中導出 Round Key，則 Round Key 長度等同於資料區塊行數 Nb。此函數也一樣具有可逆性。

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$

$\oplus$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$

=

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$	$b_{0,4}$	$b_{0,5}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	$b_{1,4}$	$b_{1,5}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$	$b_{2,4}$	$b_{2,5}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$	$b_{3,4}$	$b_{3,5}$

針對每一個 function 的優化方案: (以下將相同性質的運算一同討論

ShiftRow( )與 Inverse_ShiftRows( ) 用邏輯電路的接線的方式處理。

Mix_column( )與 Inverse_MixColumn( ) 如果是乘以二的項，採用接線處理，向左位移一個位元。如果是乘以三的項，採用接線與一個加法器處理，向左位移一個位元並加一，取代原本使用選擇器做出來的結果，實現硬體上的面積減小。

ByteSub( ) 實現[2]提供的硬體架構，取代原本使用選擇器做出來的結果，實現硬體上的面積減小即可以管線化的其他優化。

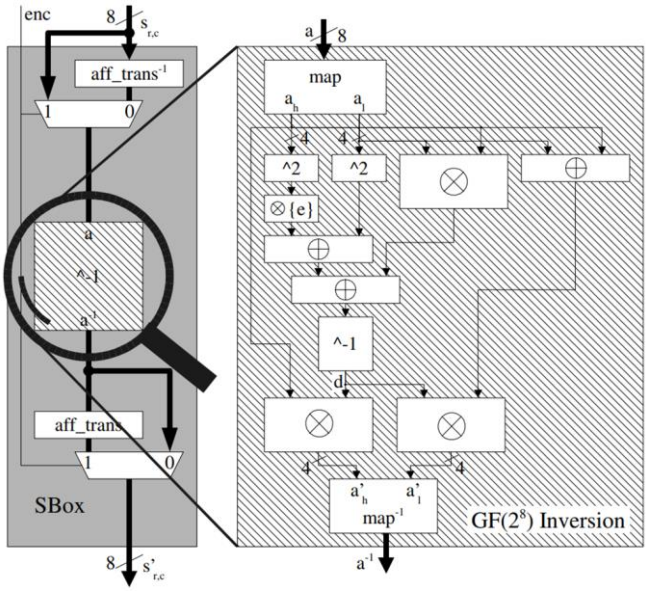


圖 1-4 參考[2] ByteSub( )設計架構圖

2.2 系統設計

以實踐 AES-128 處理器電路為首要目標，針對每一個功能做優化，以我們所能做到最低面積的硬體設計。並且參考[3]管線化系統設計，在每一個 round 中間

插入暫存器(10 stage)，實踐兩種系統。

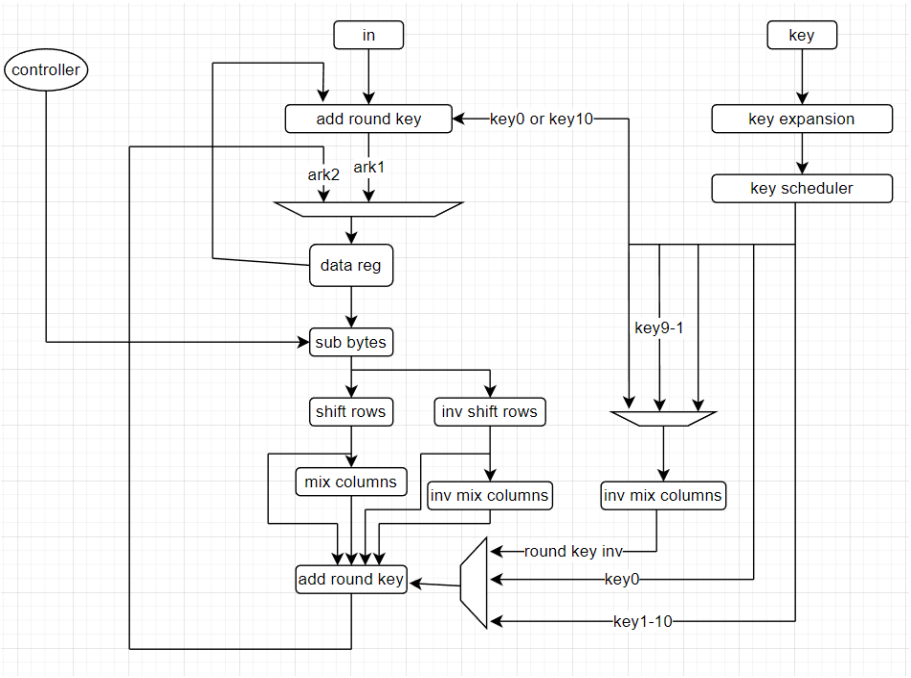


圖 2-1 低面積 AES-128 硬體架構

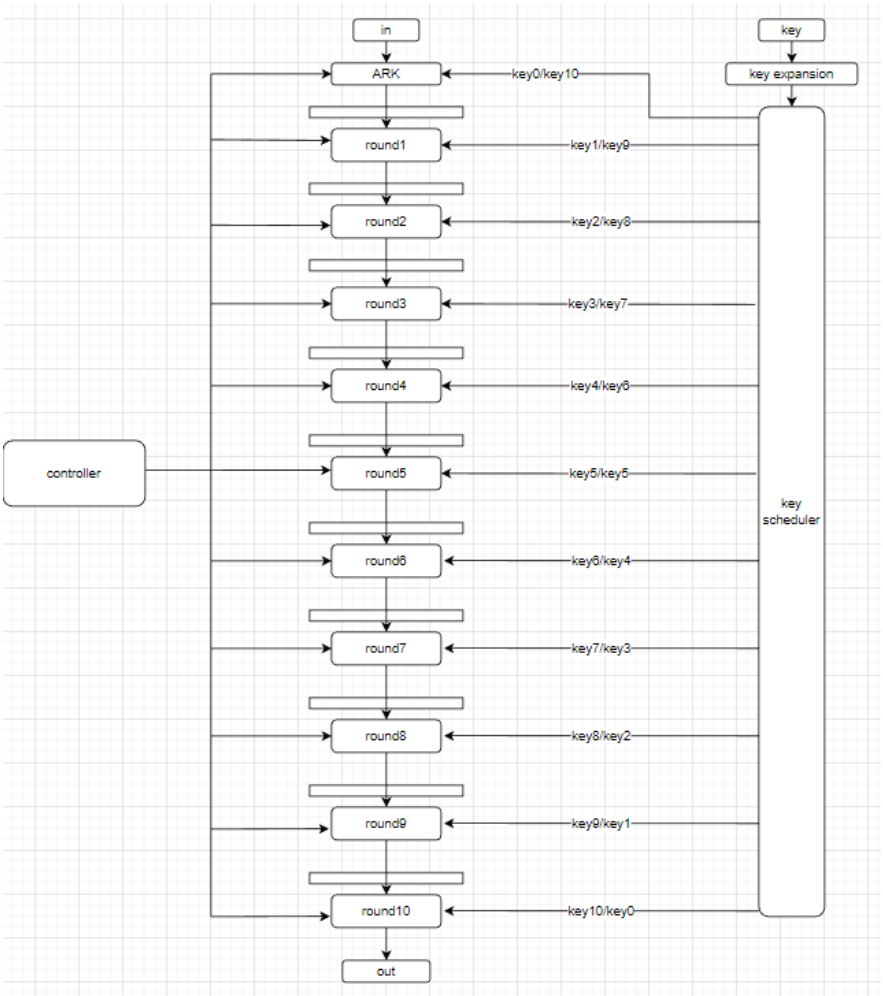


圖 2-2 管線化 AES-128 硬體架構

state	de/en	key
0	rst	key0
1 2 … 9 10	en	key1 key2 … key9 key10
11		key10
12 13 … 20 21	de	key9 key8 … key1 key0
22	store	x

表 2-1 兩架構 Finite State Machine

Signal name	I/O	Width	Description
clk	I	1	時脈訊號。
rst	I	1	高準位非同步重置訊號。
in	I	128	明文資料內容。
key	I	128	加密金鑰。
sel	I	1	運作模式控制訊號。若 High，則為解密模式; 若 low，則為加密模式。
state	O	6	有限狀態機。
out	O	128	暗文資料內容。

