BITS Pilani

Pilani Campus

# 8-bit Scalable Montgomery Multiplier mod 255 using Static CMOS technology

Presented by:
Gaurav Kumar(2025H1230128P)
Vignesh Kenche(2025H1230131P)

*Supervisor:*
*Dr. Nitin Chaturvedi*

# Objective

Design a scalable 8-bit Montgomery Modular Multiplier using static CMOS that performs (AxB) mod 255.

# Montgomery Modular Multiplier

- Very efficiently perform **(A x B) mod M** without using standard expensive division operation.
- Used in modern cryptography like RSA.
- **Montgomery Form:**
  - ➢ Choose R such that, R>M and *gcd*(R,M) = 1
  - ➢ X' = X.R mod M
- **Montgomery Arithmetic**(in Montgomery form)**:**
  - ➢ X'+y' = (X+Y)%M
  - ➢ X'.Y'.$R^{-1}$ = (X*Y)%M

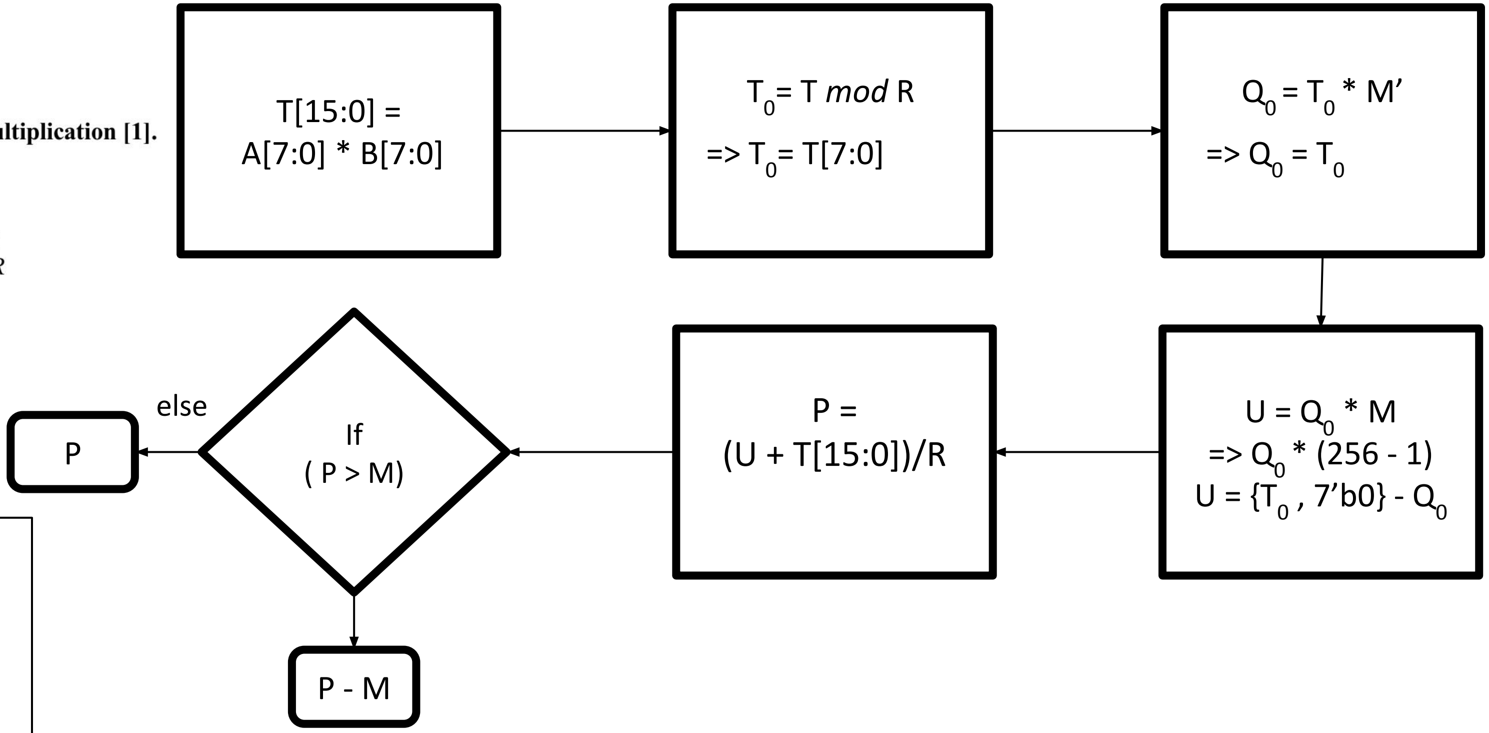
# Algorithm:

