FIG. 1A

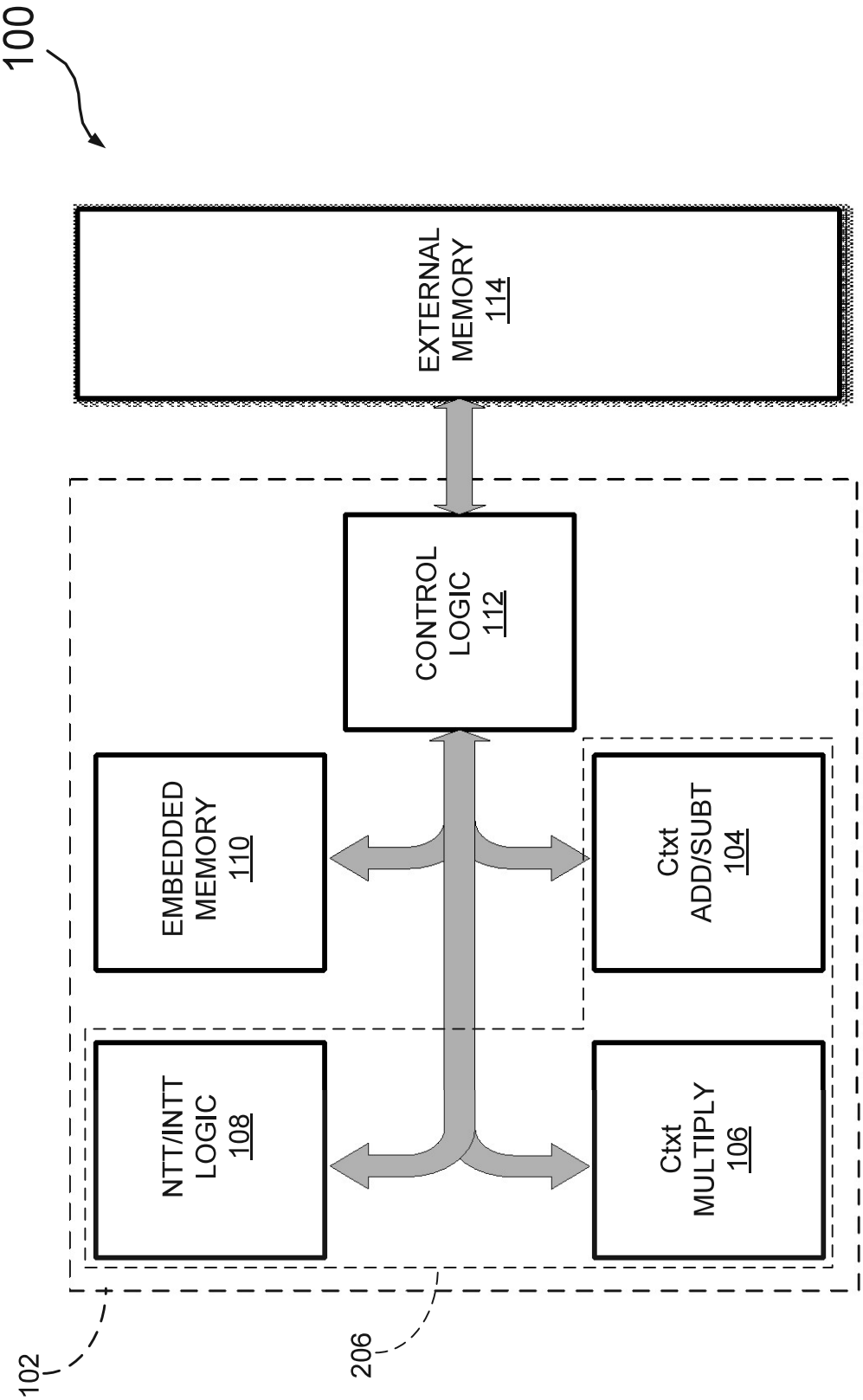
100
EXTERNAL MEMORY 114
CONTROL LOGIC 112
EMBEDDED MEMORY 110
Ctxt ADD/SUBT 104
NTT/INTT LOGIC 108
Ctxt MULTIPLY 106
102
206

FIG. 1B

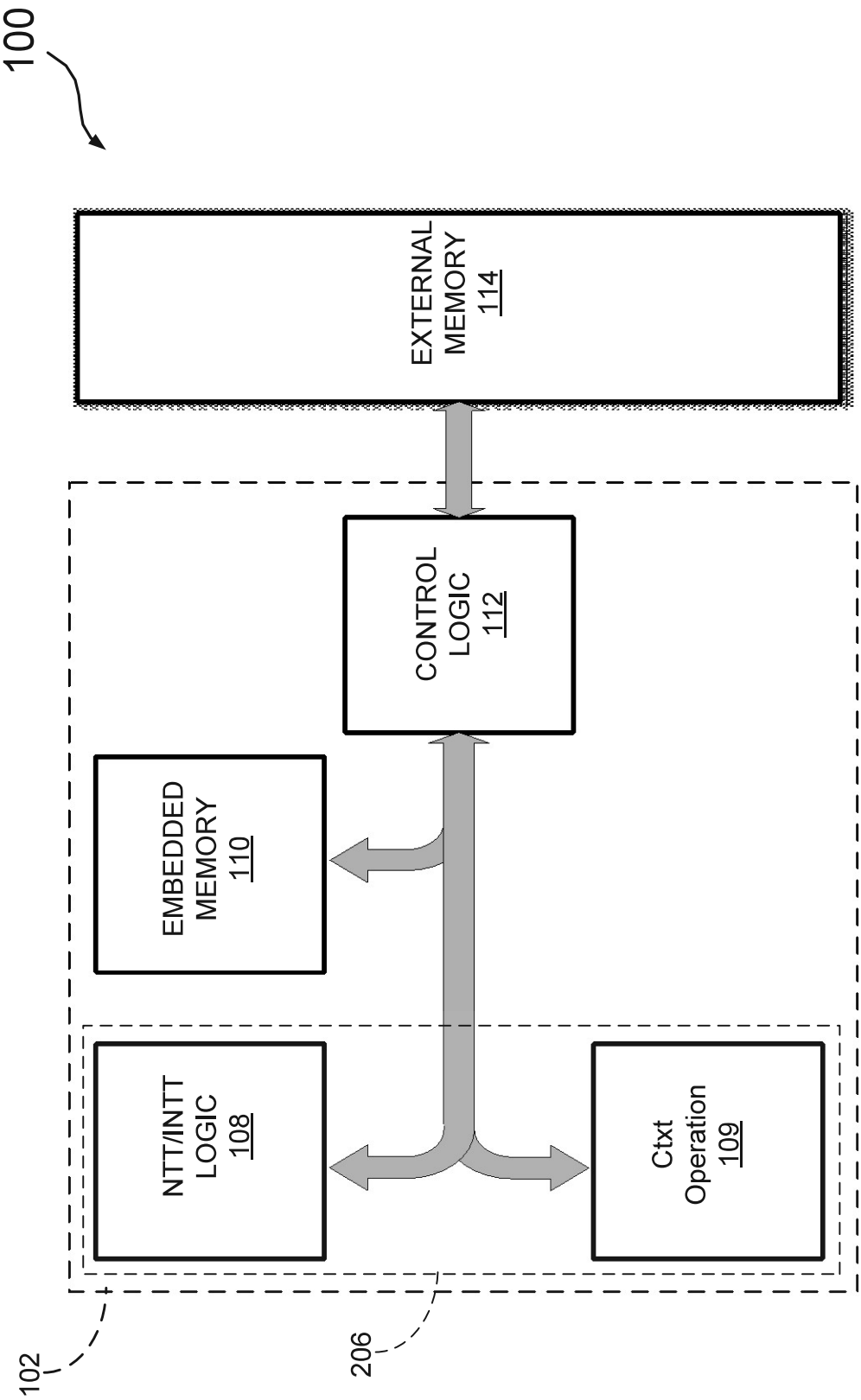
100
EXTERNAL MEMORY 114
CONTROL LOGIC 112
EMBEDDED MEMORY 110
NTT/INTT LOGIC 108
Ctxt Operation 109
102
206

