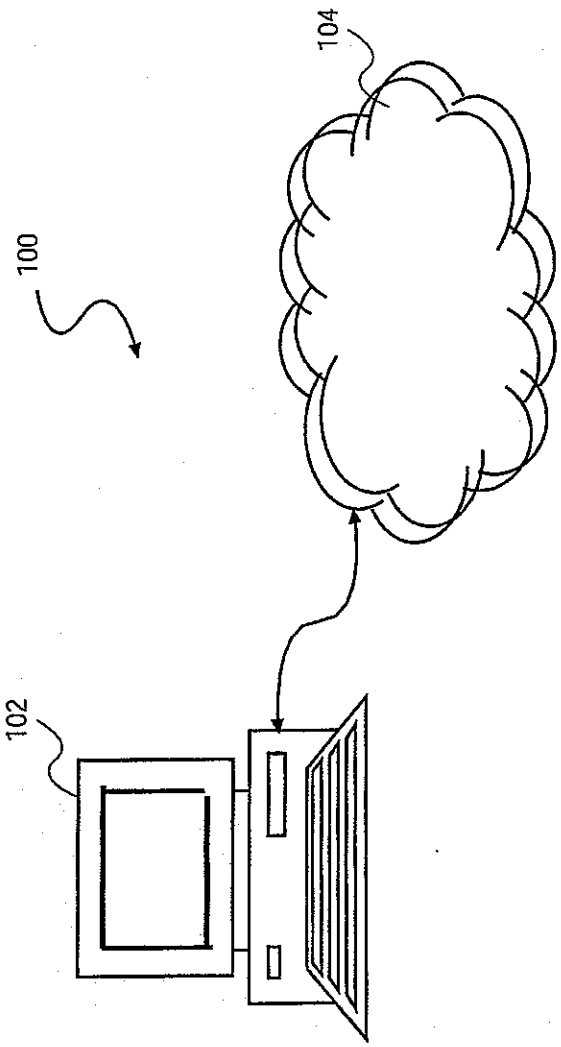


FIG. 1

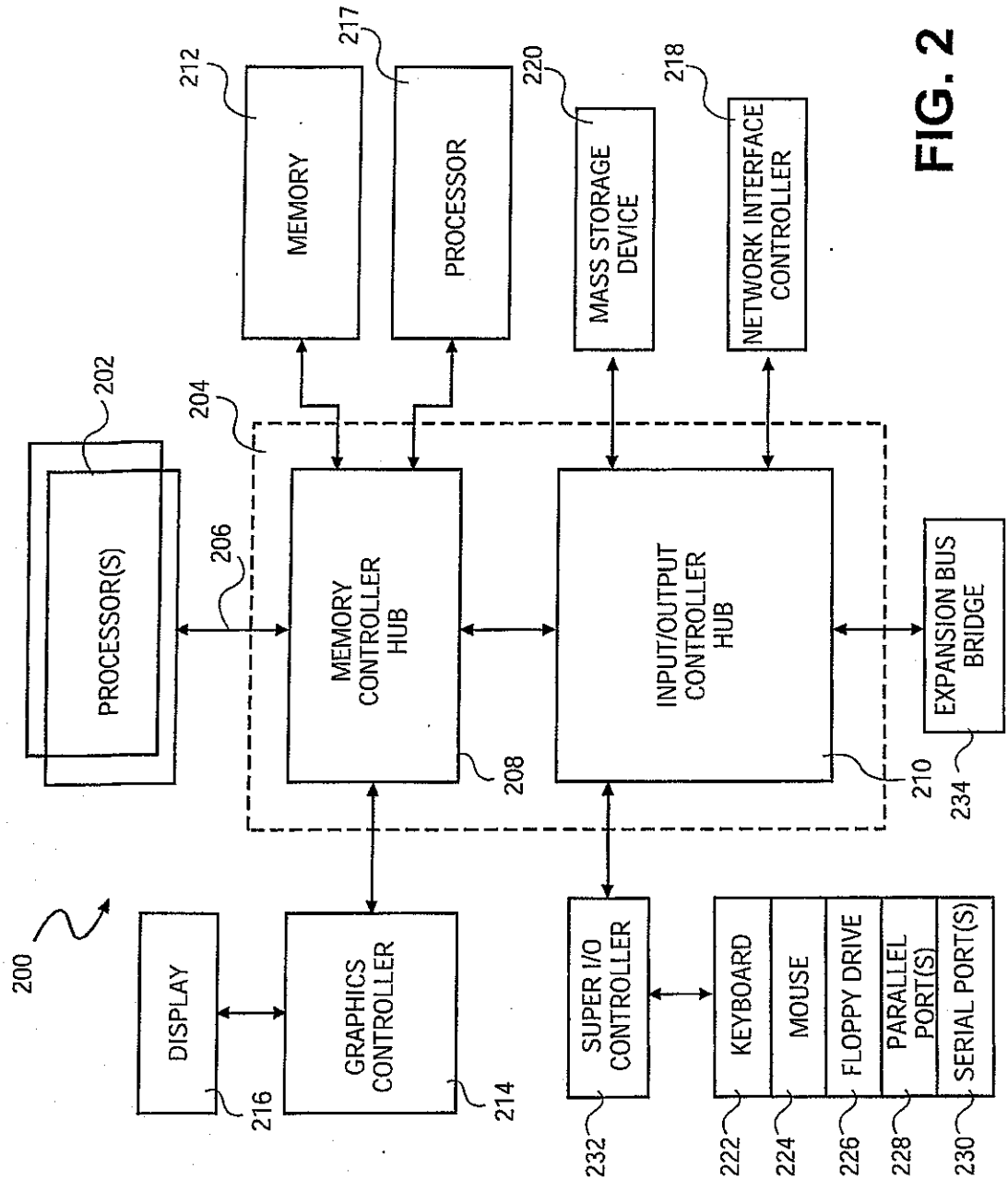

200
PROCESSOR(S)
202
204
206
MEMORY CONTROLLER HUB
208
INPUT/OUTPUT CONTROLLER HUB
210
EXPANSION BUS BRIDGE
234
MEMORY
212
PROCESSOR
217
MASS STORAGE DEVICE
220
NETWORK INTERFACE CONTROLLER
218
DISPLAY
216
GRAPHICS CONTROLLER
214
SUPER I/O CONTROLLER
232
KEYBOARD
222
MOUSE
224
FLOPPY DRIVE
226
PARALLEL PORT(S)
228
SERIAL PORT(S)
230