Input: Two 8-bit binary number(A, B)
Output: $P = ABR^{-1} \bmod M$

**Algorithm 1. Montgomery Multiplication [1].**

```
Input:   $A, B$
Output:  $P = ABR^{-1} \bmod M$

1. $T = AB$              $T_0 = T \bmod R$
2. $Q = T_0M'$           $Q_0 = Q \bmod R$
3. $U = Q_0M$
4. $P = (T + U) / R$
5. if ($P > M$):
6.         $P = P - M$
7. end if
8. return $P$
```



R = 256
M = 255
$M^{-1}$ = 255
M’ = 1

[1] T. J. Grale and E. E. Swartzlander, "Improved Montgomery Multiplication," *2023 IEEE 30th Symposium on Computer Arithmetic (ARITH)*, Portland, OR, USA, 2023, pp. 60-67, doi: 10.1109/ARITH58626.2023.00019.

# Schematic

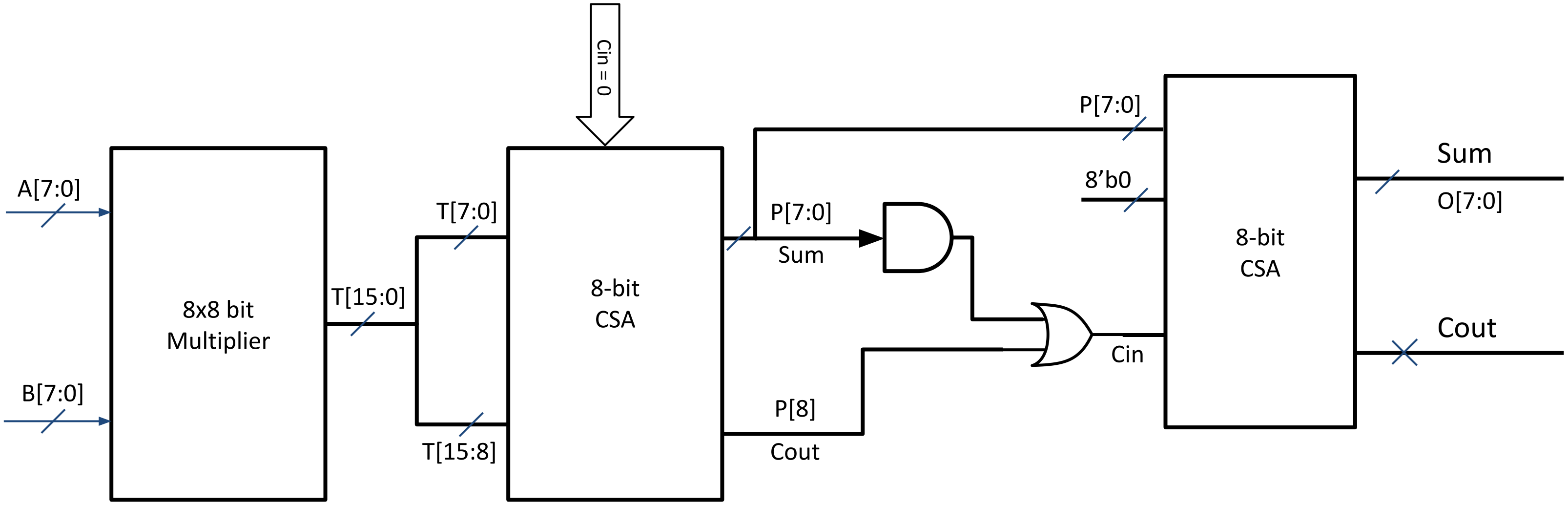


*Fig. 1: Schematic of 8-bit Montgomery modular multiplier (mod 255)*

# Schematic

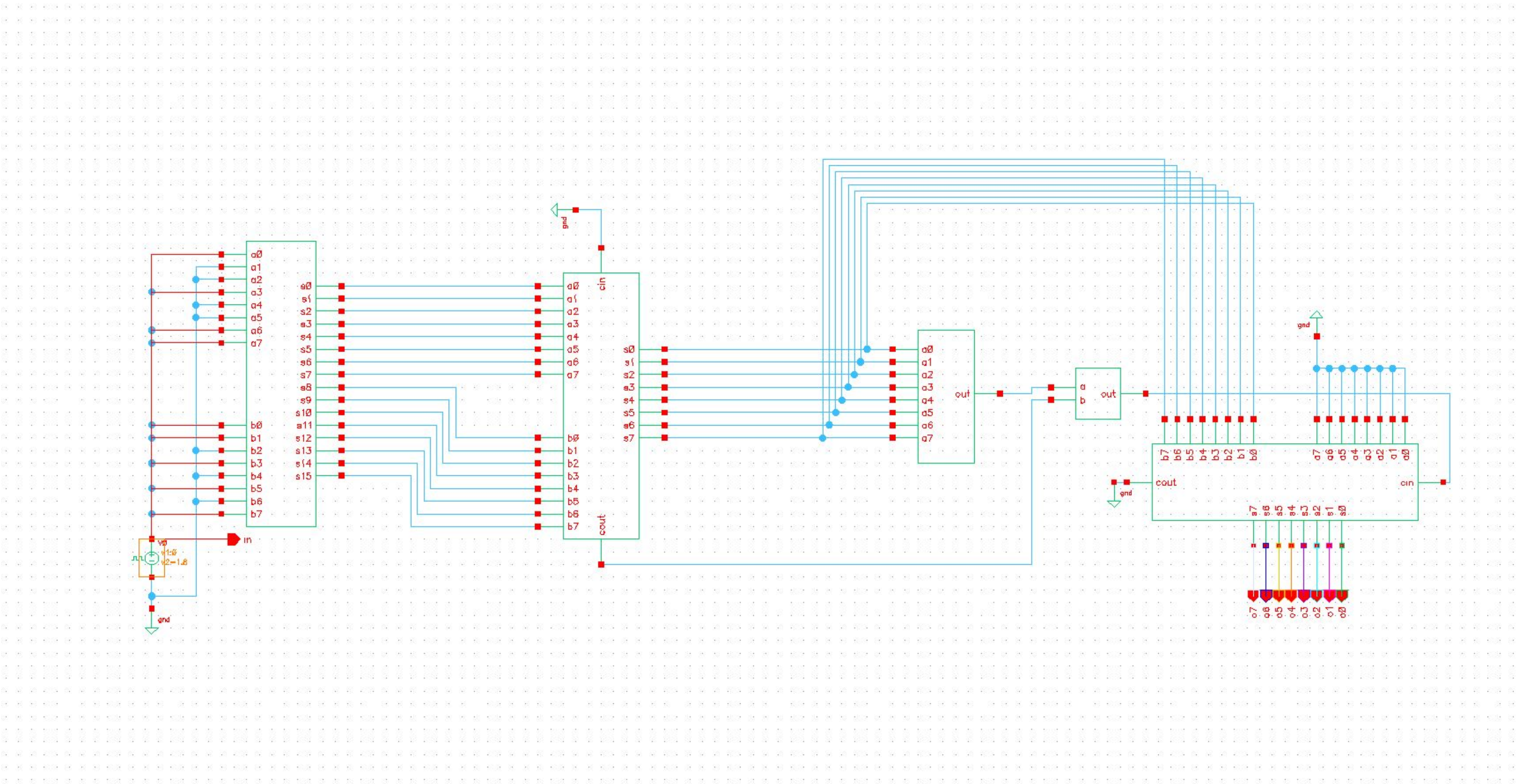


*Fig. 2: Schematic of 8-bit Montgomery modular multiplier in Cadence Virtuoso*

# Schematic

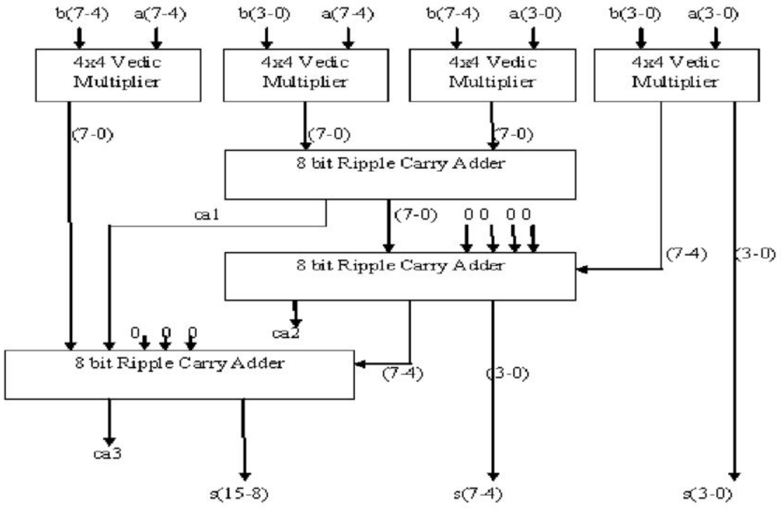


*Fig. 3: Schematic of 8-bit Multiplier using 4-bit Multiplier*

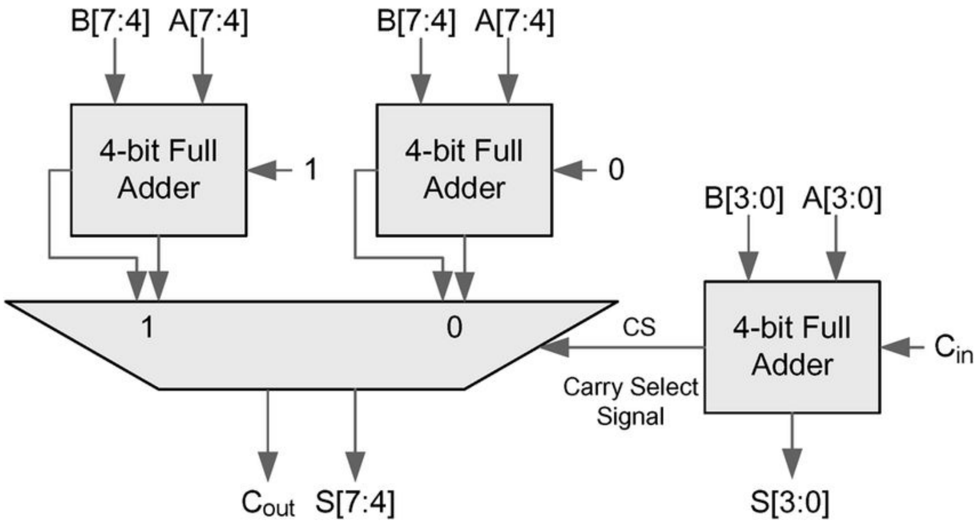


*Fig. 4: Schematic of 8-bit Carry Select Adder*

Source: Internet

# Schematic

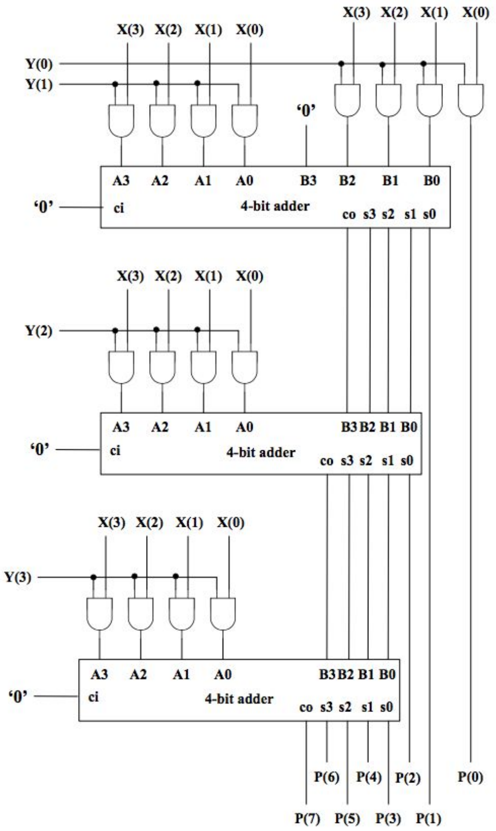


*Fig. 5: 4-bit Array Multiplier*

