Elliptic Curve Cryptographic Processor

Computer-Aided VLSI System Design Final Project

Team members: 謝宗翰、吳凱濠

● Algorithm Design

I. 方法 1： 簡化 Modular Multiplication

在助教提供的 Modular Mul 算法中$x \times y \bmod q = MM(MM(x,y), R^2 \bmod q)$
會用到大量的乘法。若能簡化 Modular Mul 將可以減少大量計算。
在 Ed25519 中，$p = 2^{255} - 19$ 而 $2^{258}(mod\ p) = 152(mod\ p)$,
$2^{255}\ (mod\ p) = 19\ (mod\ p)$ ，我們利用這兩點數學式進行化簡。

I. 以 10 進位的95×46為例，根據 Karatsuba Algorithm 可得

$a = 95 = (a_1 \times 10 + a_0)$,

$b = 46 = (b_1 \times 10 + b_0)$,

藉由把a, b拆成高位及低位，得到H, M, L。並令$\alpha = 10$ (10 進位)

$H = a_1 b_1 = 36$,

$M = (a_0 + a_1)(b_0 + b_1) = 140$,

$L = a_0 b_0 = 30$,

$95 \times 46 = H \times \mathbf{10^2} + L + (M - H - L) \times \mathbf{10} = 4370$

$\Rightarrow a \times b = \boldsymbol{\alpha^2} H + L + \boldsymbol{\alpha}(M - H - L) = c$

II. 因此，按照上述方法令$\alpha = 2^{129}$，$C = 2^{258}\, H + 2^{129}(M - H - L) + L$

i. $C_h = H,\ C_l = 2^{129}(M - H - L) + L$

ii. 因為$2^{258}(mod\ p) = 152(mod\ p)$,
因此可以令 $T = 152C_h + C_l = 2^{255}T_h + T_l$

iii. 為了能利用$2^{258}(mod\ p) = 152(mod\ p)$，把 T_h以2^{255}拆分高位及低位，得到

$$T_h = (T_{391}, T_{390}, \ldots, T_{256}, T_{255})_2,\ T_l = (T_{254}, T_{253}, \ldots, T_1, T_0)_2$$

$$\Rightarrow T = 19T_h + T_l$$

iv. 最後進行$mod\ q$判斷，如果$T > q$，則$T = T - q$，否則$T = T$

II. 方法 2： Point Multiplication 減少 Point addition 與增加 Doubling 次數

Point Multiplication 方面，我們採用比 Window Method 更有效率的 Sliding Window 的演算法，來達到 Doubling 次數最大化。以下為算法介紹。

I. Sliding Windows 演算法特點：

i. 僅預先計算 P 的奇數倍：如 P, 3P, 5P，減少額外計算

ii. 跳過 0 的處理：遇到連續 0 時，只執行 Doubling。

iii. window 從 1 開始：window 從第一個 1 開始，略過多餘的 0

II. 簡單的例子(Window size = 3)：

$scalar\_m = 410 = (110011010)_2$

$\Rightarrow window = 110 \mid 0 \mid 110 \mid 10$

i. $first\ window\ (110)$: $Dbl, Dbl, Add(3P), Dbl$

ii. $Skip(0)$: Dbl

iii. $Second\ window(110)$: $Dbl, Dbl, Add(3P), Dbl$

iv. $Third\ window(10)$: $Dbl, Add(P), Dbl$

III. 我們實作的細節

i. 我們這次 Final Project 採用 window size = 3 的算法，先將 P_3, P_5, P_7計算好 Permute Table，並令 $r = (0,1,1), P = (x, y, 1)$

$P_d = 2P,\ P_3 = P_d + P,\ P_5 = 2P_d + P,\ P_7 = 2P_3 + P$

ii. 當$index = 0 \sim 254$

如果$m[index] == 0$:

$r = double$

否則$win = m[index: index + 2]$:

$win =$ "111": $r = double \rightarrow double \rightarrow double \rightarrow add(P7)$

$win =$ "110": $r = double \rightarrow double \rightarrow add(P3) \rightarrow double$

$win =$ "111": $r = double \rightarrow double \rightarrow double \rightarrow add(P5)$

$win =$ "100": $r = double \rightarrow add(P) \rightarrow double \rightarrow double$

$win =$ "11": $r = double \rightarrow double \rightarrow add(P3) \rightarrow double$