表 2-2　I/O specification

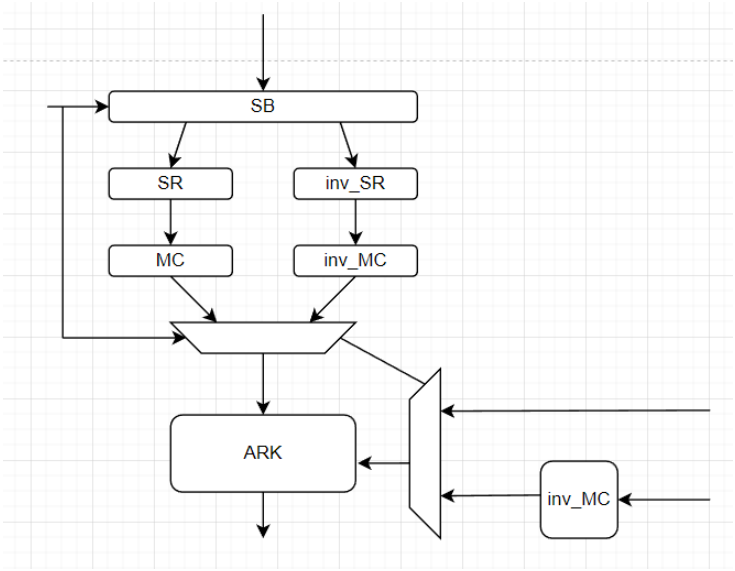


圖 2-3 管線化 AES-128 round 1~9 架構細節

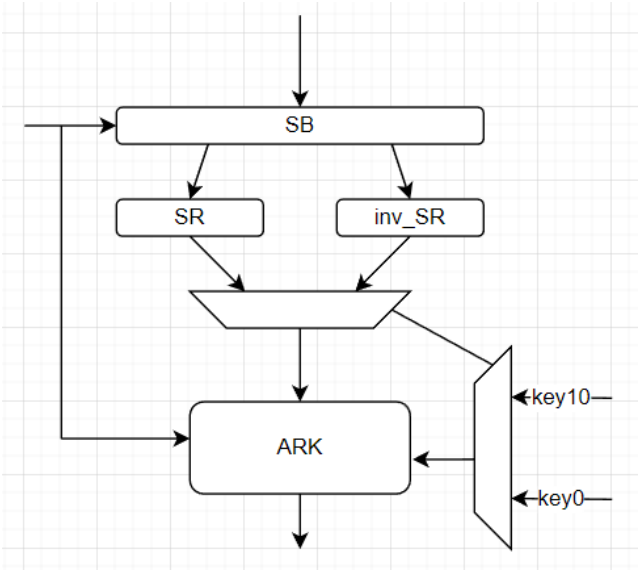
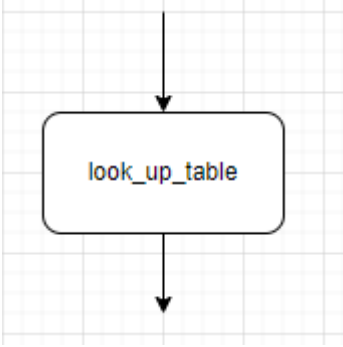