FIG. 2

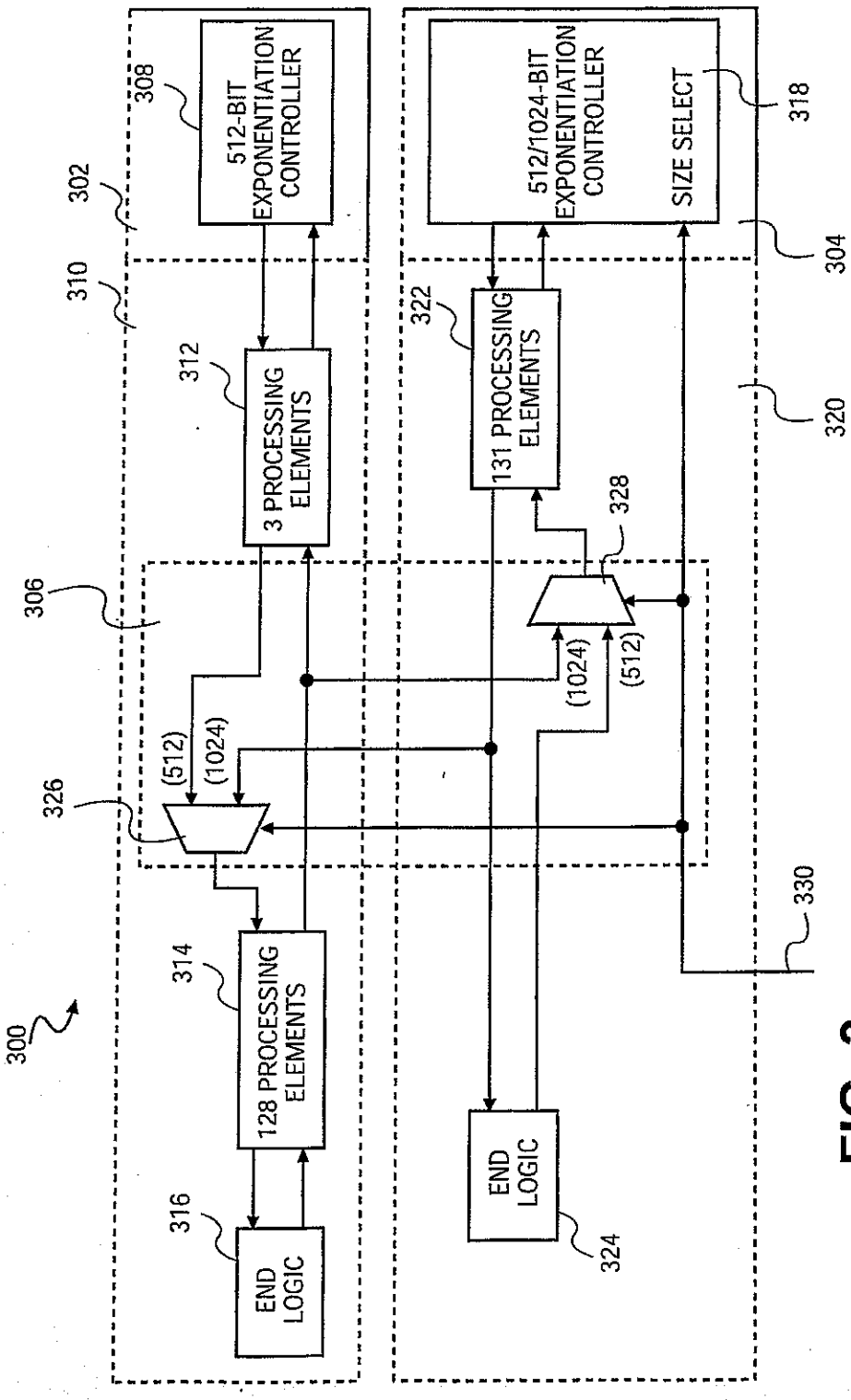

512-BIT EXPONENTIATION CONTROLLER
512/1024-BIT EXPONENTIATION CONTROLLER
SIZE SELECT
3 PROCESSING ELEMENTS
131 PROCESSING ELEMENTS
128 PROCESSING ELEMENTS
END LOGIC
END LOGIC
(512)
(1024)
(1024)
(512)
300
302
304
306
308
310
312
314
316
318
320
322
324
326
328
330