$win =$ "10": $r = double \rightarrow add(P) \rightarrow double$

$win =$ "1": $r = double \rightarrow add(P)$

$index = index + len(win)$

以 PAT1 來說，相較原本的 Double-Add 算法，Sliding Window 從 5312 cycle 減少至 4599 cycle。

iii. 演算法流程

a. 讀取 M,X,Y，並令$r = (0,1,1), index = 254, P = (X, Y, 1)$

b. 當$index > 0$:

$$Sliding\ Windows(r, P, M, index)$$

c. 令$index = 254, n = 1$進行 reduction

d. 進行$Point\ r(X_r, Y_r, Z_r)$的 reduction

1. 當$index > 0$:

$$n = n \times n$$

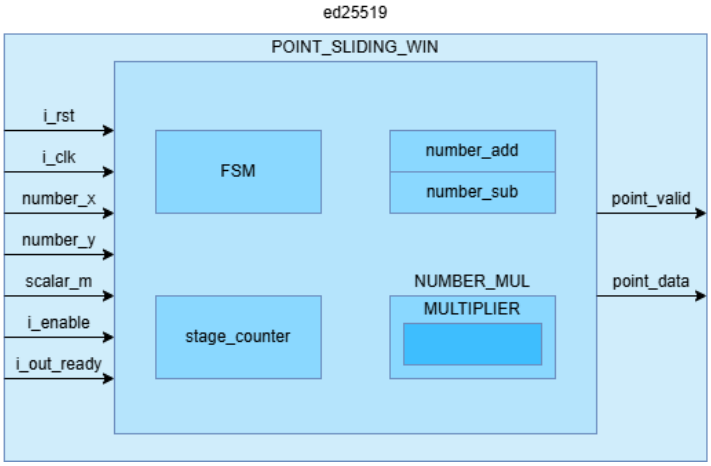
如果$index\ != 2,4$:

$$n = Z_r \times n$$

2. 此時$n = Z_r^{-1}\ mod\ q$，再將 n 與X_r, Y_r相乘得到輸出$X = X_r \times n,\ Y = Y_r \times n$

● Hardware Implementation

I. 總體電路架構圖



II. Optimization Techniques: 乘法器 Pipeline，Input Reschedule 以及 Register Sharing

在我們設計中，兩數相乘需要 3 cycle 才能完成，以 double 來說，會用到 7 個乘法，若不進行 pipeline，至少需要 21 cycle 才能完成，並且需要 8 個 Register 儲存變數。

經過 Pipeline 以及 Input Reschedule 並分析 Register 的生命週期後，只需要 4 個 Register，9 cycle 便能完成運算

