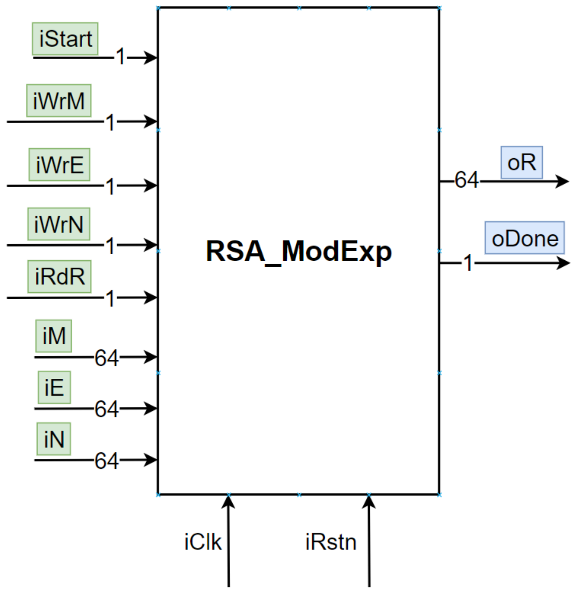
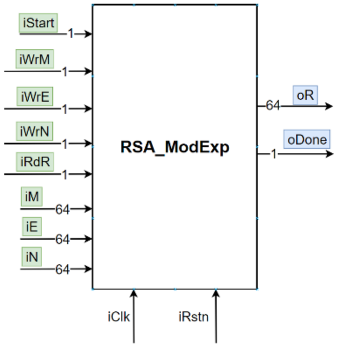
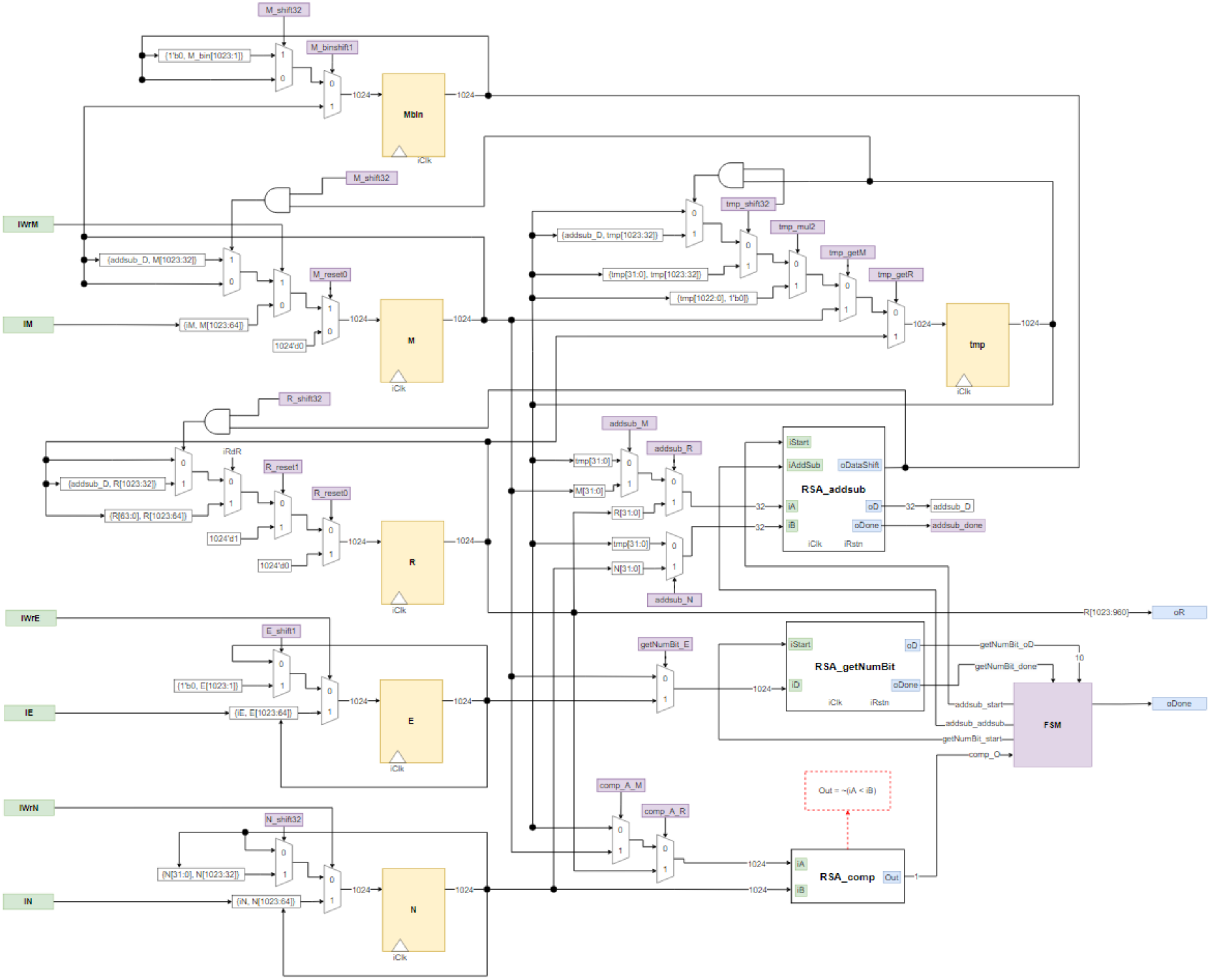
RSA
DIAGRAMS
and STATE MACHINE



