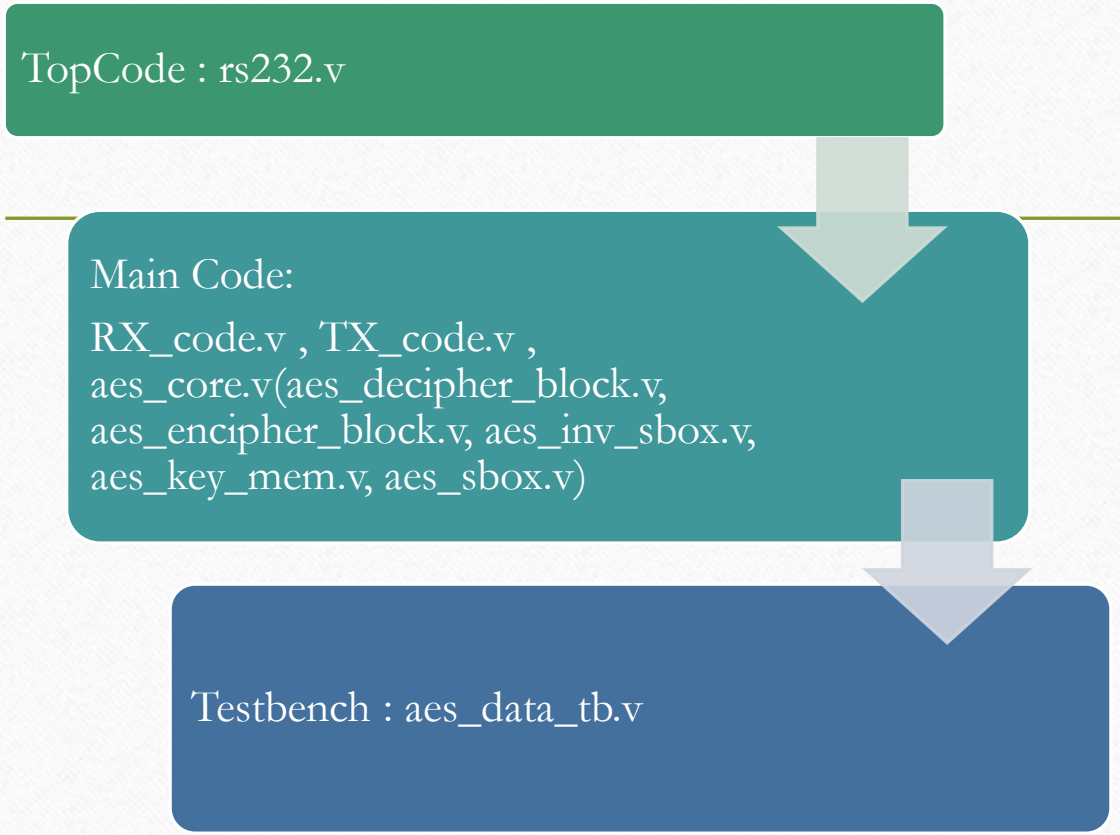
Keypro

架構

Verilog程式


TopCode : rs232.v
Main Code:
RX_code.v , TX_code.v ,
aes_core.v(aes_decipher_block.v,
aes_encipher_block.v, aes_inv_sbox.v,
aes_key_mem.v, aes_sbox.v)
Testbench : aes_data_tb.v