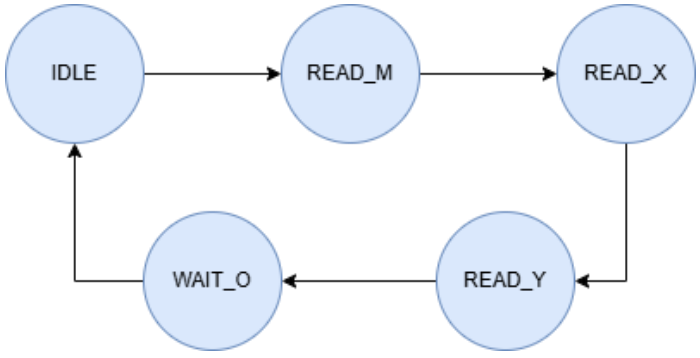
乘法器有 input：
乘法器運算：
快速 mod：
加減法：

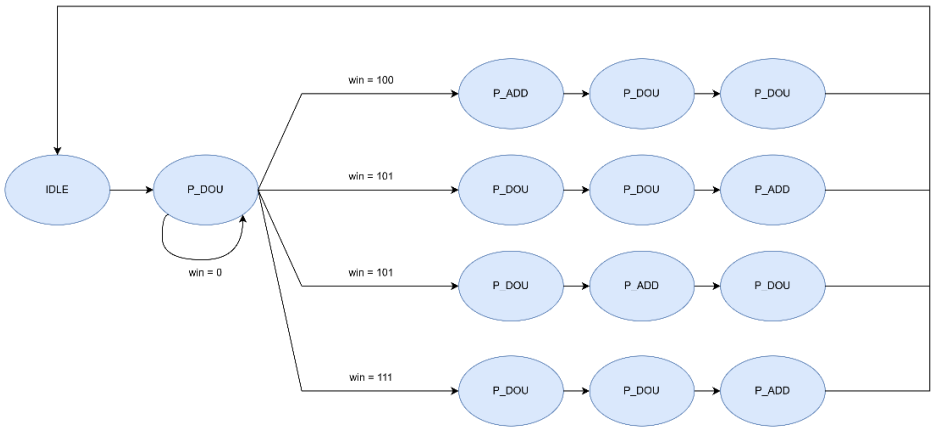
Doubling Pipeline Analysis									
Cycle	0	1	2	3	4	5	6	7	8
XY=X+Y			XY						
C=XX	C								
D=YY		D							
H=ZZ			H						
B=XYXY				B					
E=0-C			E						
F=E+D				E-D	H+H				
Y3=F(E-D)					Y3				
J=F-(H+H)					F-2H				
Z3=FJ						Z3			
X3=(B-C-D)J							X3		
Input Reschedule & Register Sharing									
r1			X+Y		J				
r2			E			B+E-D			Y3
r3				E-D				Z3	
r4				F					

Point-Add Pipeline Analysis														
Cycle	0	1	2	3	4	5	6	7	8	9	10	11	12	13
X1X2	X1X2													
Y1Y2		Y1Y2												

Z1Z2			Z1Z2											
X1+Y1	X1+Y1													
X2+Y2		X2+Y2												
E=X1+Y1*X2+Y2				E			*Y1Y2							
X1X2Y1Y2=d*X1X2*Y1Y2					d*X1X2									
Z1Z2_2=Z1Z2*Z1Z2						$Z1Z2^2$								
I=Y1Y2+X1X2				I										
H=E-X1X2-Y1Y2						H=E - I								
F=Z1Z2_2-X1X2Y1Y2									F	*F				
X3=Z1Z2*H*F								Z1Z2*H						
G=Z1Z2_2+X1X2Y1Y2										G	*G			
Y3=Z1Z2*I*G									Z1Z2*I					
Z3=F*G												F*G		

III. Design of key modules

Ed25519 Module

Module ed25519 負責與 Testbench 的 Handshake，主要包含了 FSM 以及 Counter，Counter 負責計算輸入 data 的 Index，FSM 流程如附圖。當接收完 X,Y,M 後，發送 enable 訊號給 module point 開始計算。當 module point 完成計算後，再由 ed25519 向 Testbench 輸出 data。

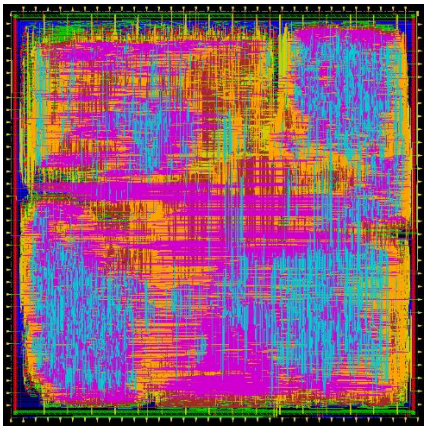
Sliding Window (point.v) Module

Sliding window 的 FSM 流程會因為 win 所接收到的值不同而不同。 $win =$ "111": $r = double \rightarrow double \rightarrow double \rightarrow add(P7)$ $win =$ "110": $r = double \rightarrow double \rightarrow add(P3) \rightarrow double$ $win =$ "111": $r = double \rightarrow double \rightarrow double \rightarrow add(P5)$ $win =$ "100": $r = double \rightarrow add(P) \rightarrow double \rightarrow double$ (為了簡化流程圖，省略了結尾的 win = 10, 11, 1 的流程)

Number_mul Module
共分成三個 Stage Stage 1：Multiplier 負責計算H, M, L Stage 2：計算$152C_h + C_l$ Stage 3：計算$T = 19T_h + T_l$以及判斷是否$> q$

Doubling & Point-add Module
根據 Input Reschedule & Register Sharing 來進行乘法器的 Input 選擇