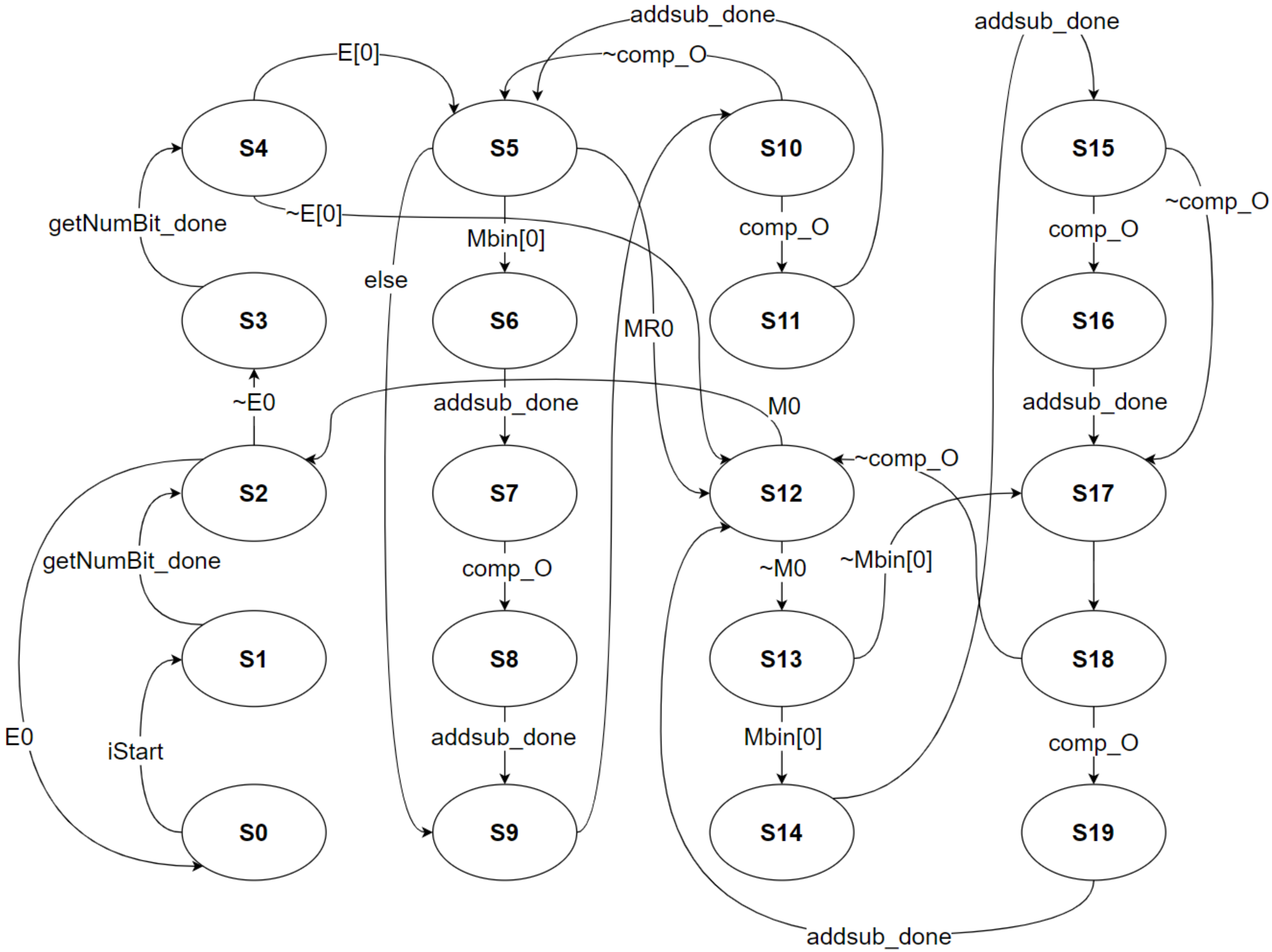
PIN	DIR	WIDTH	Description
Control signals			
iClk	Input	1	Clock
iRstn	Input	1	Reset low
iStart	Input	1	Start computing
iWrM	Input	1	Write M
iWrE	Input	1	Write E
iWrN	Input	1	Write N
iRdR	Input	1	Read Result
Input Data			
iM	Input	64	M
iE	Input	64	E
iN	Input	64	N
Output Data			
oR	Output	64	Result
oDone	Output	1	Finish computing