FIG. 1C

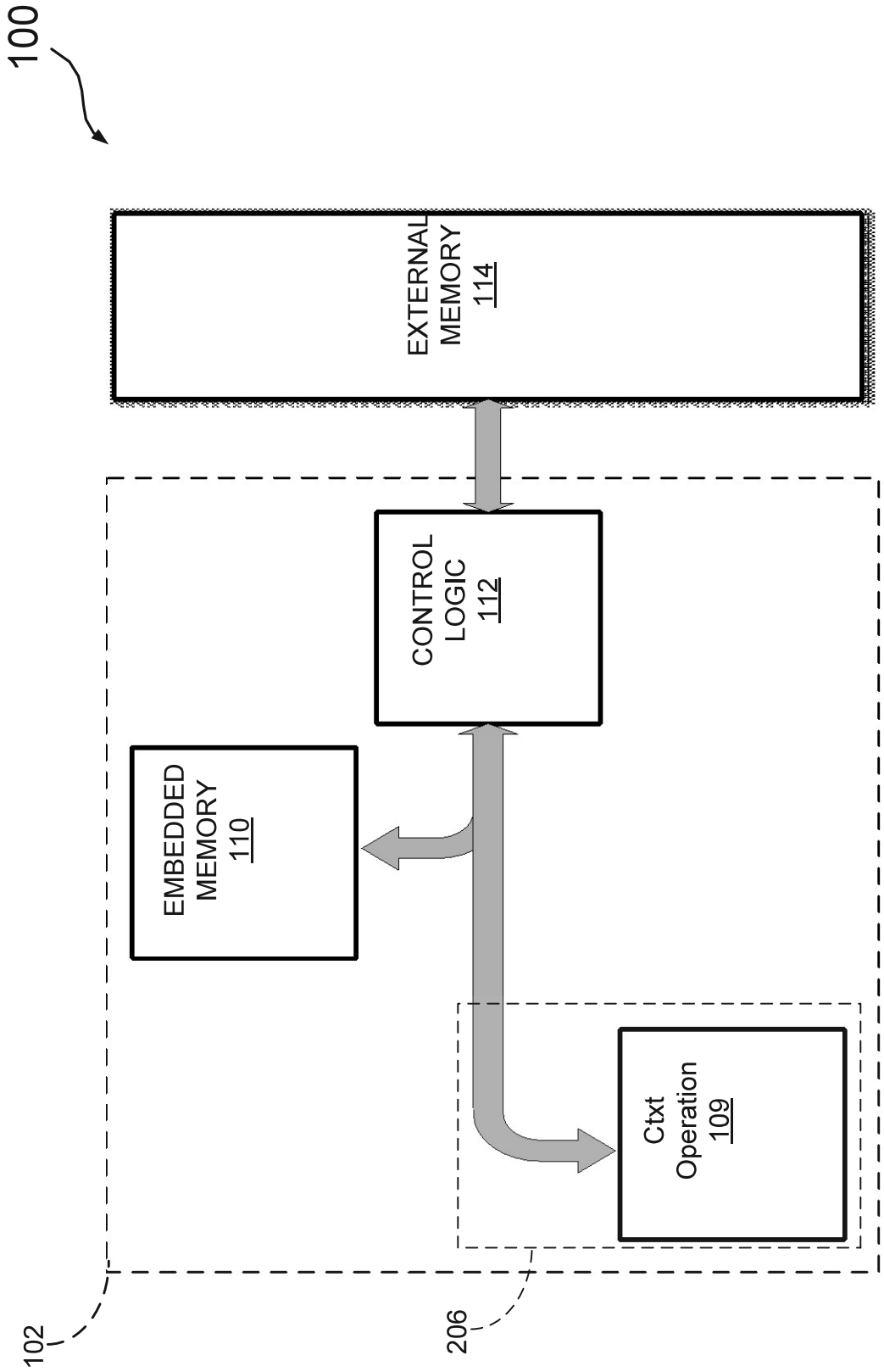
100
EXTERNAL MEMORY 114
CONTROL LOGIC 112
EMBEDDED MEMORY 110
Ctxt Operation 109
102
206

FIG. 2

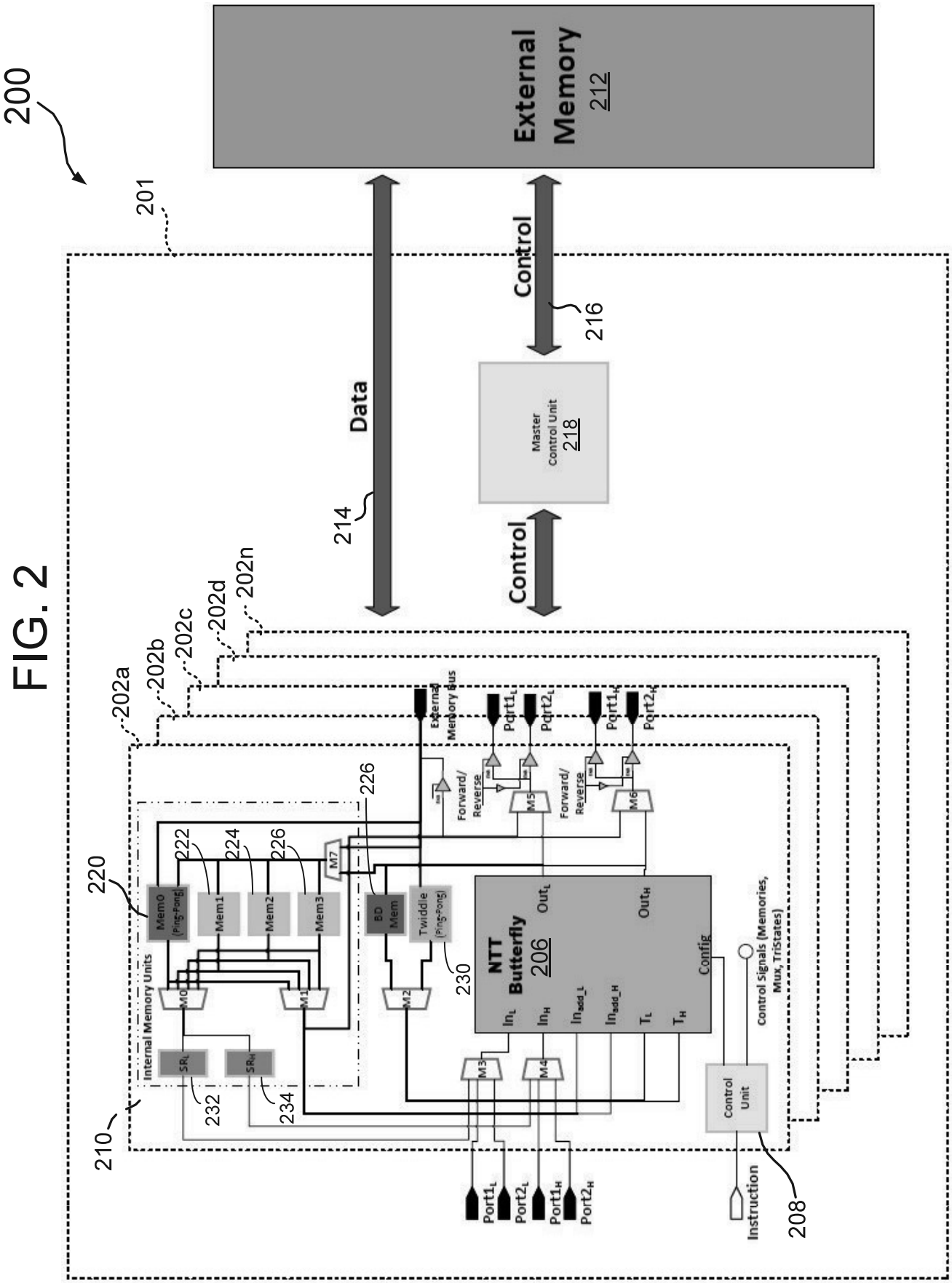
200
201
External Memory
212
Data
214
Control
216
Master Control Unit
218
Control
202a
202b
202c
202d
202n
220
210
External Memory Bus
Port1L
Port2L
Port1H
Port2H
Forward/ Reverse
M5
M6
M7
226
222
224
Mem0 (Ping-Pong)
Mem1
Mem2
Mem3
BD Mem
Twiddle (Ping-Pong)
230
Internal Memory Units
M0
M1
M2
SRL
SRH
232
234
NTT Butterfly 206
InL
InH
Inadd_L
Inadd_H
TL
TH
OutL
OutH
Config
M3
M4
Control Unit
Control Signals (Memories, Mux, TriStates)
Instruction
208