- # APR Results

I. Screenshot of the layout



II. DRC/LVS results

i. verify_drc

```
VERIFY DRC ..... Sub-Area : 63 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {0.000 1408.960 201.280 1610.240} 64 of 81
VERIFY DRC ..... Sub-Area : 64 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {201.280 1408.960 402.560 1610.240} 65 of 81
VERIFY DRC ..... Sub-Area : 65 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {402.560 1408.960 603.840 1610.240} 66 of 81
VERIFY DRC ..... Sub-Area : 66 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {603.840 1408.960 805.120 1610.240} 67 of 81
VERIFY DRC ..... Sub-Area : 67 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {805.120 1408.960 1006.400 1610.240} 68 of 81
VERIFY DRC ..... Sub-Area : 68 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1006.400 1408.960 1207.680 1610.240} 69 of 81
VERIFY DRC ..... Sub-Area : 69 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1207.680 1408.960 1408.960 1610.240} 70 of 81
VERIFY DRC ..... Sub-Area : 70 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1408.960 1408.960 1610.240 1610.240} 71 of 81
VERIFY DRC ..... Sub-Area : 71 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1610.240 1408.960 1809.640 1610.240} 72 of 81
VERIFY DRC ..... Sub-Area : 72 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {0.000 1610.240 201.280 1806.460} 73 of 81
VERIFY DRC ..... Sub-Area : 73 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {201.280 1610.240 402.560 1806.460} 74 of 81
VERIFY DRC ..... Sub-Area : 74 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {402.560 1610.240 603.840 1806.460} 75 of 81
VERIFY DRC ..... Sub-Area : 75 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {603.840 1610.240 805.120 1806.460} 76 of 81
VERIFY DRC ..... Sub-Area : 76 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {805.120 1610.240 1006.400 1806.460} 77 of 81
VERIFY DRC ..... Sub-Area : 77 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1006.400 1610.240 1207.680 1806.460} 78 of 81
VERIFY DRC ..... Sub-Area : 78 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1207.680 1610.240 1408.960 1806.460} 79 of 81
VERIFY DRC ..... Sub-Area : 79 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1408.960 1610.240 1610.240 1806.460} 80 of 81
VERIFY DRC ..... Sub-Area : 80 complete 0 Viols.
VERIFY DRC ..... Sub-Area: {1610.240 1610.240 1809.640 1806.460} 81 of 81
VERIFY DRC ..... Sub-Area : 81 complete 0 Viols.

Verification Complete : 0 Viols.

*** End Verify DRC (CPU: 0:00:35.2  ELAPSED TIME: 35.00  MEM: 120.0M) ***
```

```
innovus 1> verify_drc
 *** Starting Verify DRC (MEM: 2500.7) ***

 VERIFY DRC ..... Starting Verification
 VERIFY DRC ..... Initializing
 VERIFY DRC ..... Deleting Existing Violations
 VERIFY DRC ..... Creating Sub-Areas
 VERIFY DRC ..... Using new threading
 VERIFY DRC ..... Sub-Area: {0.000 0.000 201.280 201.280} 1 of 81
 VERIFY DRC ..... Sub-Area : 1 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {201.280 0.000 402.560 201.280} 2 of 81
 VERIFY DRC ..... Sub-Area : 2 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {402.560 0.000 603.840 201.280} 3 of 81
 VERIFY DRC ..... Sub-Area : 3 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {603.840 0.000 805.120 201.280} 4 of 81
 VERIFY DRC ..... Sub-Area : 4 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {805.120 0.000 1006.400 201.280} 5 of 81
 VERIFY DRC ..... Sub-Area : 5 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1006.400 0.000 1207.680 201.280} 6 of 81
 VERIFY DRC ..... Sub-Area : 6 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1207.680 0.000 1408.960 201.280} 7 of 81
 VERIFY DRC ..... Sub-Area : 7 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1408.960 0.000 1610.240 201.280} 8 of 81
 VERIFY DRC ..... Sub-Area : 8 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1610.240 0.000 1809.640 201.280} 9 of 81
 VERIFY DRC ..... Sub-Area : 9 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {0.000 201.280 201.280 402.560} 10 of 81
 VERIFY DRC ..... Sub-Area : 10 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {201.280 201.280 402.560 402.560} 11 of 81
 VERIFY DRC ..... Sub-Area : 11 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {402.560 201.280 603.840 402.560} 12 of 81
 VERIFY DRC ..... Sub-Area : 12 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {603.840 201.280 805.120 402.560} 13 of 81
 VERIFY DRC ..... Sub-Area : 13 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {805.120 201.280 1006.400 402.560} 14 of 81
 VERIFY DRC ..... Sub-Area : 14 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1006.400 201.280 1207.680 402.560} 15 of 81
 VERIFY DRC ..... Sub-Area : 15 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1207.680 201.280 1408.960 402.560} 16 of 81
 VERIFY DRC ..... Sub-Area : 16 complete 0 Viols.
 VERIFY DRC ..... Sub-Area: {1408.960 201.280 1610.240 402.560} 17 of 81
 VERIFY DRC ..... Sub-Area : 17 complete 0 Viols.
```