Submodule	File Name
RSA_addsub	RSA_addsub.v
RSA_getNumBit	RSA_getNumBit.v
RSA_comp	RSA_comp.v

Name	File Name
RSA_ModExp	RSA_ModExp.v



Finite State Machine

FSM Signals

RESET

```
oDone = 1’b0
State = 5’d0
M_reset0 = 1’b0
M_shift32 = 1’b0
Mbin_update = 1’b0
Mbin_shift1 = 1’b0
E_shift1 = 1’b0
N_shift32 = 1’b0
R_reset0 = 1’b0
R_reset1 = 1’b0
R_shift32 = 1’b0
tmp_getR = 1’b0
tmp_getM = 1’b0
tmp_mul2 = 1’b0
tmp_shift32 = 1’b0
tmp_shift32_update = 1’b0
addsub_start = 1’b0
addsub_addsub = 1’b0
getNumBit_start = 1’b0
comp_A_R = 1’b0
comp_A_M = 1’b0
getNumBit_E = 1’b0
addsub_R = 1’b0
addsub_M = 1’b0
addsub_N = 1’b0
lenE = 11’d0
lenM = 11’d0
```

STATE0

```
if (iStart) begin
     State = 5’d1
     getNumBit_start = 1’b1
     getNumBit_E = 1’b1
else
     State = State
```

STATE1

```
getNumBit_start = 1’b0
if(getNumBit_done)
     lenE = getNumBit_oD
     R_reset1 = 1
     State = 5’d2
else
     State = State
```

STATE2

```
R_reset1 = 1’b0
if (lenE = 11’b0)
     oDone = 1’b1
     State = 5’d0
else
     getNumBit_start = 1’b1
     getNumBit_E = 1’b0
     State = 5’d3
```

STATE3

```
getNumBit_start = 1’b0
if (getNumBit_done)
     lenM = getNumBit_oD
     lenMR = getNumBit_oD
     Mbin_update = 1’b1
     State = 5’d4
else
     State = State
```

STATE4

```
E_shift1 = 1’b1
if (E[0])
     Mbin_update = 1’b0
     tmp_getR = 1’b1
     R_reset0 = 1’b1
     State = 5’d5
else
     Mbin_update = 1’b1
     tmp_getR = 1’b1
     M_reset0 = 1’b1
     State = 5’d12
```