FIG. 3

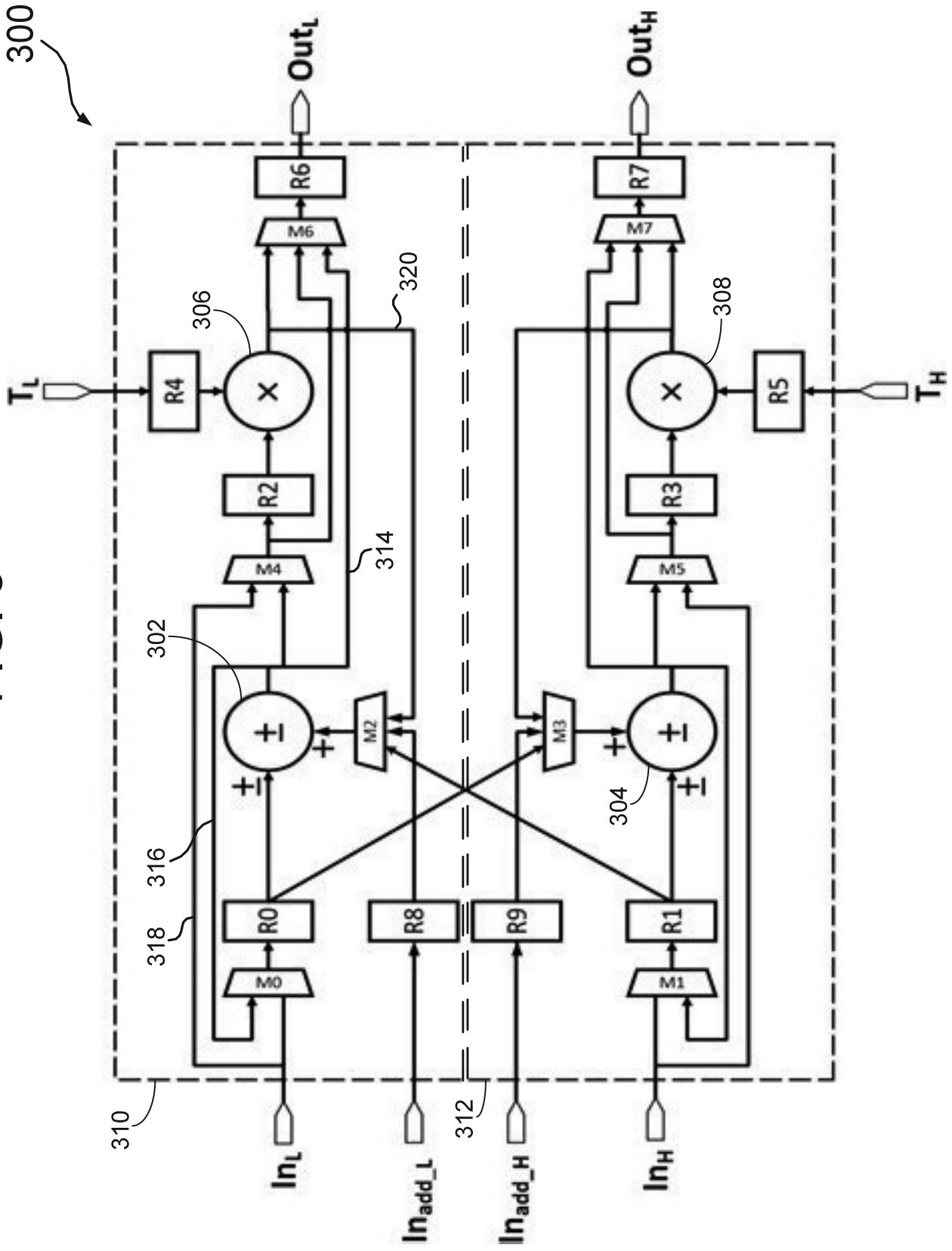
300
Out_L
Out_H
R6
R7
M6
M7
320
306
308
T_L
R4
R5
T_H
R2
R3
M4
M5
314
302
M2
M3
304
316
318
R0
R8
R9
R1
M0
M1
310
312
In_L
In_{add_L}
In_{add_H}
In_H