FIG. 3

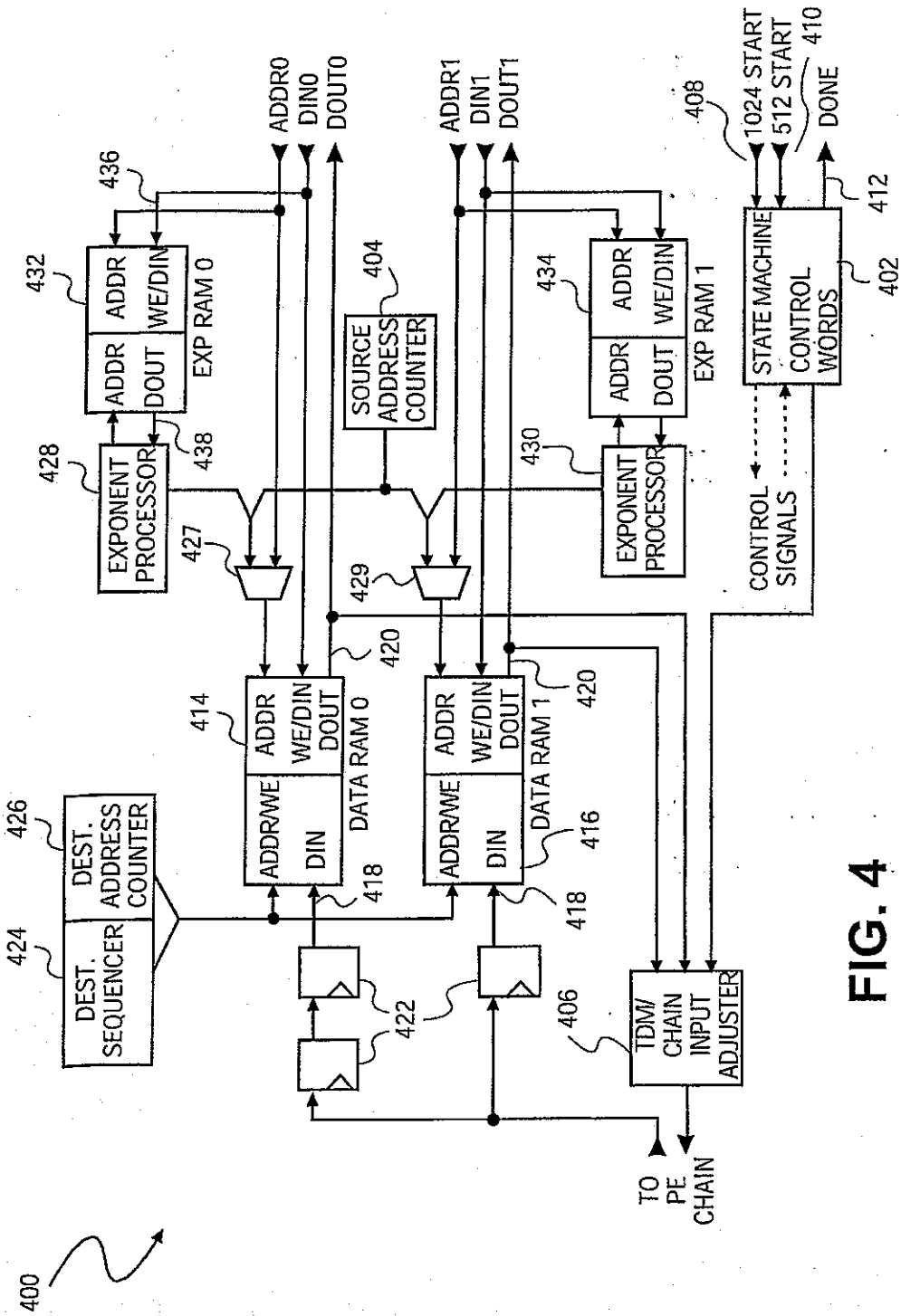

400
ADDR0
DIN0
DOUT0
ADDR1
DIN1
DOUT1
1024 START
512 START
DONE
408
410
412
436
432
ADDR
WE/DIN
ADDR
DOUT
EXP RAM 0
404
SOURCE ADDRESS COUNTER
434
ADDR
WE/DIN
ADDR
DOUT
EXP RAM 1
STATE MACHINE
CONTROL WORDS
402
428
EXPONENT PROCESSOR
438
430