RX、TX傳送接收格式

- RX接收格式

一次接收8組bytes，以下為每組bits的功能

第1組：輸入02以表示開始接收資料。

第2組：1~7個bits控制資料ram位置，第8個bit為1則為寫入，0則為輸出。

第3~6組：需要存放的資料。

第7組：check bit(未使用)。

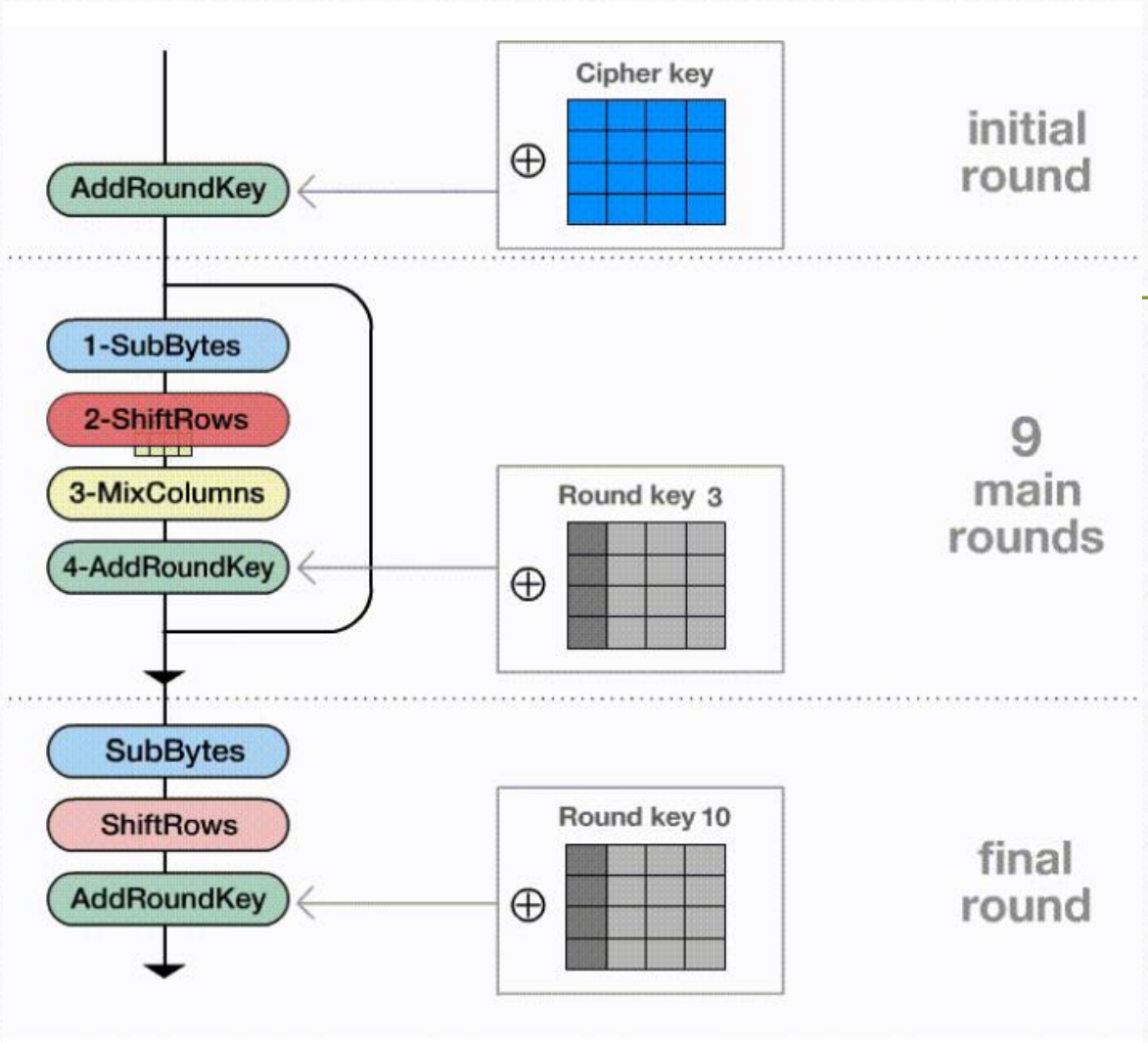
第8組：輸入03已表示資料接收完畢。

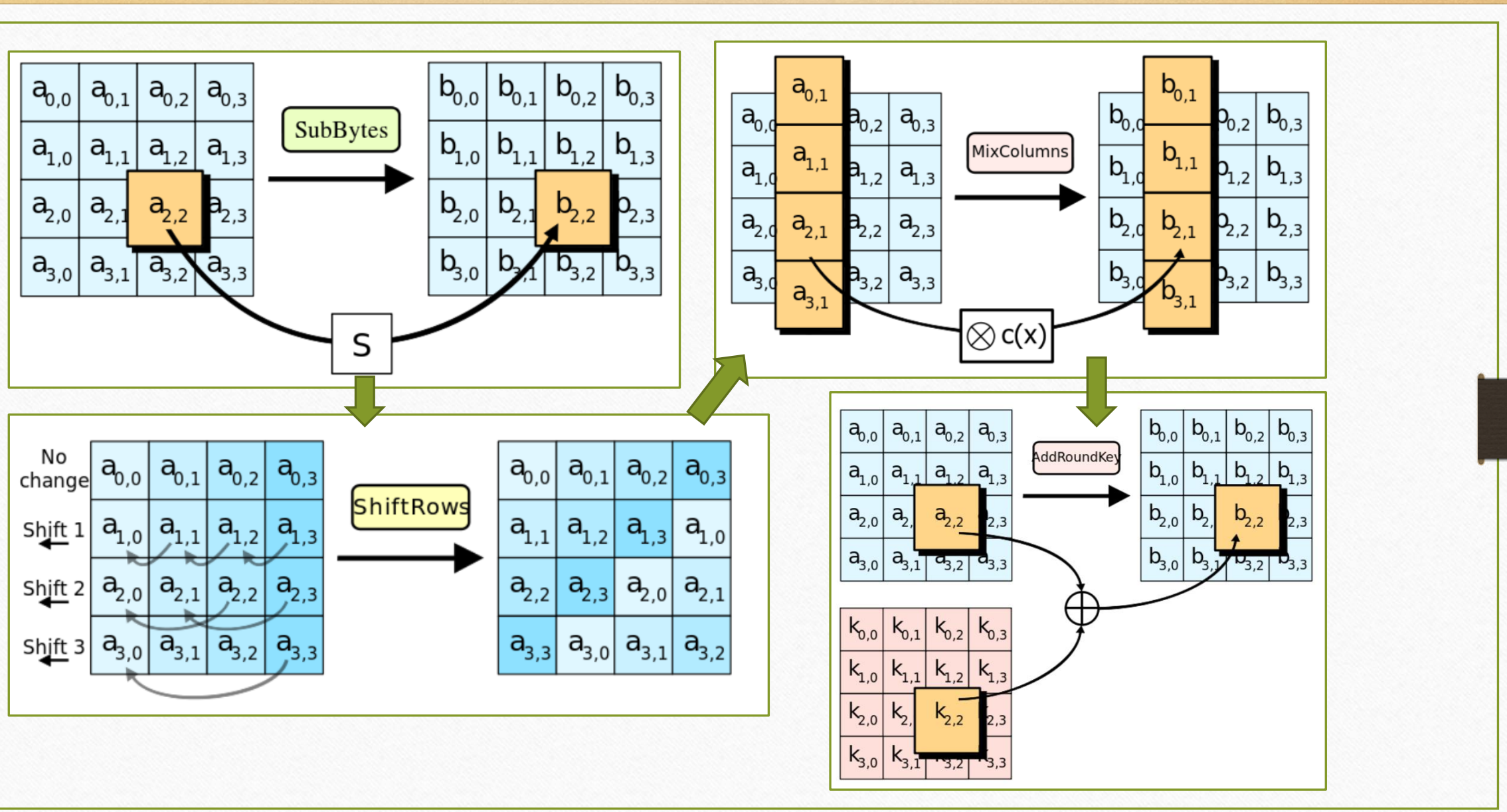
- TX傳送格式

一次傳送4組bytes