FIG. 4

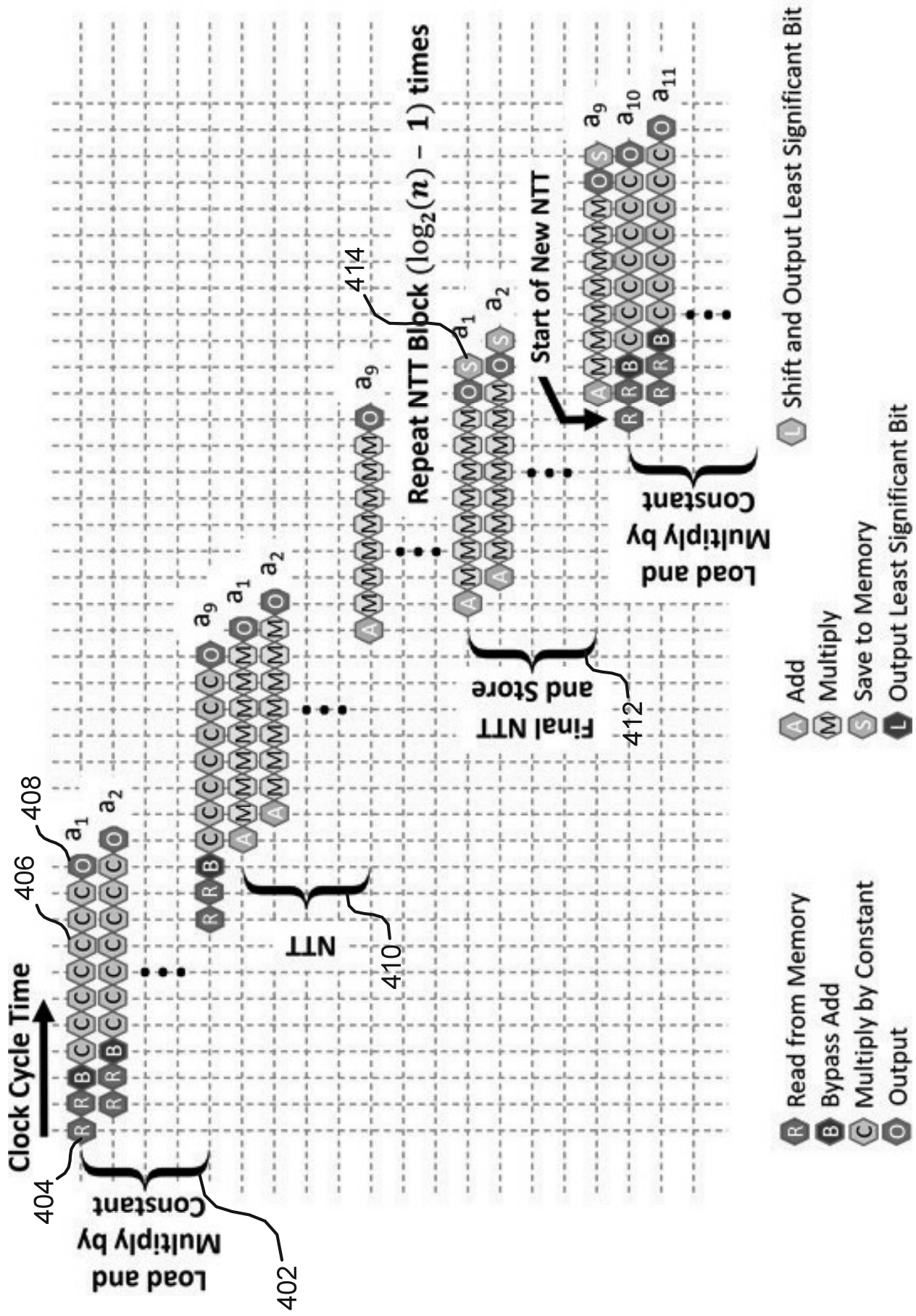
Clock Cycle Time
404
Load and Multiply by Constant
402
406
408
410
NTT
414
Repeat NTT Block $(\log_2(n) - 1)$ times
412
Final NTT and Store
Start of New NTT
Load and Multiply by Constant
Read from Memory
Bypass Add
Multiply by Constant
Output
Add
Multiply
Save to Memory
Output Least Significant Bit
Shift and Output Least Significant Bit

FIG. 5

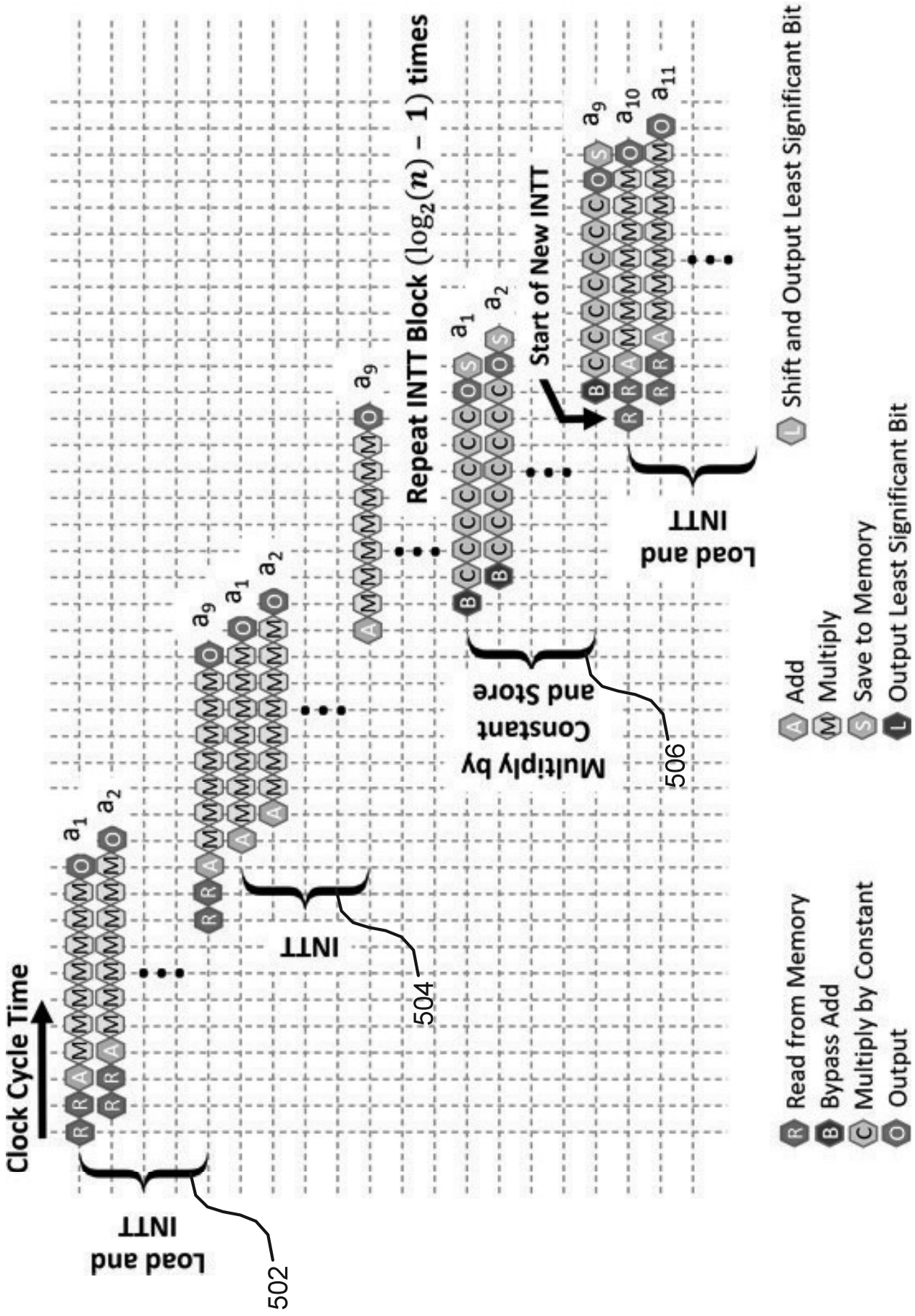
Clock Cycle Time
Load and INTT
INTT
Repeat INTT Block $(\log_2(n) - 1)$ times
Multiply by Constant and Store
Start of New INTT
Load and INTT
502
504
506
Read from Memory
Bypass Add
Multiply by Constant
Output
Add
Multiply
Save to Memory
Output Least Significant Bit
Shift and Output Least Significant Bit