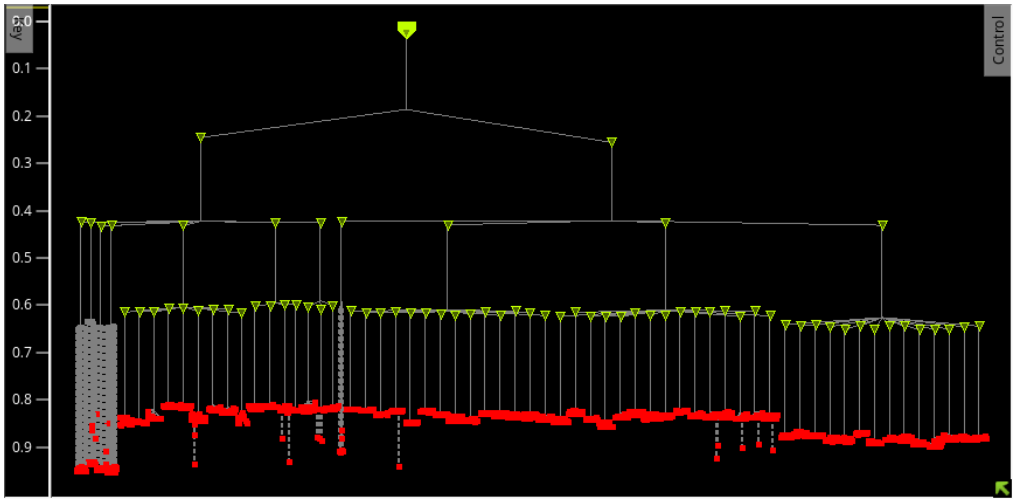
ii. Verify Connectivity

```
**** 00:07:45 **** Processed 130000 nets.
**** 00:07:45 **** Processed 135000 nets.
**** 00:07:45 **** Processed 140000 nets.
**** 00:07:45 **** Processed 145000 nets.
**** 00:07:45 **** Processed 150000 nets.
**** 00:07:45 **** Processed 155000 nets.
**** 00:07:45 **** Processed 160000 nets.
**** 00:07:45 **** Processed 165000 nets.
**** 00:07:45 **** Processed 170000 nets.
**** 00:07:46 **** Processed 175000 nets.
**** 00:07:46 **** Processed 180000 nets.
**** 00:07:46 **** Processed 185000 nets.
**** 00:07:46 **** Processed 190000 nets.
**** 00:07:46 **** Processed 195000 nets.
**** 00:07:46 **** Processed 200000 nets.
*** 00:07:46 *** Building data for Net VDD
*** 00:07:48 *** Building data for Net VSS

Begin Summary
  Found no problems or warnings.
End Summary

End Time: Mon Dec 16 00:07:49 2024
Time Elapsed: 0:00:09.0

******** End: VERIFY CONNECTIVITY ********
  Verification Complete : 0 Viols.  0 Wrngs.
  (CPU Time: 0:00:09.1  MEM: 217.188M)
```

iii. Verify Process Antenna

```
innovus 2>
******* START VERIFY ANTENNA ********
Report File: ed25519.antenna.rpt
LEF Macro File: ed25519.antenna.lef
5000 nets processed: 0 violations
10000 nets processed: 0 violations
15000 nets processed: 0 violations
20000 nets processed: 0 violations
25000 nets processed: 0 violations
30000 nets processed: 0 violations
35000 nets processed: 0 violations
40000 nets processed: 0 violations
45000 nets processed: 0 violations
50000 nets processed: 0 violations
55000 nets processed: 0 violations
60000 nets processed: 0 violations
65000 nets processed: 0 violations
70000 nets processed: 0 violations
75000 nets processed: 0 violations
80000 nets processed: 0 violations
85000 nets processed: 0 violations
90000 nets processed: 0 violations
95000 nets processed: 0 violations
100000 nets processed: 0 violations
105000 nets processed: 0 violations
110000 nets processed: 0 violations
115000 nets processed: 0 violations
120000 nets processed: 0 violations
125000 nets processed: 0 violations
130000 nets processed: 0 violations
135000 nets processed: 0 violations
140000 nets processed: 0 violations
145000 nets processed: 0 violations
150000 nets processed: 0 violations
155000 nets processed: 0 violations
160000 nets processed: 0 violations
165000 nets processed: 0 violations
170000 nets processed: 0 violations
175000 nets processed: 0 violations
180000 nets processed: 0 violations
185000 nets processed: 0 violations
190000 nets processed: 0 violations
195000 nets processed: 0 violations
200000 nets processed: 0 violations
Verification Complete: 0 Violations
******* DONE VERIFY ANTENNA ********
```