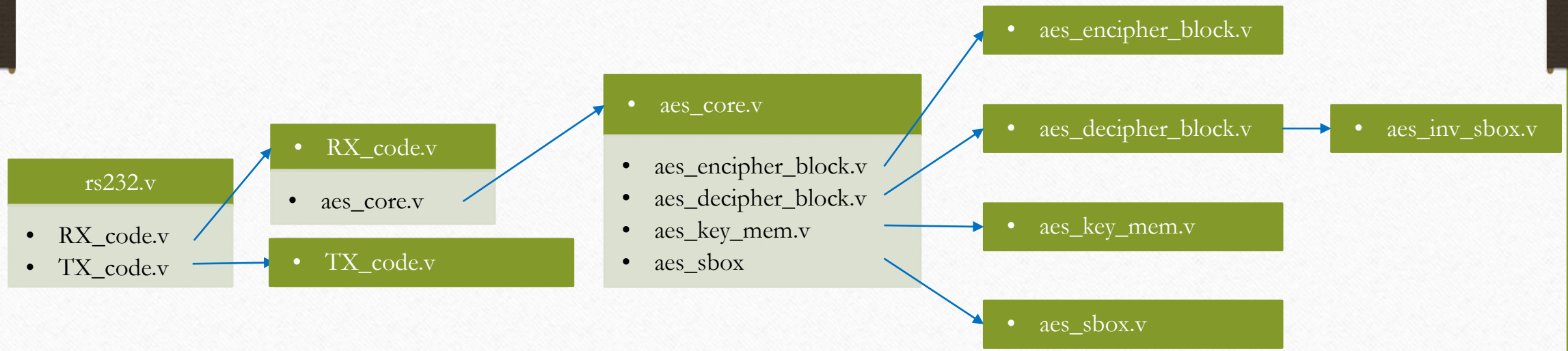
上述RX存取的第3~6組bytes(4bytes)會存入32bits的ram，判斷address後將對應ram位置的32bits全部讀出。

AES


Cipher key
initial round
AddRoundKey
1-SubBytes
2-ShiftRows
3-MixColumns
4-AddRoundKey
Round key 3
9 main rounds
SubBytes
ShiftRows
AddRoundKey
Round key 10
final round