FIG. 6

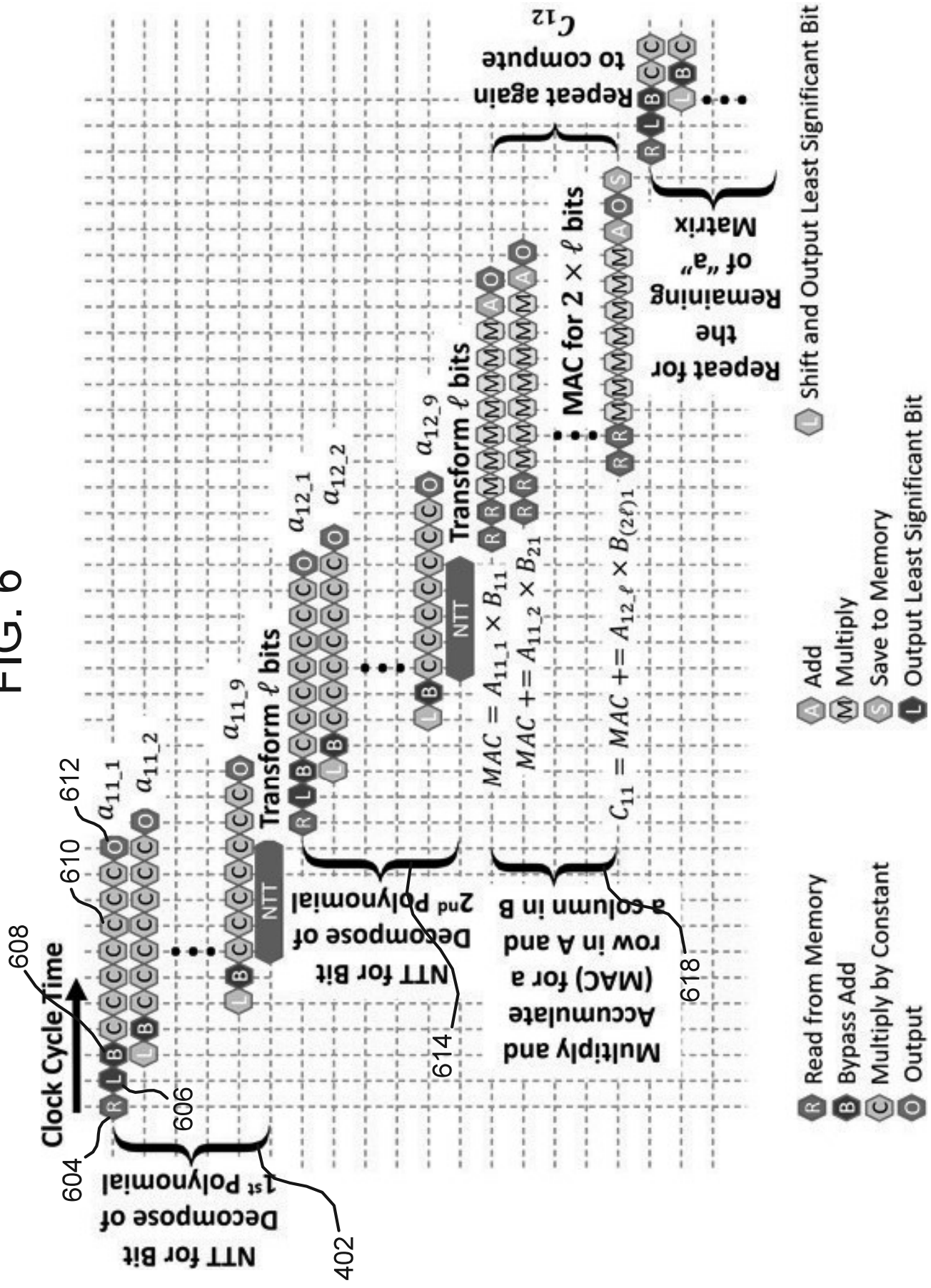
Clock Cycle Time
608
604
606
610
612
614
618
402
NTT for Bit Decompose of 1st Polynomial
Transform ℓ bits
NTT for Bit Decompose of 2nd Polynomial
Transform ℓ bits
Multiply and Accumulate (MAC) for a row in A and a column in B
MAC for 2 × ℓ bits
Repeat for the Remaining of "a" Matrix
Repeat again to compute C12
Read from Memory
Bypass Add
Multiply by Constant
Output
Add
Multiply
Save to Memory
Output Least Significant Bit
Shift and Output Least Significant Bit