圖 2-3 管線化 AES-128 round 0、10 架構細節

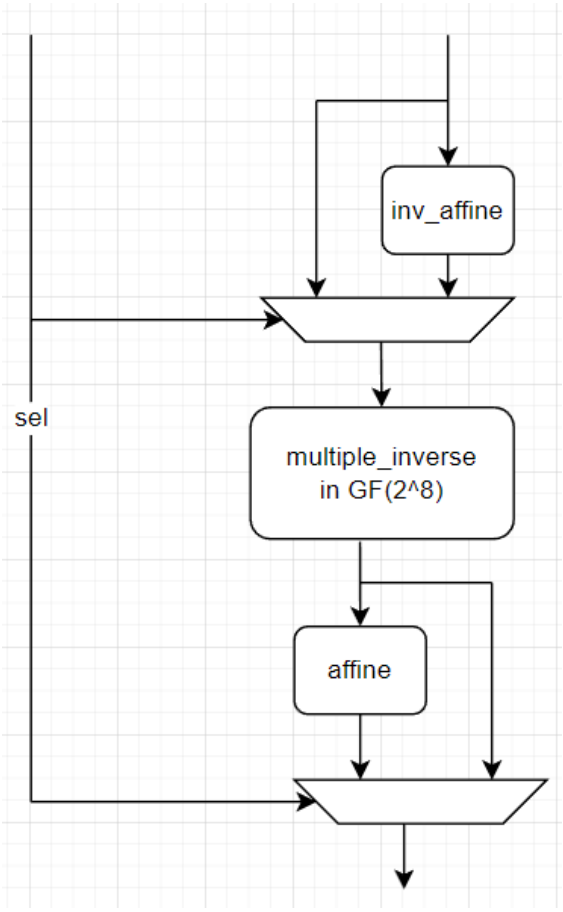
[註] : ARK→Add Round Key SB→ Byte Sub

SR→Shift Row MC→Mix Column

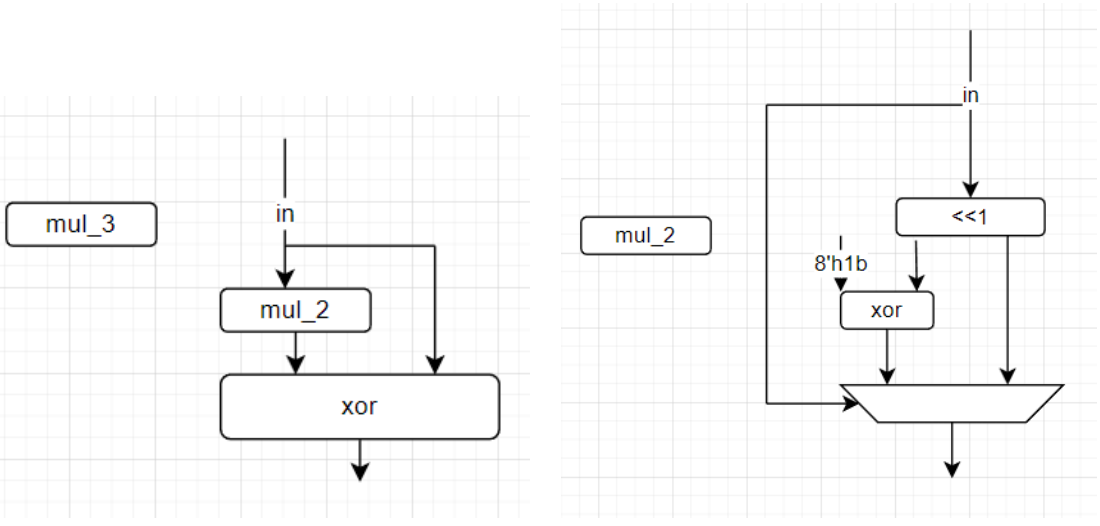
原本 AES-128 的 Byte Sub()跟 Mix Column()的架構採用 lookuptable 設計:



優化後: Byte Sub()架構



優化後: Mix Column ()架構



三、實驗結果

我們以 verilog 語言設計一個包含加解密功能的 AES-128 處理器電路，兩架構對同一組 128 資料加解密的成果:

```
  4 in=1212aeae1212aeae8888888888888888, out=00000000000000000000000000000000, state= 0, sel=0(0->encrypt, 1->decrypt)
  5 in=1212aeae1212aeae8888888888888888, out=396cbbb83abc7c08237f9d008147c7b4, state= 1, sel=0(0->encrypt, 1->decrypt)
  7 in=1212aeae1212aeae8888888888888888, out=1b74e8ccdebf0e72de648693b943fa91, state= 2, sel=0(0->encrypt, 1->decrypt)
  9 in=1212aeae1212aeae8888888888888888, out=7b055c4d015ee772b387eafbe266480d, state= 3, sel=0(0->encrypt, 1->decrypt)
 11 in=1212aeae1212aeae8888888888888888, out=be9b453d24cd123edbdd670e92f98365, state= 4, sel=0(0->encrypt, 1->decrypt)
 13 in=1212aeae1212aeae8888888888888888, out=c74c2fd7fb773c9213ea746d734b831d, state= 5, sel=0(0->encrypt, 1->decrypt)
 15 in=1212aeae1212aeae8888888888888888, out=b3379643f1234be849fdbd44166f4c71, state= 6, sel=0(0->encrypt, 1->decrypt)
 17 in=1212aeae1212aeae8888888888888888, out=67ebb6c0e90646e851b71264b222c365, state= 7, sel=0(0->encrypt, 1->decrypt)
 19 in=1212aeae1212aeae8888888888888888, out=20abefa48ddfb14e9c2faf042e682c7f, state= 8, sel=0(0->encrypt, 1->decrypt)
 21 in=1212aeae1212aeae8888888888888888, out=ef27ba68f98e216df4861b8f80c30732, state= 9, sel=0(0->encrypt, 1->decrypt)
 23 in=1212aeae1212aeae8888888888888888, out=cbcfe7f0e2b4decf0d9039ba21989204, state=10, sel=0(0->encrypt, 1->decrypt)
 25 in=1212aeae1212aeae8888888888888888, out=4874b6241ea8b1031cb5113ca9ee1e54, state=11, sel=0(0->encrypt, 1->decrypt)
 27 in=1212aeae1212aeae8888888888888888, out=98604f8cd746948afd8a1df41f8d12f2, state=12, sel=1(0->encrypt, 1->decrypt)
 29 in=1212aeae1212aeae8888888888888888, out=9944c545bf2ef43ccdccfd73df19af23, state=13, sel=1(0->encrypt, 1->decrypt)
 31 in=1212aeae1212aeae8888888888888888, out=5d157149de45df2f3162c8f2b79e79d2, state=14, sel=1(0->encrypt, 1->decrypt)
 33 in=1212aeae1212aeae8888888888888888, out=1ea92ebad1934e9b37e95a43856fc94d, state=15, sel=1(0->encrypt, 1->decrypt)
 35 in=1212aeae1212aeae8888888888888888, out=a154291a3ba8909b479ab31b6d267aa3, state=16, sel=1(0->encrypt, 1->decrypt)
 37 in=1212aeae1212aeae8888888888888888, out=0f87ec0e7db3154f8f29eb3cc6f592a4, state=17, sel=1(0->encrypt, 1->decrypt)
 39 in=1212aeae1212aeae8888888888888888, out=36c1ec27b9996eb24f14c9abaebd854d, state=18, sel=1(0->encrypt, 1->decrypt)
 41 in=1212aeae1212aeae8888888888888888, out=7c1752e36d334a40986b940f215887d7, state=19, sel=1(0->encrypt, 1->decrypt)
 43 in=1212aeae1212aeae8888888888888888, out=1d432d4b1d1a9b405692abdcaf084481, state=20, sel=1(0->encrypt, 1->decrypt)
 45 in=1212aeae1212aeae8888888888888888, out=80d2c66c26a0ea300c50106312655e8d, state=21, sel=1(0->encrypt, 1->decrypt)
 47 in=1212aeae1212aeae8888888888888888, out=1212aeae1212aeae8888888888888888, state=22, sel=1(0->encrypt, 1->decrypt)
```

管線化架構 presim 結果:

```
  4 out=b3779acbaa8d46ea825c6fabd5006fc5, sel=0
  5 out=0a2302c87a9b4ea5f9c5045b3c8dda71, sel=0
  7 out=bc764437e84e714f990b1dadd4a1980b, sel=0
  9 out=b77a50ff549d4cc2fca27d87cd927642, sel=0
 11 out=71889e0b9a2d1204003250a512666283, sel=0
 13 out=13d8fc1a453a4bd7c99b4a50a56eaf29, sel=0
 15 out=6aacd9f28a430b07c7d26b291a456456, sel=0
 17 out=c33b4a28d225de8298c2d89feb40f91a, sel=0
 19 out=dd1899a5d2eb8c560d60ff740134a594, sel=0
 21 out=692518293a34e431ce5600943c993a9c, sel=0
 23 out=471667611c17e6379be53e30f5ef5cdd, sel=0
 25 out=7206720946c642f34a3f00ccfb373457, sel=0
 27 out=4874b6241ea8b1031cb5113ca9ee1e54, sel=0
108 out=50e88901714c89f990a86148fa09ff0c, sel=1
109 out=c529c8eb3d18e63589befcea06972eec, sel=1
111 out=0b49535505edc274182911209a2b58aa, sel=1
113 out=a825e2d6e0f5357d00861231c90a52d2, sel=1
115 out=0e092f5109ca8f65f211b06b7de3b98a, sel=1
117 out=7c45b00996c459b4a6937563a3954d43, sel=1
119 out=2f2a5e6aae171ea372949635fa58518e, sel=1
121 out=5913317e429793787afeaad6b3c8030a, sel=1
123 out=46cc4d748dd5c28b3f94801a0878870f, sel=1
125 out=c3a575e48a2e2c0677b33092bc5fbeeb, sel=1
127 out=128128aefaef128aef12855555555555, sel=1
129 out=6bc1bee22e409f96e93d7e117393172a, sel=1
131 out=1212aeae1212aeae8888888888888888, sel=1
```