SubBytes
S
MixColumns
c(x)
No change
Shift 1
Shift 2
Shift 3
ShiftRows
AddRoundKey

Verilog程式架構



rs232.v

- rs232(TX, RX, clk, rst)

output

- TX : 從FPGA傳出資料(64bits)

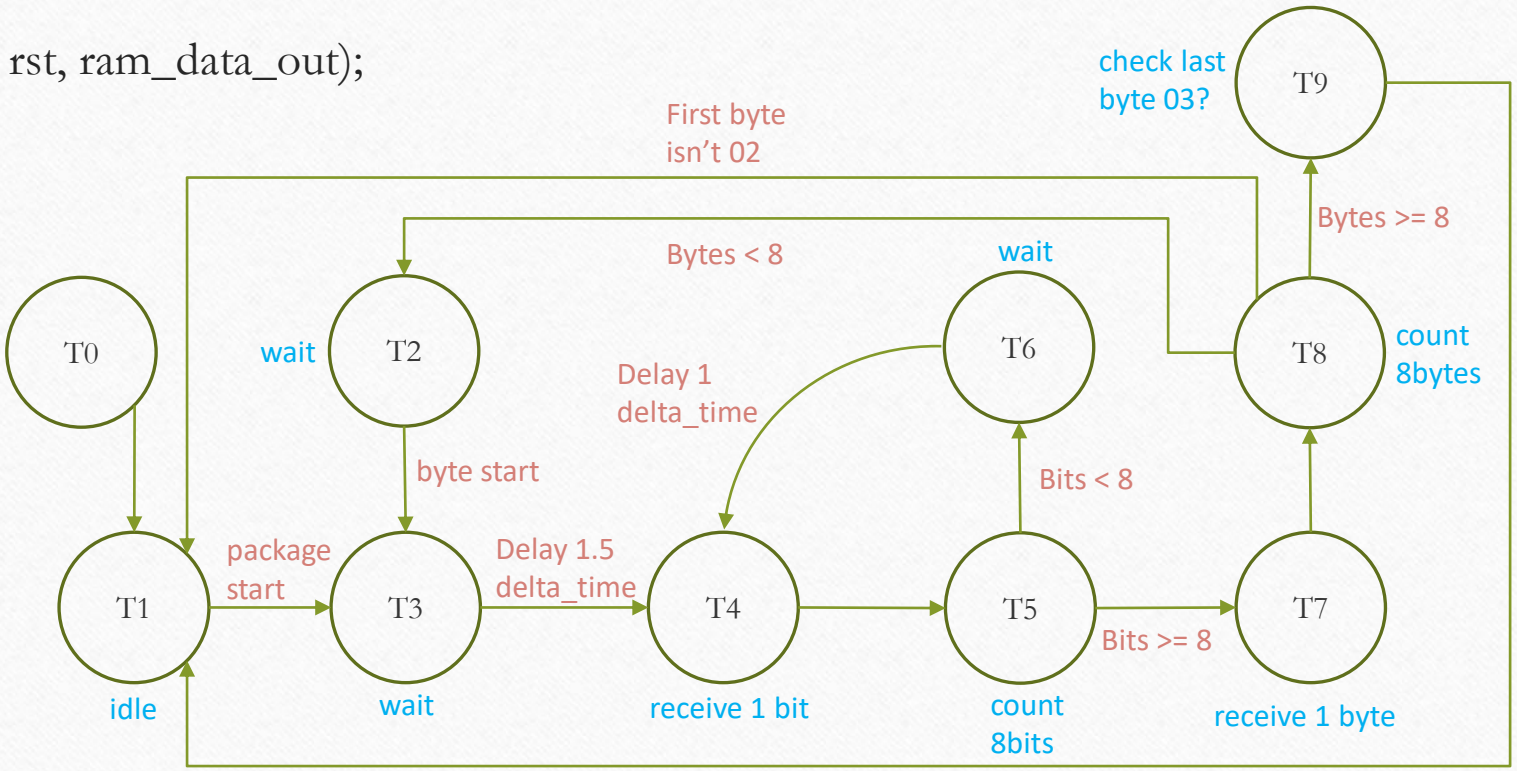
input

- RX : FPGA接收資料(64bits)
- clk : 50MHz
- rst : 重製資料

RX_code.v

- RX_code(data_in, tx_start, clk, rst, ram_data_out);