FIG. 7

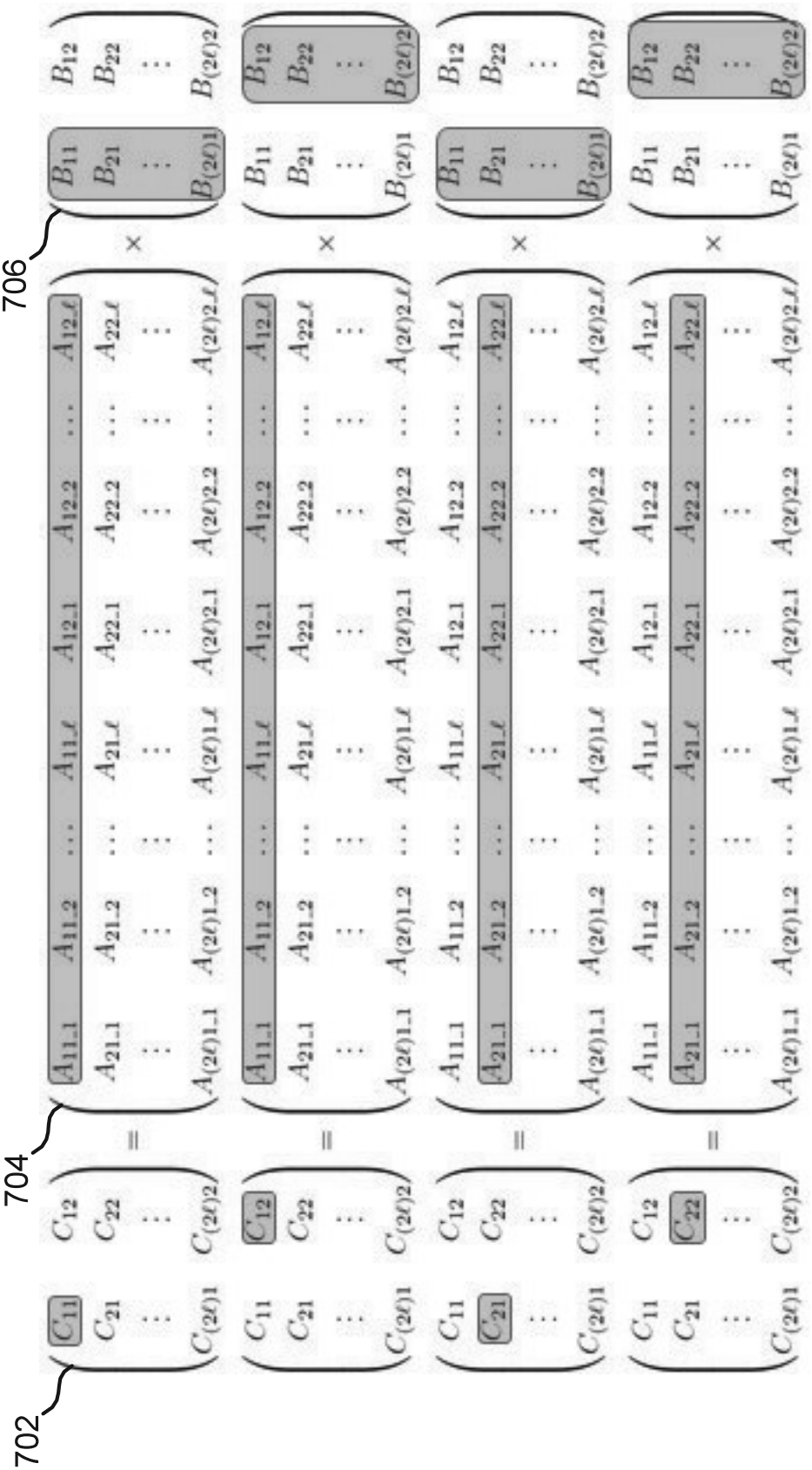

FIG. 8

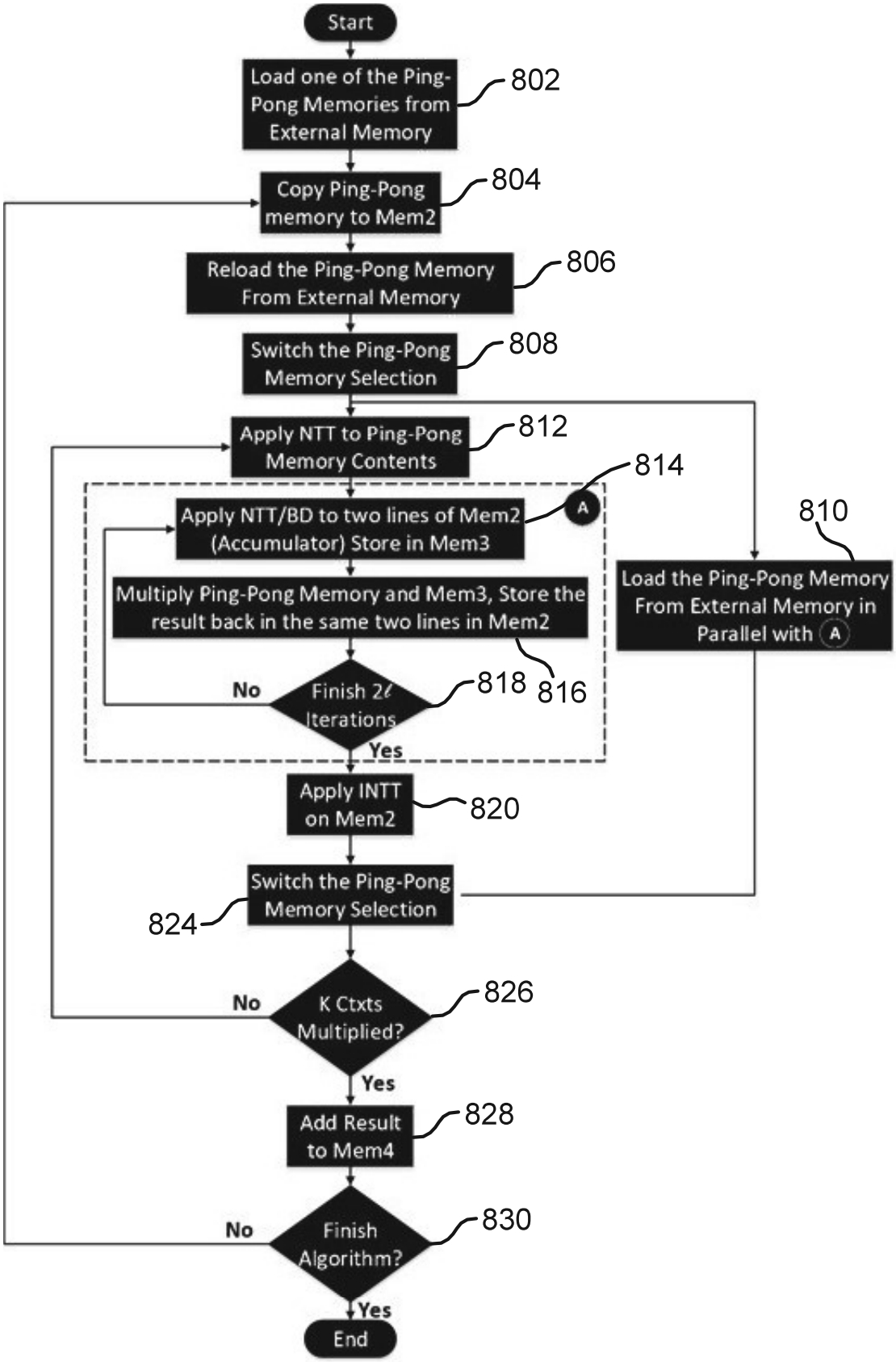
Start
Load one of the Ping-Pong Memories from External Memory
802
Copy Ping-Pong memory to Mem2
804
Reload the Ping-Pong Memory From External Memory
806
Switch the Ping-Pong Memory Selection
808
Apply NTT to Ping-Pong Memory Contents
812
814
Apply NTT/BD to two lines of Mem2 (Accumulator) Store in Mem3
A
Multiply Ping-Pong Memory and Mem3, Store the result back in the same two lines in Mem2
816
No
Finish 2ℓ Iterations
818
Yes
810
Load the Ping-Pong Memory From External Memory in Parallel with A
Apply INTT on Mem2
820
Switch the Ping-Pong Memory Selection
824
No
K Ctxts Multiplied?
826
Yes
Add Result to Mem4
828
No
Finish Algorithm?
830
Yes
End