III. Clock Trees result



IV. setup time and hold time with no timing violation

```
------------------------------------------------------------------
          timeDesign Summary
------------------------------------------------------------------

Setup views included:
 av_func_mode_max

+--------------------+---------+---------+---------+---------+---------+---------+
|     Setup mode     |   all   | reg2reg | in2reg  | reg2out | in2out  | default |
+--------------------+---------+---------+---------+---------+---------+---------+
|           WNS (ns):|  0.054  |  0.054  |  1.536  |  2.695  |   N/A   |  0.000  |
|           TNS (ns):|  0.000  |  0.000  |  0.000  |  0.000  |   N/A   |  0.000  |
|    Violating Paths:|    0    |    0    |    0    |    0    |   N/A   |    0    |
|          All Paths:|  6118   |  6052   |  6052   |   65    |   N/A   |    0    |
+--------------------+---------+---------+---------+---------+---------+---------+

+----------------+-------------------------------+------------------+
|                |             Real              |       Total      |
|    DRVs        +------------------+------------+------------------|
|                |  Nr nets(terms)  | Worst Vio  |  Nr nets(terms)  |
+----------------+------------------+------------+------------------+
|   max_cap      |      0 (0)       |   0.000    |      0 (0)       |
|   max_tran     |      0 (0)       |   0.000    |      0 (0)       |
|   max_fanout   |      0 (0)       |     0      |      0 (0)       |
|   max_length   |      0 (0)       |     0      |      0 (0)       |
+----------------+------------------+------------+------------------+

Density: 92.813%
Total number of glitch violations: 0
------------------------------------------------------------------
```

```
------------------------------------------------------------------
          timeDesign Summary
------------------------------------------------------------------

Hold views included:
 av_func_mode_max

+--------------------+---------+---------+---------+---------+---------+---------+
|     Hold mode      |   all   | reg2reg | in2reg  | reg2out | in2out  | default |
+--------------------+---------+---------+---------+---------+---------+---------+
|           WNS (ns):|  0.867  |  0.867  |  1.506  |  2.458  |   N/A   |  0.000  |
|           TNS (ns):|  0.000  |  0.000  |  0.000  |  0.000  |   N/A   |  0.000  |
|    Violating Paths:|    0    |    0    |    0    |    0    |   N/A   |    0    |
|          All Paths:|  6118   |  6052   |  6052   |   65    |   N/A   |    0    |
+--------------------+---------+---------+---------+---------+---------+---------+

Density: 92.813%
------------------------------------------------------------------
```