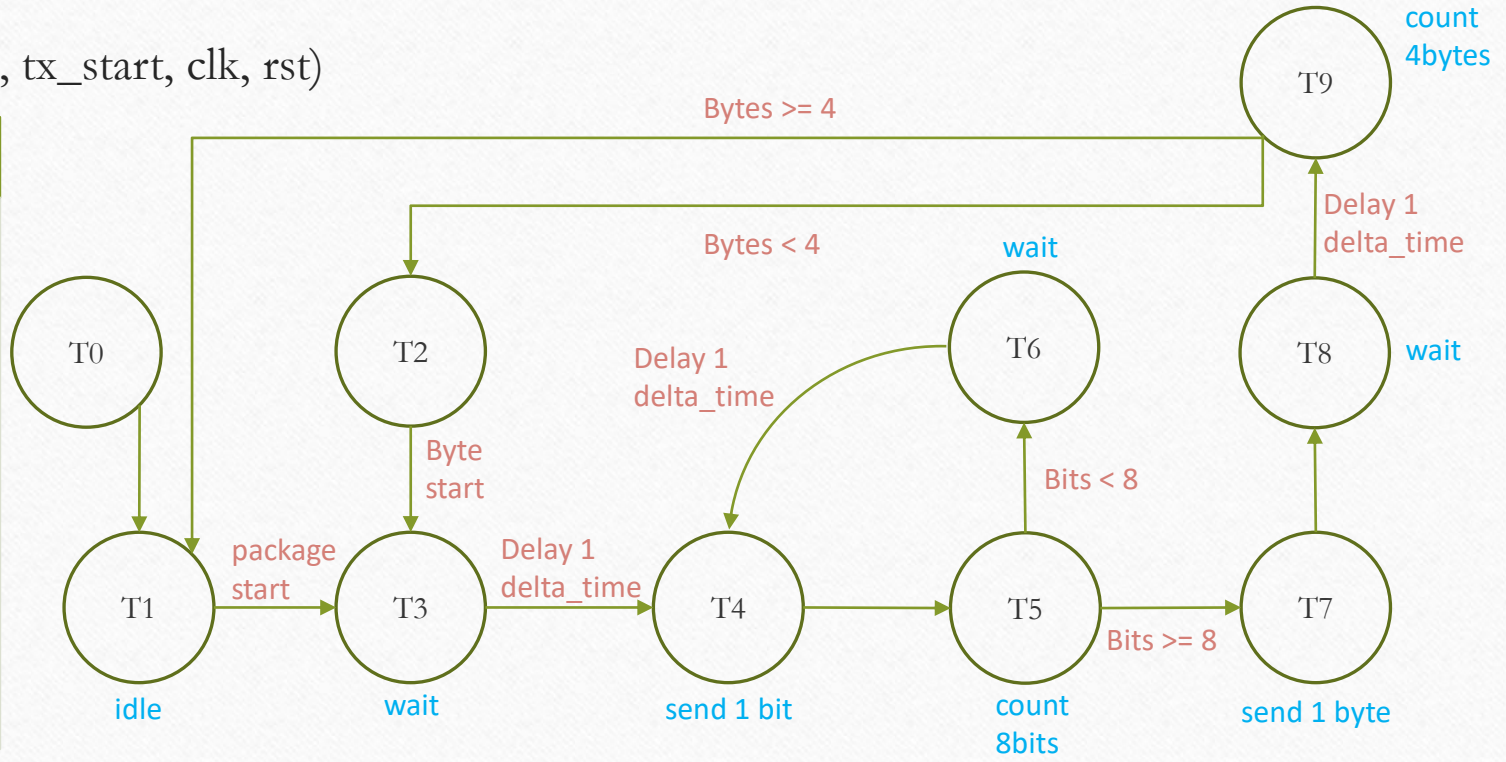
output	input
• ram_data_out: 傳送從ram讀取的資料。 • tx_start : RX接收到需要read ram資料的指令時，控制TX回傳資料。	• data_in : RX線接收到的資料。 • clk : 50MHz。 • rst : 重製資料。



TX_code.v

- TX_code(data_out, data_in, tx_start, clk, rst)

output	input
• data_out : 需要傳輸的資料。	• data_in : 從ram讀取到的資料。 • tx_start : 接收開始傳輸的指令。 • clk : 50MHz。 • rst : 重製資料。



aes_core.v

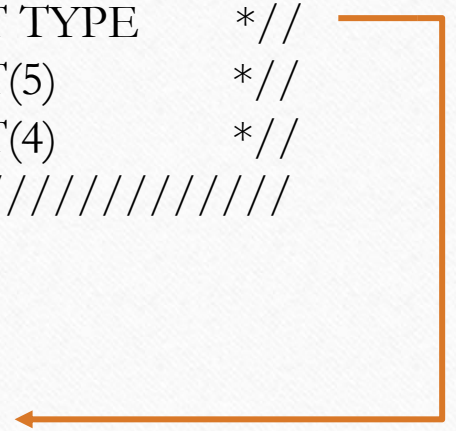
- aes_core(clk, reset_n, encdec, init, next, ready, key, keylen, block, result, result_valid)

output	input
• ready : key擴展完成或是加密完成都會使ready為1 • result : 加密後結果資料 • result_valid : 判斷加密成功	• encdec : 加解密控制接腳 • init : key開始擴展 • next : 資料開始加密 • key : 初始key • keylen : 加密寬度控制 (128/256) • block : 需加密資料