FIG. 9

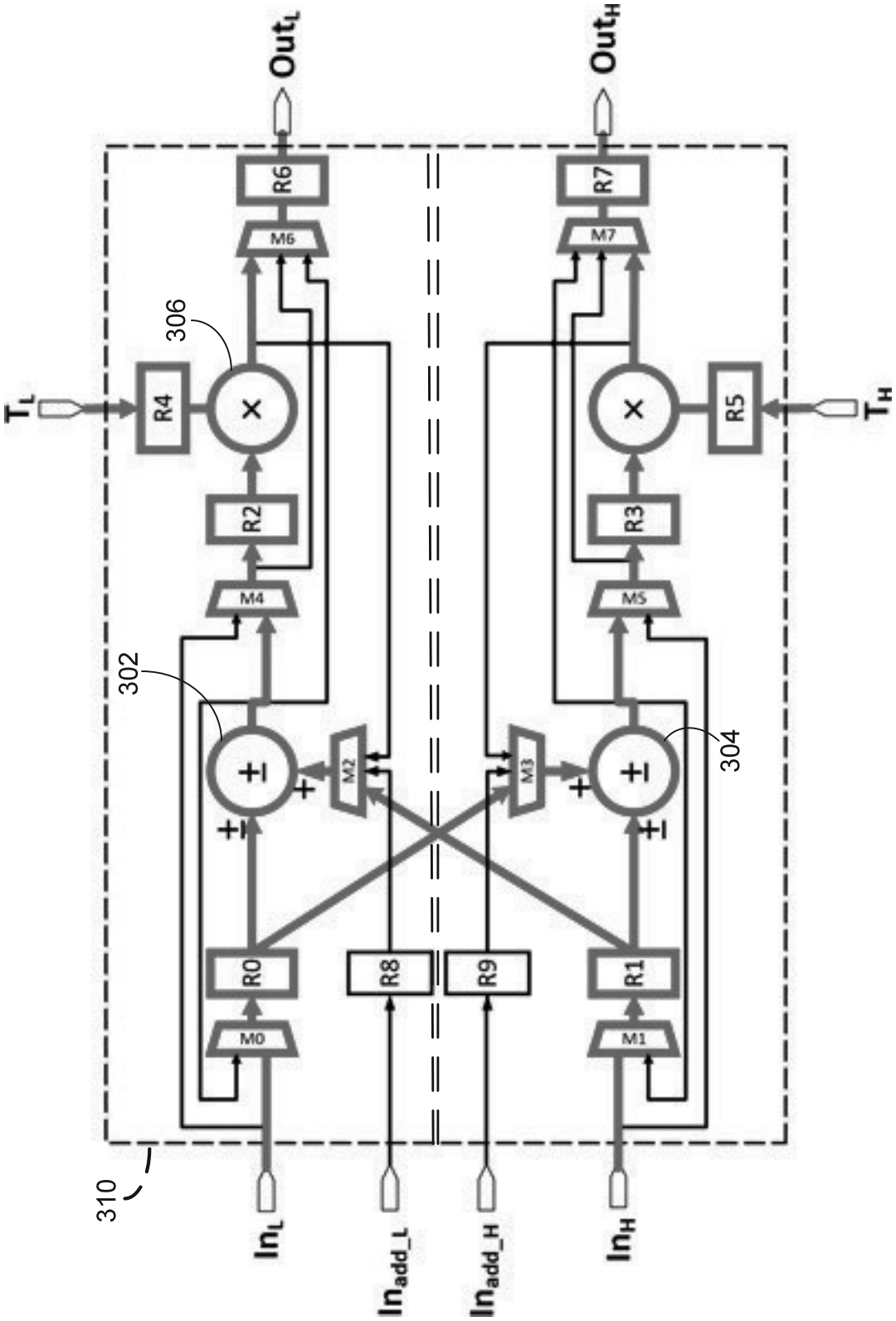
Out_L
Out_H
R6
R7
M6
M7
306
T_L
R4
R5
T_H
R2
R3
M4
M5
302
304
M2
M3
R0
R8
R9
R1
M0
M1
310
In_L
In_add_L
In_add_H
In_H

FIG. 10

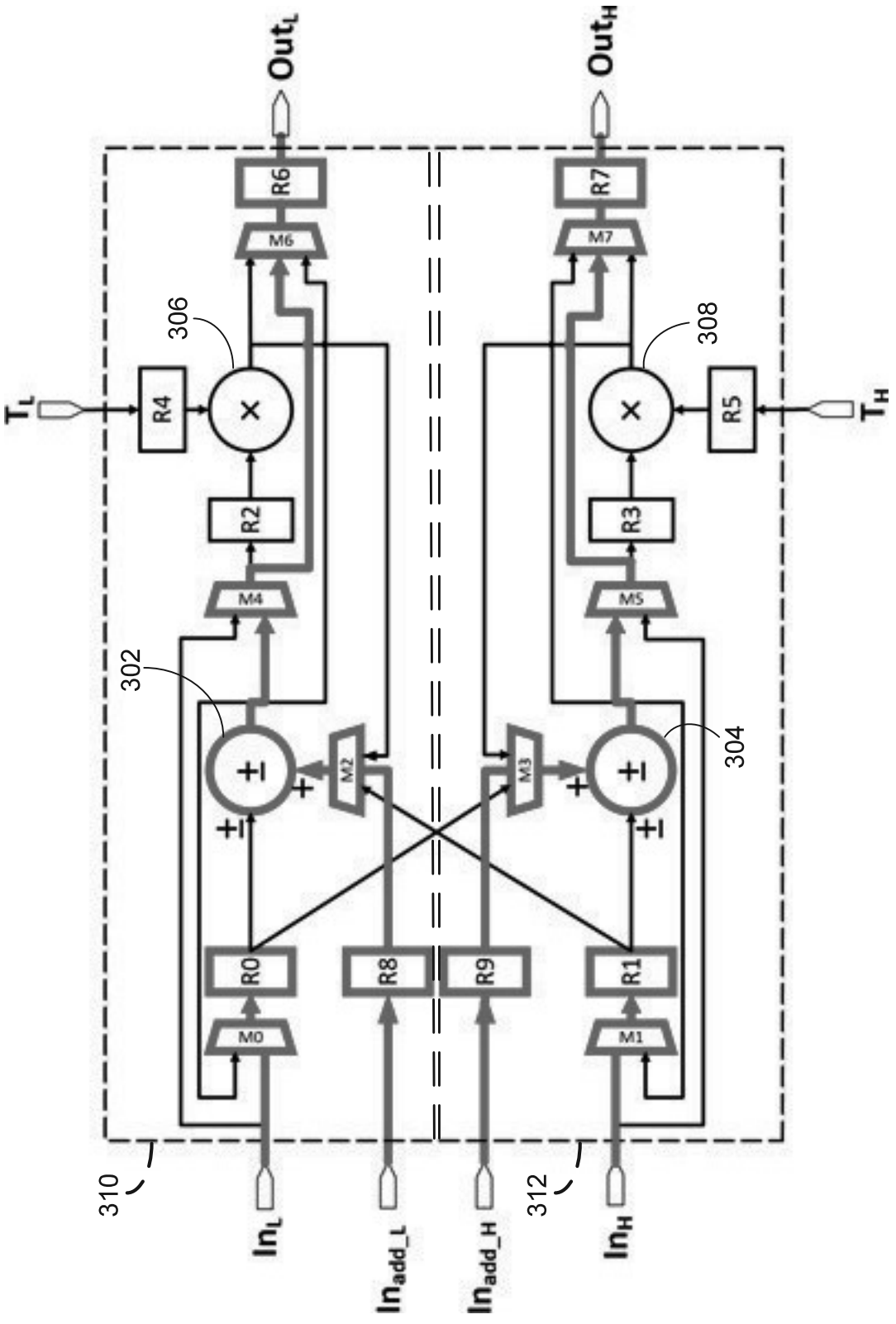
Out_L
Out_H
R6
R7
M6
M7
306
308
T_L
R4
R5
T_H
R2
R3
M4
M5
302
304
M2
M3
R0
R8
R9
R1
M0
M1
310
312
In_L
In_add_L
In_add_H
In_H