V. critical path after post-route optimization

```
Path 1: MET Setup Check with Pin u_point_u_number_mul_s1_T_r_reg_386_/CK
Endpoint:   u_point_u_number_mul_s1_T_r_reg_386_/D            (^) checked with
leading edge of 'i_clk'
Beginpoint: u_point_u_number_mul_u_multiplier_1_L_r_reg_66_/Q (v) triggered by
leading edge of 'i_clk'
Path Groups: {reg2reg}
Analysis View: av_func_mode_max
Other End Arrival Time          0.698
- Setup                         0.121
+ Phase Shift                  10.000
+ CPPR Adjustment               0.000
= Required Time                10.577
- Arrival Time                 10.523
= Slack Time                    0.054
     Clock Rise Edge                 0.000
     + Clock Network Latency (Prop)  0.437
     = Beginpoint Arrival Time       0.437
     +-------------------------------------------------------------------------------------------------------+
     |                   Instance                    |     Arc      |   Cell    | Delay | Arrival | Required |
     |                                               |              |           |       |  Time   |   Time   |
     |-----------------------------------------------+--------------+-----------+-------+---------+----------|
     | u_point_u_number_mul_u_multiplier_1_L_r_reg_66_ | CK ^         |           |       |   0.437 |    0.491 |
     | u_point_u_number_mul_u_multiplier_1_L_r_reg_66_ | CK ^ -> Q v  | DFFQX1    | 0.327 |   0.763 |    0.818 |
     | FE_OFC17513_u_point_u_number_mul_L_66         | A v -> Y ^   | INVX3     | 1.047 |   1.811 |    1.865 |
     | U115290                                       | B ^ -> CO ^  | ADDFX2    | 0.543 |   2.354 |    2.409 |
     | U115291                                       | B ^ -> Y v   | NOR2X1    | 0.083 |   2.437 |    2.491 |
     | U115304                                       | B v -> Y ^   | NOR2XL    | 0.291 |   2.727 |    2.782 |
     | U115305                                       | B ^ -> Y v   | NAND2X1   | 0.391 |   3.119 |    3.173 |
     | U115404                                       | A v -> Y ^   | NOR2X1    | 0.338 |   3.457 |    3.512 |
     | U120288                                       | A ^ -> Y v   | NAND2X1   | 0.203 |   3.660 |    3.714 |
     | U9082                                         | A v -> Y ^   | NOR2X2    | 0.213 |   3.873 |    3.927 |
     | U120439                                       | A ^ -> Y v   | NAND2X1   | 0.156 |   4.029 |    4.083 |
     | U9953                                         | A1 v -> Y ^  | OAI21X4   | 0.185 |   4.214 |    4.268 |
     | FE_OFC32374_n92934                            | A ^ -> Y v   | INVX6     | 0.125 |   4.339 |    4.393 |
     | U40848                                        | A0 v -> Y ^  | OAI21X4   | 0.135 |   4.474 |    4.528 |
     | FE_OFC4534_n93128                             | A ^ -> Y v   | INVX2     | 0.123 |   4.597 |    4.651 |
     | U41825                                        | A0 v -> Y ^  | OAI21X1   | 0.140 |   4.738 |    4.792 |
     | FE_OFC4551_n93377                             | A ^ -> Y v   | INVX1     | 0.166 |   4.903 |    4.958 |
     | U121663                                       | A0 v -> Y ^  | OAI21XL   | 0.310 |   5.213 |    5.268 |
     | FE_OFC21053_n93408                            | A ^ -> Y v   | INVX1     | 0.118 |   5.332 |    5.386 |
     | U34512                                        | A0 v -> Y ^  | OAI21XL   | 0.323 |   5.654 |    5.709 |
     | U42410                                        | A0 ^ -> Y v  | AOI21XL   | 0.173 |   5.827 |    5.881 |
     | U121683                                       | A v -> Y v   | XNOR2X1   | 0.243 |   6.070 |    6.125 |
     | U121688                                       | A v -> Y ^   | NOR2XL    | 0.156 |   6.226 |    6.281 |
     | U121689                                       | B ^ -> Y v   | NAND2XL   | 0.113 |   6.340 |    6.394 |
     | U25703                                        | A v -> Y ^   | NOR2X1    | 0.164 |   6.503 |    6.558 |
     | U121744                                       | A ^ -> Y v   | NAND2X1   | 0.134 |   6.637 |    6.692 |
     | U9951                                         | B v -> Y ^   | NOR2X4    | 0.233 |   6.870 |    6.924 |
     | U121891                                       | A ^ -> Y v   | NAND2X1   | 0.179 |   7.049 |    7.103 |
     | U121892                                       | B v -> Y ^   | NOR2X4    | 0.121 |   7.170 |    7.224 |
     | U122095                                       | A ^ -> Y v   | NAND2X1   | 0.063 |   7.233 |    7.288 |
     | FE_RC_3301_0                                  | A v -> Y ^   | CLKINVX1  | 0.095 |   7.329 |    7.383 |
     | FE_RC_3300_0                                  | B ^ -> Y v   | NAND2BX4  | 0.076 |   7.405 |    7.460 |
     | FE_RC_3299_0                                  | A v -> Y ^   | NAND2X6   | 0.086 |   7.492 |    7.546 |
     | U122171                                       | A ^ -> Y v   | NAND2X4   | 0.073 |   7.565 |    7.619 |
     | U24837                                        | A v -> Y ^   | NOR2X4    | 0.092 |   7.656 |    7.711 |
     | U19306                                        | A ^ -> Y v   | NAND2X4   | 0.083 |   7.739 |    7.794 |
     | U122176                                       | A v -> Y ^   | NOR2X4    | 0.102 |   7.841 |    7.896 |
     | U54088                                        | A ^ -> Y v   | NAND2X2   | 0.085 |   7.927 |    7.981 |
     | U24678                                        | A v -> Y ^   | NOR2X4    | 0.105 |   8.032 |    8.086 |
     | U24609                                        | A ^ -> Y v   | NAND2X2   | 0.088 |   8.119 |    8.174 |
     | U122183                                       | A v -> Y ^   | NOR2X4    | 0.110 |   8.229 |    8.283 |
     | U12843                                        | A ^ -> Y v   | NAND2X2   | 0.076 |   8.305 |    8.359 |
     | U24475                                        | A v -> Y ^   | NOR2X2    | 0.147 |   8.452 |    8.506 |
     | U24361                                        | A ^ -> Y v   | NAND2X2   | 0.112 |   8.564 |    8.618 |
     | U122190                                       | A v -> Y ^   | NOR2X4    | 0.094 |   8.658 |    8.712 |
     | U27364                                        | A ^ -> Y ^   | AND2X6    | 0.122 |   8.779 |    8.834 |
     | FE_RC_909_0                                   | A ^ -> Y ^   | AND2X8    | 0.111 |   8.890 |    8.945 |
     | FE_RC_1790_0                                  | B ^ -> Y v   | NAND2BX4  | 0.066 |   8.956 |    9.011 |
     | FE_RC_1789_0                                  | B v -> Y ^   | NOR2BX4   | 0.088 |   9.044 |    9.098 |
     | U128394                                       | B ^ -> CO ^  | ADDHX2    | 0.154 |   9.198 |    9.252 |
     | U128403                                       | B ^ -> CO ^  | ADDHX2    | 0.151 |   9.349 |    9.403 |
     | FE_RC_2557_0                                  | B ^ -> Y ^   | AND2X4    | 0.130 |   9.479 |    9.533 |
     | FE_RC_2495_0                                  | B ^ -> Y ^   | AND2X4    | 0.125 |   9.604 |    9.659 |
     | U128451                                       | B ^ -> CO ^  | ADDHX2    | 0.146 |   9.750 |    9.805 |
     | U125548                                       | B ^ -> CO ^  | ADDHX2    | 0.149 |   9.900 |    9.954 |
     | U122465                                       | B ^ -> CO ^  | ADDHX2    | 0.145 |  10.045 |   10.099 |
     | FE_RC_4071_0                                  | B ^ -> Y ^   | XOR2X1    | 0.256 |  10.301 |   10.355 |
     | U122466                                       | AN ^ -> Y ^  | NOR2BX1   | 0.222 |  10.523 |   10.577 |
     | u_point_u_number_mul_s1_T_r_reg_386_          | D ^          | DFFHQX8   | 0.000 |  10.523 |   10.577 |
     +-------------------------------------------------------------------------------------------------------+
```