Ram存放格式

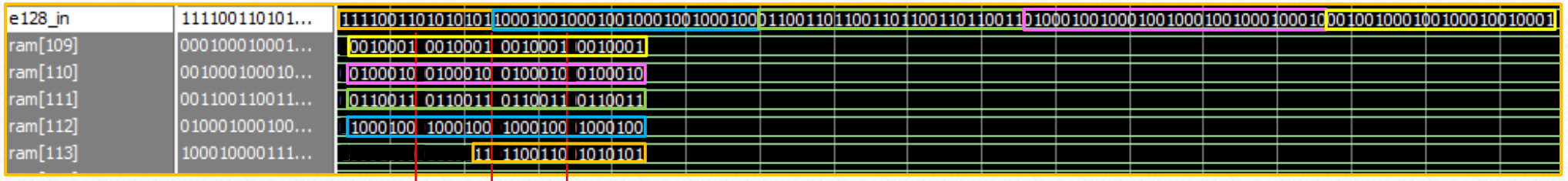
- //////WRITE AND READ/////////
- //*[4]-[8] INPUT DATA(5) *//
- //*[9] DO 128 ENCRYPT *//
- //*[10] DO 128 DECRYPT *//
- //*[11] DO 256 ENCRYPT *//
- //*[12] DO 256 DECRYPT *//
- //*[13]-[16] INPUT DATA(4) *//
- //*[24-33] KEY *//
- ////////////////////////////////

//////////////READ ONLY//////////
//*[60] AES OUTPUT TYPE *//
//*[64]-[68] AES OUTPUT(5) *//
//*[73]-[76] AES OUTPUT(4) *//
////////////////////////////////



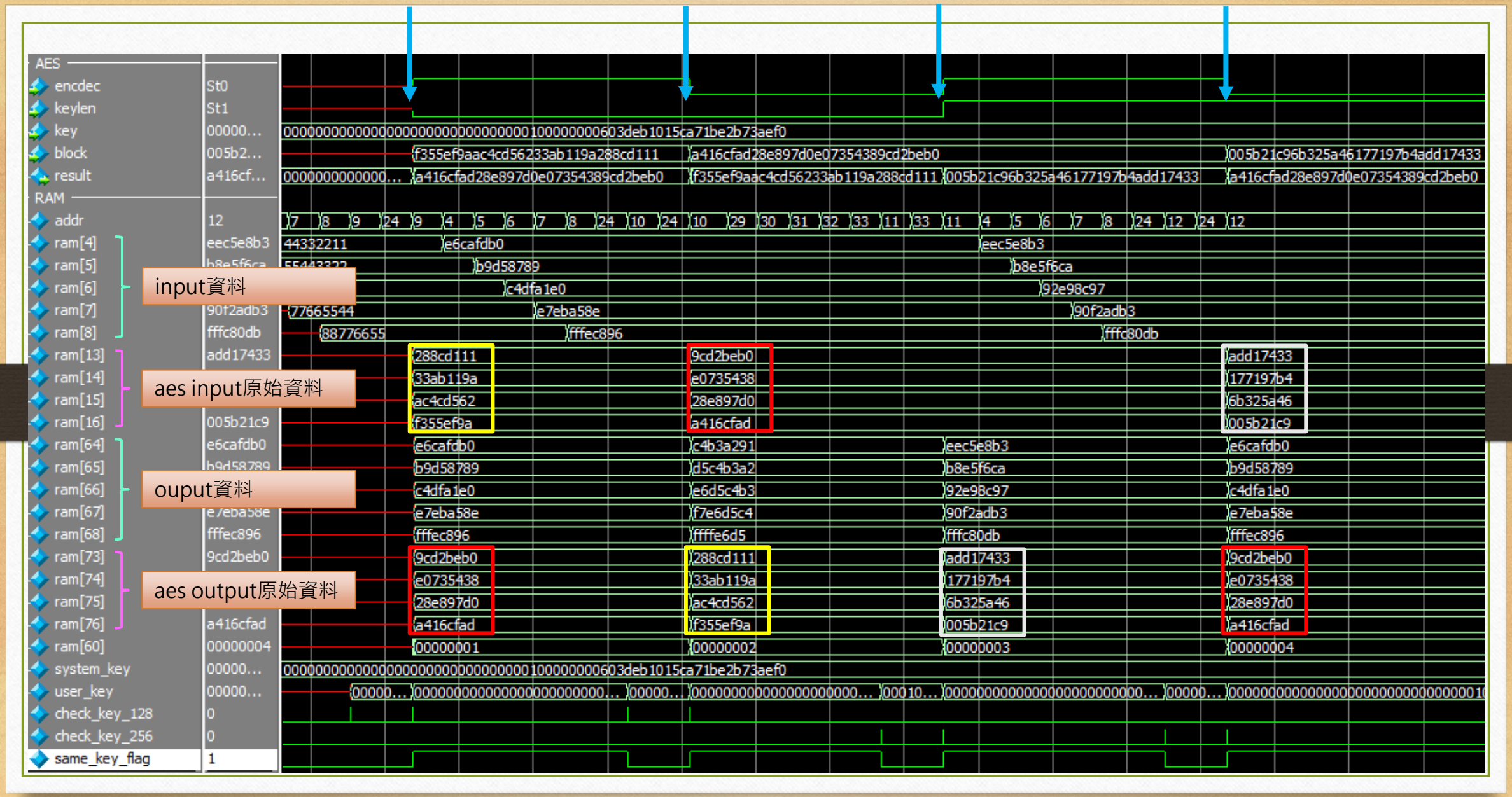
///////AES TYPE//////
//* 1:128 ENCRYPT *//
//* 2:128 DECRYPT *//
//* 3:256 ENCRYPT *//
//* 4:256 DECRYPT *//
////////////////////////