我們採用 tsmc90 製成，合成結果:

Mc1:

```
****************************************
Report : area
Design : mix_columns
Version: R-2020.09
Date   : Tue Nov 29 15:38:34 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUTI

Number of ports:                          256
Number of nets:                          4280
Number of cells:                         4152
Number of combinational cells:           4152
Number of sequential cells:                 0
Number of macros/black boxes:               0
Number of buf/inv:                        697
Number of references:                     105

Combinational area:              15343.272449
Buf/Inv area:                     1478.937649
Noncombinational area:               0.000000
Macro/Black Box area:                0.000000
Net Interconnect area:          491775.798889

Total cell area:                 15343.272449
Total area:                     507119.071338
1
```

Inv_Mc1:

```
****************************************
Report : area
Design : inv_mix_columns
Version: R-2020.09
Date   : Tue Nov 29 15:43:04 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GU

Number of ports:                          256
Number of nets:                         19026
Number of cells:                        18898
Number of combinational cells:          18898
Number of sequential cells:                 0
Number of macros/black boxes:               0
Number of buf/inv:                       2565
Number of references:                     142

Combinational area:              70912.801812
Buf/Inv area:                     5558.011383
Noncombinational area:               0.000000
Macro/Black Box area:                0.000000
Net Interconnect area:         2404745.324829

Total cell area:                 70912.801812
Total area:                    2475658.126641
1
```

Mc2:

```
****************************************
Report : area
Design : mix_columns
Version: R-2020.09
Date   : Tue Nov 29 15:54:05 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUTM

Number of ports:                          256
Number of nets:                          3326
Number of cells:                         3198
Number of combinational cells:           3198
Number of sequential cells:                 0
Number of macros/black boxes:               0
Number of buf/inv:                        524
Number of references:                     117

Combinational area:              12249.921956
Buf/Inv area:                     1114.142437
Noncombinational area:               0.000000
Macro/Black Box area:                0.000000
Net Interconnect area:          379961.905121

Total cell area:                 12249.921956
Total area:                     392211.827076
1
```

InvMc2:

```
****************************************
Report : area
Design : inv_mix_columns
Version: R-2020.09
Date   : Tue Nov 29 15:50:40 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUT

Number of ports:                          256
Number of nets:                         18664
Number of cells:                        18536
Number of combinational cells:          18536
Number of sequential cells:                 0
Number of macros/black boxes:               0
Number of buf/inv:                       2566
Number of references:                     140

Combinational area:              70350.438545
Buf/Inv area:                     5579.884984
Noncombinational area:               0.000000
Macro/Black Box area:                0.000000
Net Interconnect area:         2376605.183960

Total cell area:                 70350.438545
Total area:                    2446955.622505
1
```

Sbox1:

```
Report : area
Design : sbox
Version: R-2020.09
Date   : Tue Nov 29 15:34:18 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUTM_Arr

Number of ports:                          113
Number of nets:                           436
Number of cells:                          339
Number of combinational cells:            329
Number of sequential cells:                 0
Number of macros/black boxes:               0
Number of buf/inv:                         32
Number of references:                      10

Combinational area:               1549.497643
Buf/Inv area:                       76.204803
Noncombinational area:               0.000000
Macro/Black Box area:                0.000000
Net Interconnect area:           35000.175476

Total cell area:                  1549.497643
Total area:                      36549.673120
1
```