● Performance Evaluation

I. $x \times y \; mod \; q$ 簡化比較 ($r + r$ 都用$doubling$來實現)

Method	Mod Mul	Mod Add & Sub
$MM(MM(x,y), R^2 \; mod \; q)$	10754	2776
快速 mod	4691	3237

II. Double and Add 與 Sliding Window 演算法的比較

因為在使用 Sliding window 時，會需要存下 P3, P5, P7 的 LUT，所以

面積比較大一點

	Algo	SYN Area	Num of Cycle	Clock Period	Area*Time
Multiplier = 4 cycle	Double and Add	1.8860	8088	10	152539.6800
	Sliding Window	2.0985	7089	10	148764.0828

	Algo	SYN Area	Num of Cycle	Clock Period	Area*Time
Multiplier = 1 cycle	Double and Add	2.0766	5312	10	11031.00544
	Sliding Window	2.2334	4599	10	10455.3666

III. 與 Baseline 比較

	Layout Area	Num of Cycle	Clock Period (ns)	Area*Time
Baseline	3.790503	732086	10	27749741.79
Our method	2.985462	4599	10	13730.14231

IV. Layout 前後比較

	Layout Area	Num of Cycle	Clock Period (ns)	Area*Time
Before Layout	2.035552	4599	10	93,615.03648
After Layout	2.985462	4599	10	13730.14231