AES加密資料規格

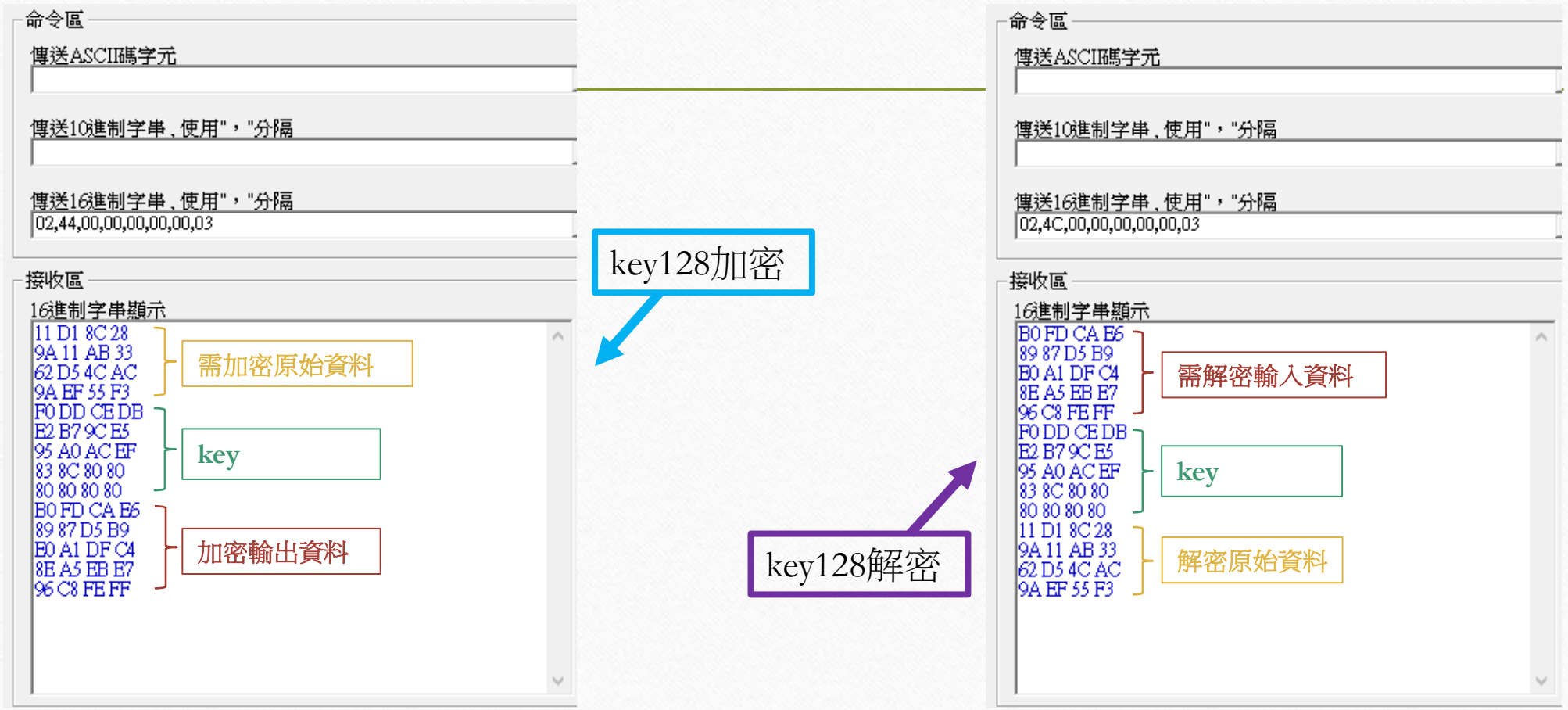


- 加密資料寬度為128，每筆RAM資料為4組bytes，但每組byte的第1個bit不使用，因此每筆RAM的可用資料為28bits，因此每筆AES資料須使用5筆RAM，第5筆僅使用16bits。

e128_in	f355891224466...	f355891224466cd9b34489122224891
ram[109]	11111111	11111111
ram[110]	22222222	22222222
ram[111]	33333333	33333333
ram[112]	44444444	44444444
ram[113]	88776655	88776655


加密128
解密128
加密256
解密256
AES
encdec
keylen
key
block
result
RAM
addr
ram[4]
ram[5]
ram[6]
ram[7]
ram[8]
ram[13]
ram[14]
ram[15]
ram[16]
ram[64]
ram[65]
ram[66]
ram[67]
ram[68]
ram[73]
ram[74]
ram[75]
ram[76]
ram[60]
system_key
user_key
check_key_128
check_key_256
same_key_flag
input資料
aes input原始資料
ouput資料
aes output原始資料

RS232測試軟體

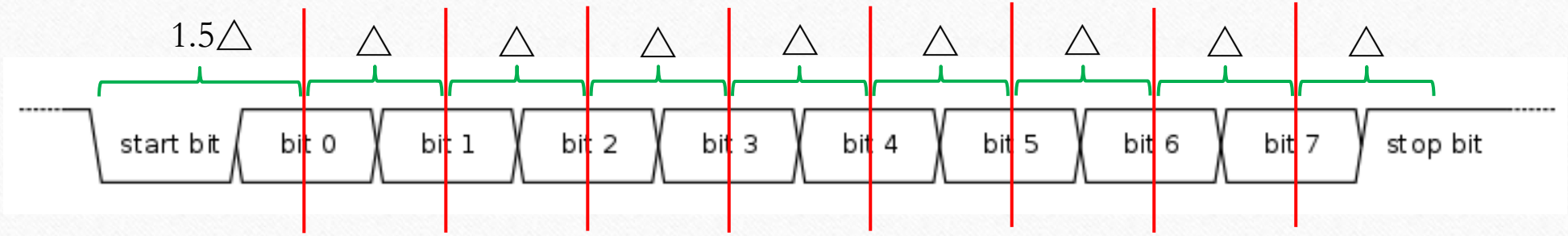

命令區
傳送ASCII碼字元
傳送10進制字串，使用","分隔
傳送16進制字串，使用","分隔
02,44,00,00,00,00,00,03
接收區