FIG. 11

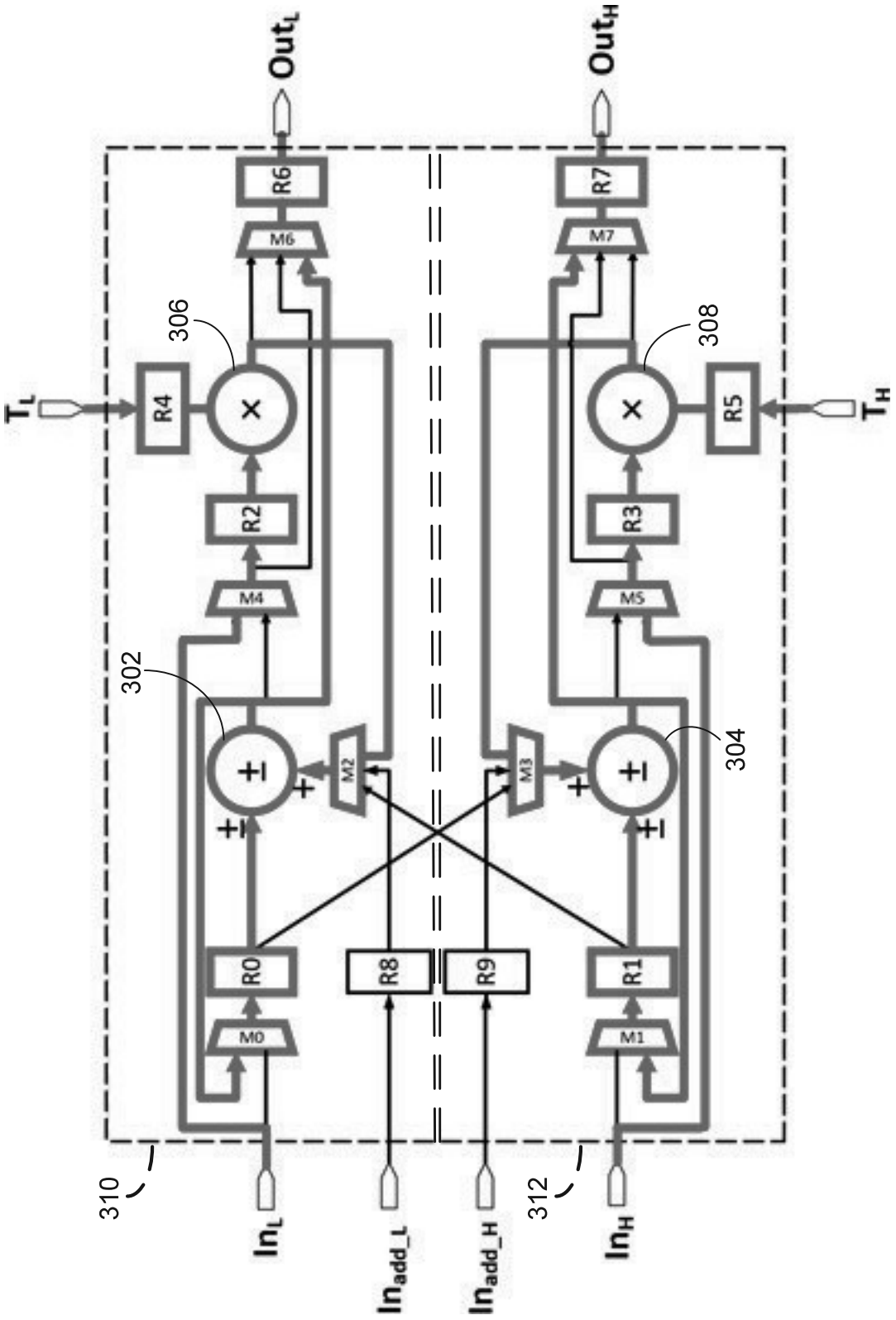
Out_L
Out_H
R6
R7
M6
M7
306
308
T_L
R4
R5
T_H
R2
R3
M4
M5
302
304
M2
M3
R0
R8
R9
R1
M0
M1
310
312
In_L
In_add_L
In_add_H
In_H

FIG. 12

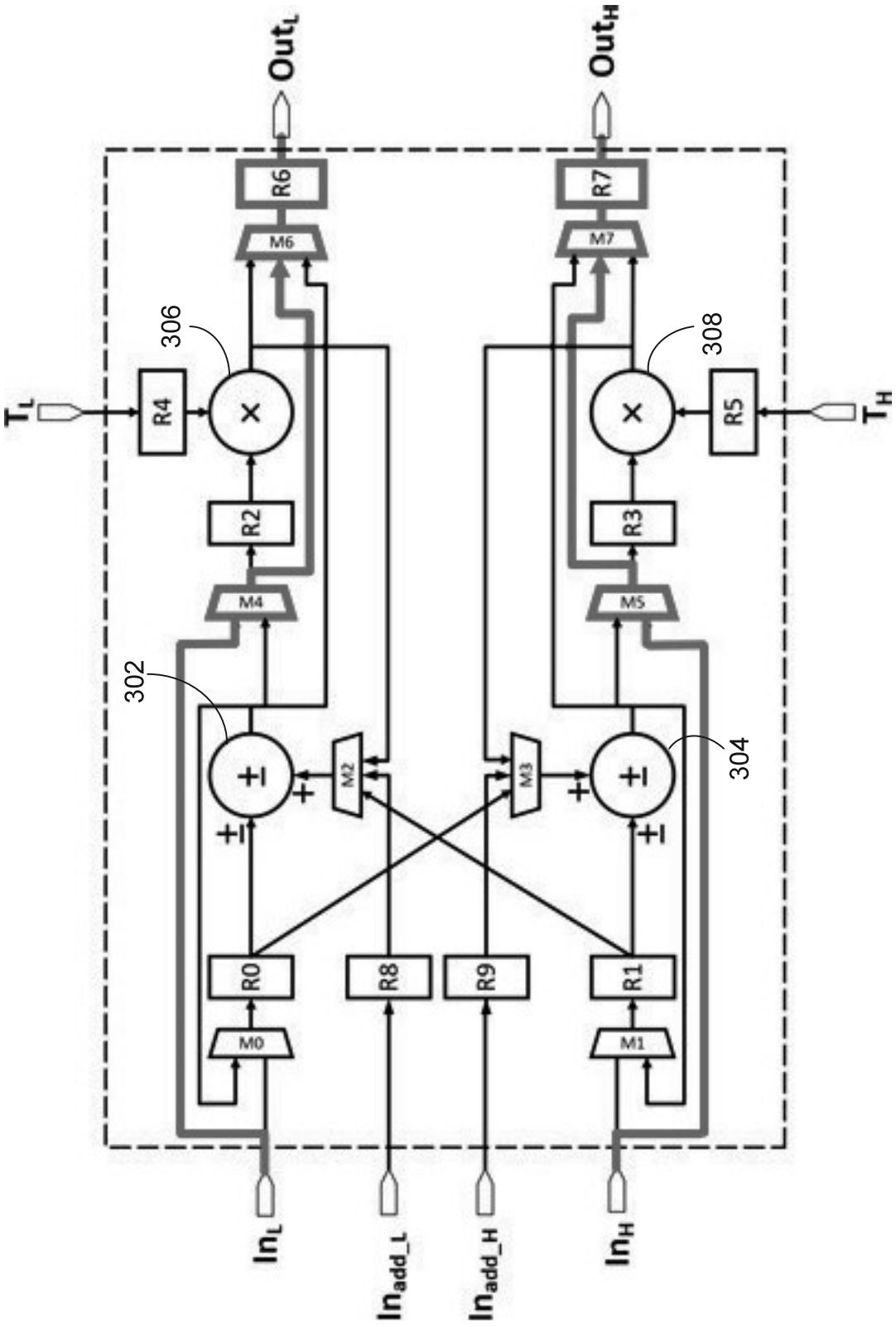
Out_L
Out_H
R6
R7
M6
M7
306
308
T_L
R4
R5
T_H
R2
R3
M4
M5
302
304
M2
M3
R0
R8
R9
R1
M0
M1
In_L
In_add_L
In_add_H
In_H

FIG. 13