STATE5

```
E_shift1 = 1’b0
tmp_getR = 1’b0
R_reset0 = 1’b0
if (lenMR = 11’d0)
     Mbin_update = 1’b1
     tmp_getM = 1’b1
     M_reset0 = 1’b1
     State = 5’d12
else
```

```
    Mbin_shift1 = 1’b1
    if(Mbin[0])
        addsub_start = 1’b1
        addsub_addusb =
1’b1
        addsub_R = 1’b1
        addsub_N = 1’b0
        R_shift32 = 1’b1
        tmp_shift32 = 1’b1
        State = 5’d6
    else
        tmp_mul2 = 1’b1
        State = 5’d9
          STATE6
Mbin_shift1 = 1’b0
addsub_start = 1’b0
if (addsub_done)
    R_shift32 = 1’b0
    tmp_shift32 = 1’b0
    comp_A_R = 1’b1
    State = 5’d7
else
    State = State
          STATE7
if (comp_O)
    addsub_start = 1’b1
    addsub_addsub = 1’b1
    addsub_R = 1’b1
    addsub_N = 1’b1
    R_shift32 = 1’b1
```

```
    N_shift32 = 1’b1
    State = 5’d8
else
    tmp_mul2 = 1’b1
    State = 5’d9
          STATE8
addsub_start = 1’b0
if (addsub_done)
    R_shift32 = 1’b0
    N_shift32 = 1’b0
    tmp_mul2 = 1’b1
    State = 5’d9
else
    State = State
          STATE9
Mbin_shift1 = 1’b0
tmp_mul2 = 1’b0
comp_A_R = 1’b0
comp_A_M = 1’b0
State = 5’d10
          STATE10
if (comp_O)
    addsub_start = 1’b1
    addsub_addsub = 1’b1
    addsub_R = 1’b0
    addsub_M = 1’b0
    addsub_N = 1’B1
    tmp_shift32_update =
1’b1
    N_shift32 = 1’b1
```

```
    State = 5’d11
else
    lenMR = lenMR – 1’b1
    State = 5’d5
          STATE11
addsub_start = 1’b0
if (addsub_done)
    tmp_shift32_update =
1’b0
    N_shift32 = 1’b0
    lenMR = len MR – 1’b1
    State = 5’d5
else
    State = State
          STATE12
E_shift1 = 1’b0
Mbin_update = 1’b0
tmp_getM = 1’b0
M_reset0 = 1’b0
if (lenM = 11’d0)
    lenE = lenE – 1’b1
    State = 5’d2
else
    State = 5’d13
          STATE13
Mbin_shift1 = 1’b1
if (Mbin[0])
    addsub_start = 1’b1
    addsub_addsub = 1’b0
    addsub_R = 1’b0
    addsub_M = 1’b1
    addsub_N = 1’b0
    M_shift32 = 1’b1
    tmp_shift32 = 1’b1
    State = 5’d14
else
    tmp_mul2 = 1’b1
    State = 5’d17
```

STATE14

```
Mbin_shift1 = 1’b0
addsub_start = 1’b0
if (addsub_done)
    M_shift32 = 1’b0
    tmp_shift32 = 1’b0
    comp_A_R = 1’b0
    comp_A_M = 1’b1
    State = 5’d15
else
    State = State
```

STATE15

```
if(comp_O)
    addsub_start = 1’b1
    addsub_addsub = 1’b1
    addsub_R = 1’b0
    addsub_M = 1’b1
    addsub_N = 1’b1
    M_shift32 = 1’b1
    N_shift32 = 1’b1
    State = 5’d16
else
    tmp_mul2 = 1’b1
    State = 5’d17
```

STATE16

```
addsub_start = 1’b0
if (addsub_done)
    M_shift32 = 1’b0
    N_shift32 = 1’b0
    tmp_mul2 = 1’b1
    State = 5’d17
else
    State = State
```