16進制字串顯示
11 D1 8C 28
9A 11 AB 33
62 D5 4C AC
9A EF 55 F3
需加密原始資料
F0 DD CE DB
E2 B7 9C E5
95 A0 AC EF
83 8C 80 80
80 80 80 80
key
B0 FD CA E6
89 87 D5 B9
E0 A1 DF C4
8E A5 EB E7
96 C8 FE FF
加密輸出資料
key128加密
key128解密
命令區
傳送ASCII碼字元
傳送10進制字串，使用","分隔
傳送16進制字串，使用","分隔
02,4C,00,00,00,00,00,03
接收區
16進制字串顯示
B0 FD CA E6
89 87 D5 B9
E0 A1 DF C4
8E A5 EB E7
96 C8 FE FF
需解密輸入資料
F0 DD CE DB
E2 B7 9C E5
95 A0 AC EF
83 8C 80 80
80 80 80 80
key
11 D1 8C 28
9A 11 AB 33
62 D5 4C AC
9A EF 55 F3
解密原始資料

GitHub紀錄

- https://github.com/Justina0331/rs232_AES.git

AES參考資料

- https://www.796t.com/content/1541892089.html
- https://ithelp.ithome.com.tw/articles/10249488
- https://github.com/michaelehab/AES-Verilog
- https://github.com/secworks/aes


1.5△
start bit
bit 0
bit 1
bit 2
bit 3
bit 4
bit 5
bit 6
bit 7
stop bit