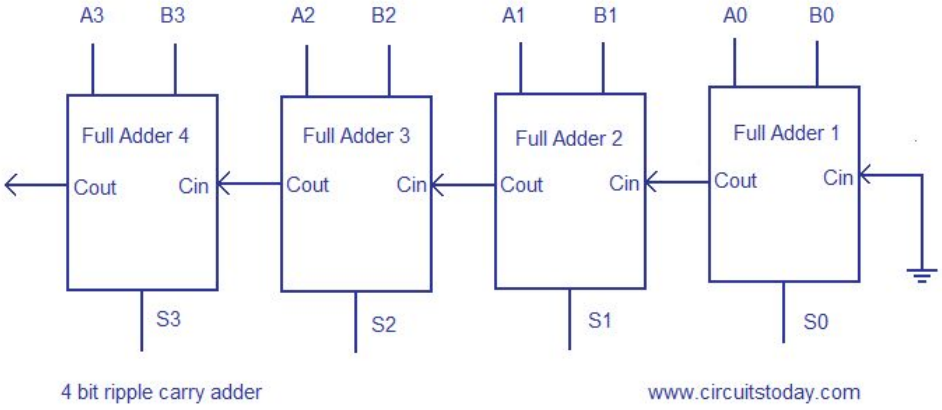


*Fig. 6: Schematic of 8-bit Carry Select Adder*

Source: Internet

# Output

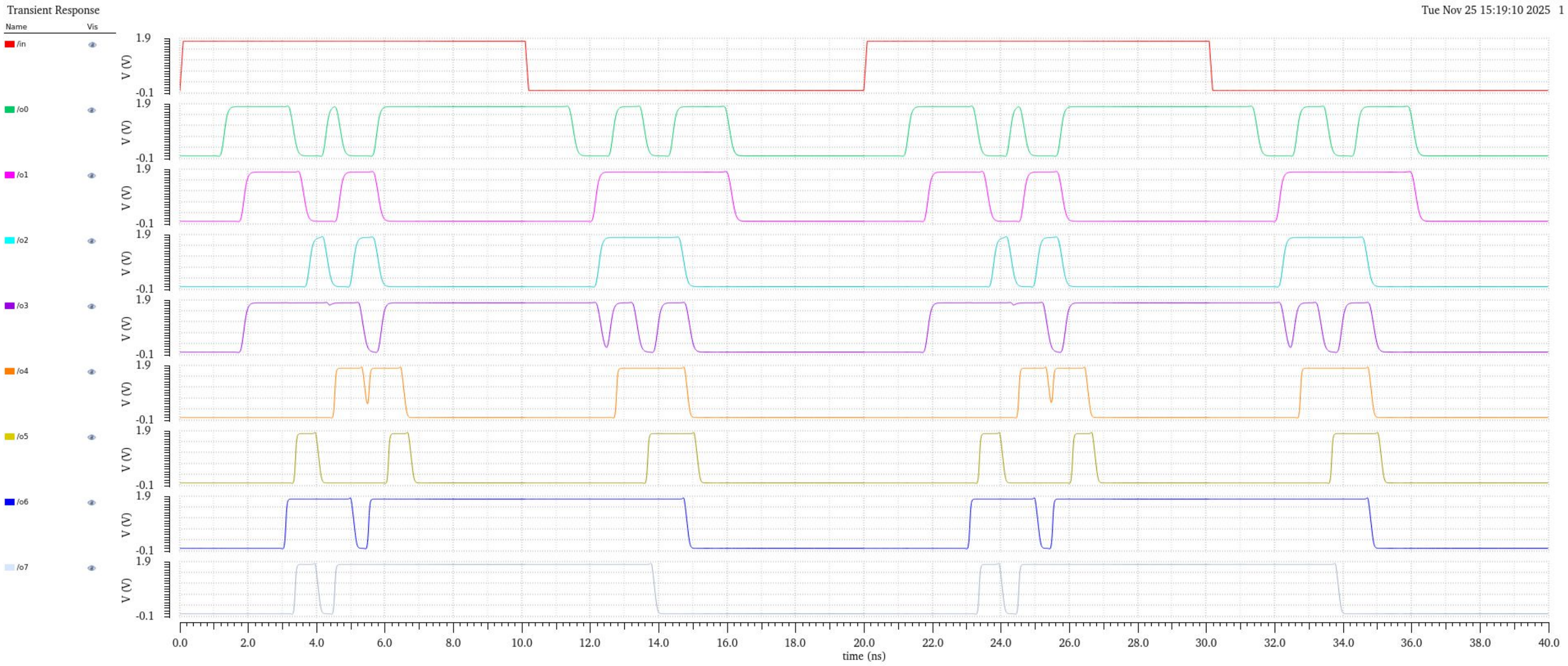


*Fig. 7: Transient characteristics of our Modular multiplier with 8 bit output*

# Results

| | Parameter | Value |
|---|---|---|
| 1. | Transistor Count | 6332 |
| 2. | Delay | 6.9169 ns |
| 3. | Average Power | 4.206 mW |
| 4. | Peak Power | 14.179 mW |
| 5. | Static Power | 1.01µW |

*Table 1: Performance Parameters*

# References:

[1] T. J. Grale and E. E. Swartzlander, "Improved Montgomery Multiplication," *2023 IEEE 30th Symposium on Computer Arithmetic (ARITH)*, Portland, OR, USA, 2023, pp. 60-67, doi: 10.1109/ARITH58626.2023.00019.

[2] A. P. Renardy, N. Ahmadi, A. A. Fadila, N. Shidqi and T. Adiono, "Hardware implementation of montgomery modular multiplication algorithm using iterative architecture," *2015 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Surabaya, Indonesia, 2015, pp. 99-102, doi: 10.1109/ISITIA.2015.7219961.

[3] Montgomery, Peter L.. “Modular multiplication without trial division.” Mathematics of Computation 44 (1985): 519-521.

innovate achieve lead

**BITS**

Pilani

Pilani Campus

# Thank You