STATE17

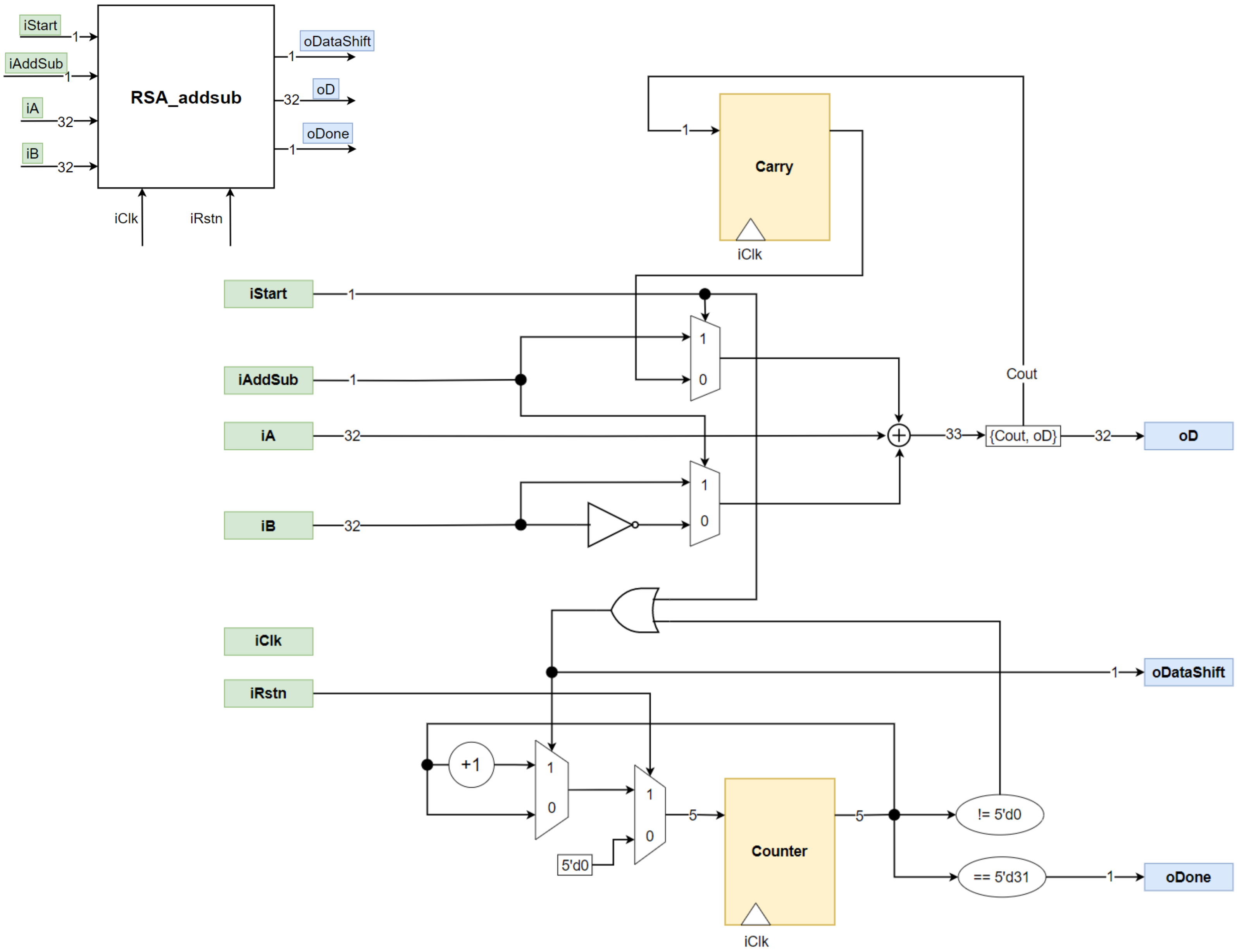
```
Mbin_shift1 = 1’b0
tmp_mul2 = 1’b0
comp_A_R = 1’b0
comp_A_M = 1’b0
State = 5’d18
```

STATE18

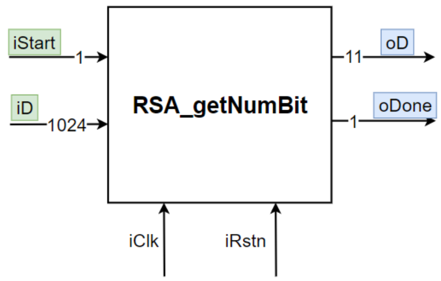
```
if (comp_O)
    addsub_start = 1’b1
    addsub_addsub = 1’b1
    addsub_R = 1’b1
    addsub_M = 1’b0
    addsub_N = 1’b1
    tmp_shift32_update = 1’b1
    N_shift32 = 1’b1
    State = 5’d19
else
    lenM = lenM – 1’b1
    State = 5’d12
```

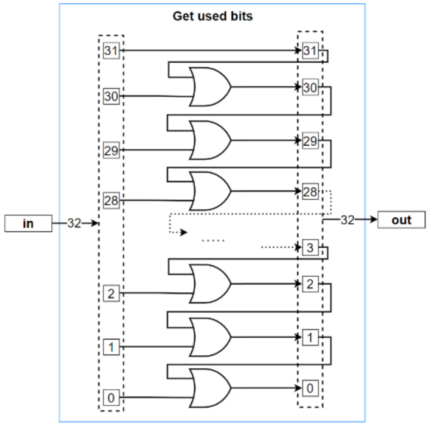
STATE19

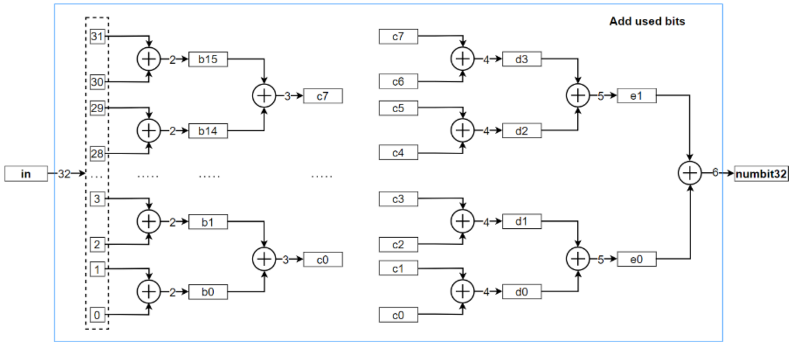
```
addsub_start = 1’b0
if (addsub_done)
    tmp_shift32_update = 1’b0
    N_shift32 = 1’b0
    lenM = lenM – 1’b1
    State = 5’d12
else
    State = State
```