Sbox2

```
****************************************
Report : area
Design : sbox
Version: R-2020.09
Date   : Tue Nov 29 15:26:20 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUTM_A

Number of ports:                          16
Number of nets:                          378
Number of cells:                         370
Number of combinational cells:           370
Number of sequential cells:                0
Number of macros/black boxes:              0
Number of buf/inv:                        51
Number of references:                     49

Combinational area:              1433.073637
Buf/Inv area:                     124.185604
Noncombinational area:              0.000000
Macro/Black Box area:               0.000000
Net Interconnect area:          52126.927673

Total cell area:                 1433.073637
Total area:                     53560.001310
```

Inv_Sbox2

```
****************************************
Report : area
Design : inv_sbox
Version: R-2020.09
Date   : Tue Nov 29 15:31:11 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUTM_

Number of ports:                          16
Number of nets:                          392
Number of cells:                         384
Number of combinational cells:           384
Number of sequential cells:                0
Number of macros/black boxes:              0
Number of buf/inv:                        51
Number of references:                     54

Combinational area:              1459.180837
Buf/Inv area:                     118.540804
Noncombinational area:              0.000000
Macro/Black Box area:               0.000000
Net Interconnect area:          53060.265747

Total cell area:                 1459.180837
Total area:                     54519.446584
1
```

Aes-128 low area (nonpipelined):

```
****************************************
Report : area
Design : aes128_top
Version: R-2020.09
Date   : Tue Nov 29 17:02:40 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GU

Number of ports:                         8858
Number of nets:                         97149
Number of cells:                        88574
Number of combinational cells:          88253
Number of sequential cells:               134
Number of macros/black boxes:               0
Number of buf/inv:                      20291
Number of references:                     159

Combinational area:             539106.630894
Buf/Inv area:                   113850.677189
Noncombinational area:            2535.926374
Macro/Black Box area:                0.000000
Net Interconnect area:        10621106.385101

Total cell area:                  541642.557268
Total area:                   11162748.942370
1
```

Aes-128 Pipeline:

```
****************************************
Report : area
Design : aes128_pip
Version: R-2020.09
Date   : Wed Nov 30 10:20:07 2022
****************************************

Library(s) Used:

    slow (File: /usr/cad/synopsys/CBDK_TSMC90GUTM

Number of ports:                        43814
Number of nets:                        533041
Number of cells:                       490219
Number of combinational cells:         487275
Number of sequential cells:              1284
Number of macros/black boxes:               0
Number of buf/inv:                      75130
Number of references:                      31

Combinational area:            1950491.541675
Buf/Inv area:                   221099.765383
Noncombinational area:           19799.136078
Macro/Black Box area:                0.000000
Net Interconnect area:        60831331.070801

Total cell area:                 1970290.677752
Total area:                   62801621.748553
1
```

四、結論

從我們最後合成的結果，Mc1為優化前，Mc2為優化後，Mix Column()的優化並沒有很明顯的進度。Mc2與Mc1總面積約完77%(392211/507119)，少了22.6%。從Mc與Inv_Mc相比，[3]所述解密系統將會比加密面積大。S-box1與S-box2相比較，少了31.7%的面積。最後低面積架構總面積為11162748.942370。有10-stage的管線化架構總面積為62801621.748553。總面積大約大了5.62倍。

五、參考文獻

[1] Joan Daemen, Vincent Rijmen, " AES Proposal: Rijndael"[online].Available:https://www.researchgate.net/publication/2237728_AES_proposal_rijndael [AccessedOct. 1999].

[2] Johannes Wolkerstorfer, Elisabeth Oswald & Mario Lamberger, “ An ASIC Implementation of the AES SBoxes,” CT-RSA 2002: Topics in Cryptology — CT-RSA 2002 pp 67–78

[3] Artur Gielata; Pawel Russek; Kazimierz Wiatr, “AES hardware implementation in FPGA for algorithm acceleration purpose,” 2008 International Conference on Signals and Electronic Systems

六、計劃管理與團隊合作方式

趙泓瑞 E14071025

相關論文閱讀與蒐集

基本功能撰寫與優化

低面積 Aes128 架構實作

Mix_column()優化

郭冠緯 E24086030

相關論文閱讀與蒐集

Sub-byte()優化

測資撰寫

低面積 Aes128 架構實作

管線化 Aes128 架構實作

合成