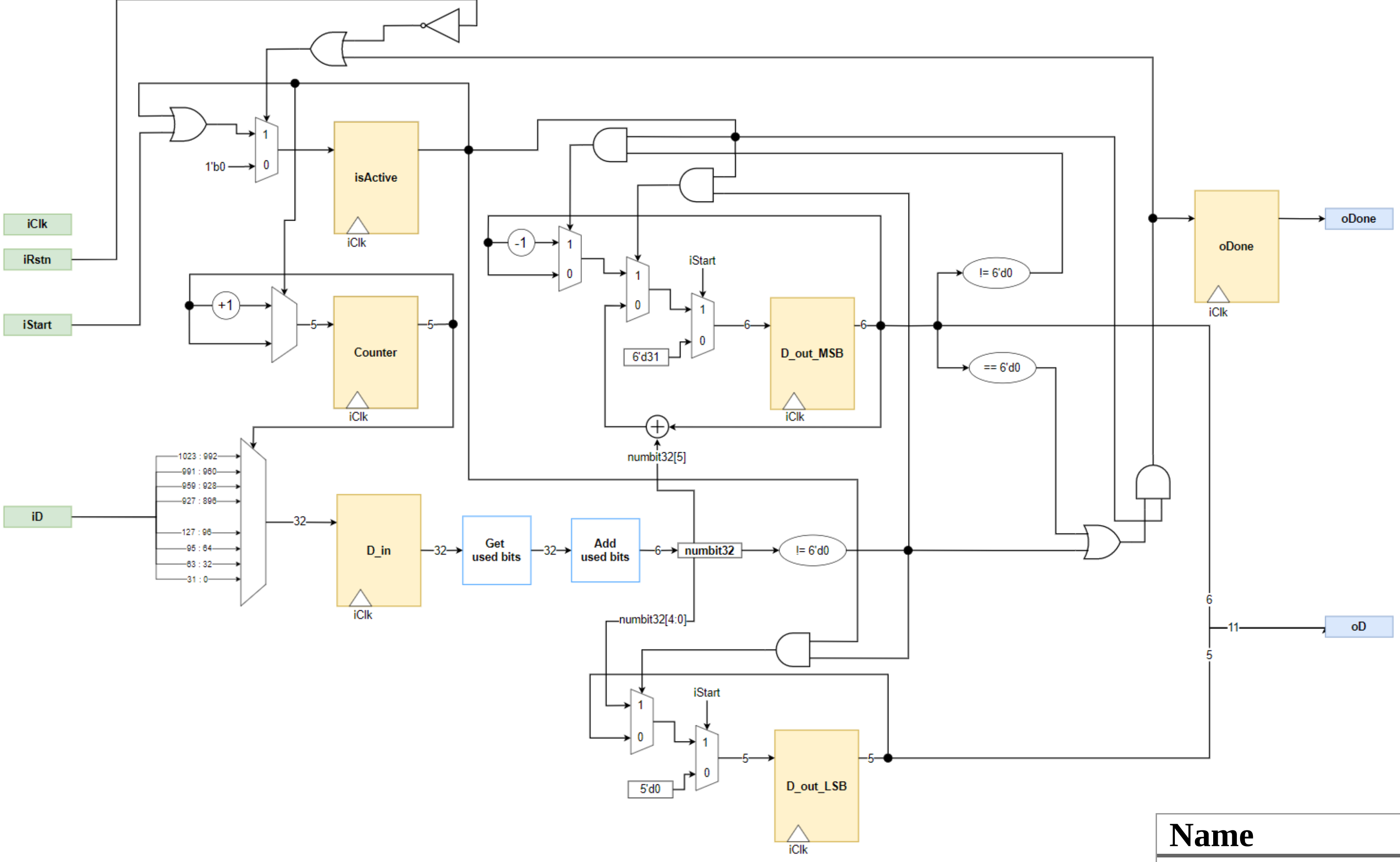


Name	File Name
RSA_addsub	RSA_addsub.v









Name	File Name
RSA_getNumBit	RSA_getNumBit.v