EXPONENT PROCESSOR
CONTROL SIGNALS
427
429
414
ADDR
WE/DIN
DOUT
ADDR/WE
DIN
DATA RAM 0
420
ADDR
WE/DIN
DOUT
ADDR/WE
DIN
DATA RAM 1
420
426
DEST. ADDRESS COUNTER
424
DEST. SEQUENCER
418
416
418
422
406
TDM/ CHAIN INPUT ADJUSTER
TO PE CHAIN

FIG. 4

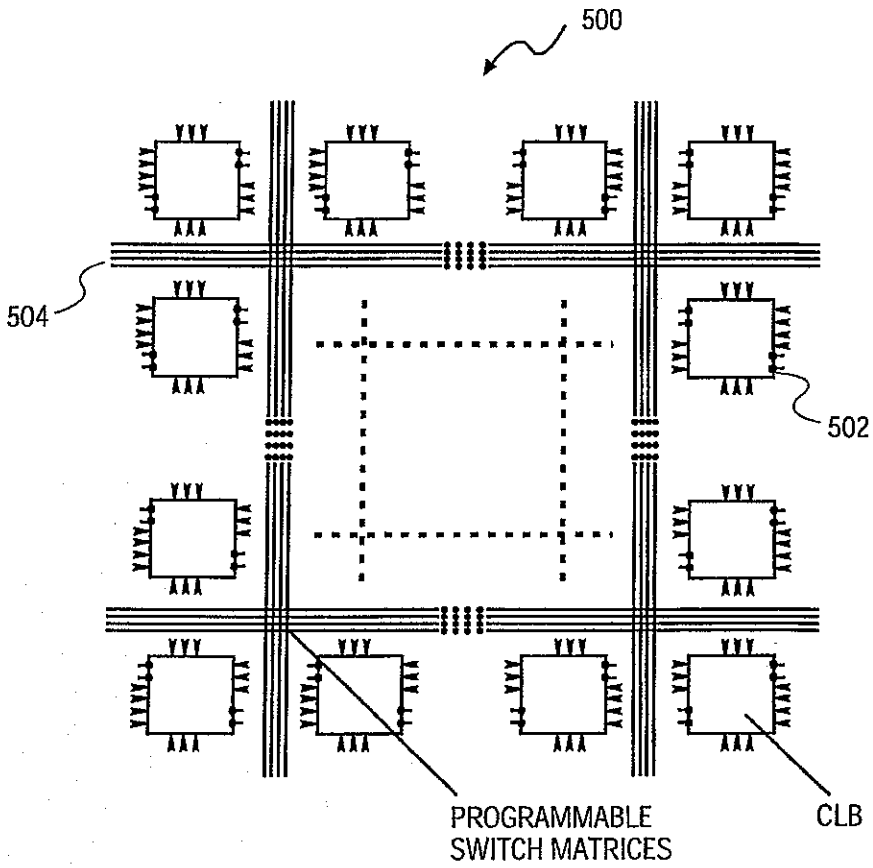


FIG. 5

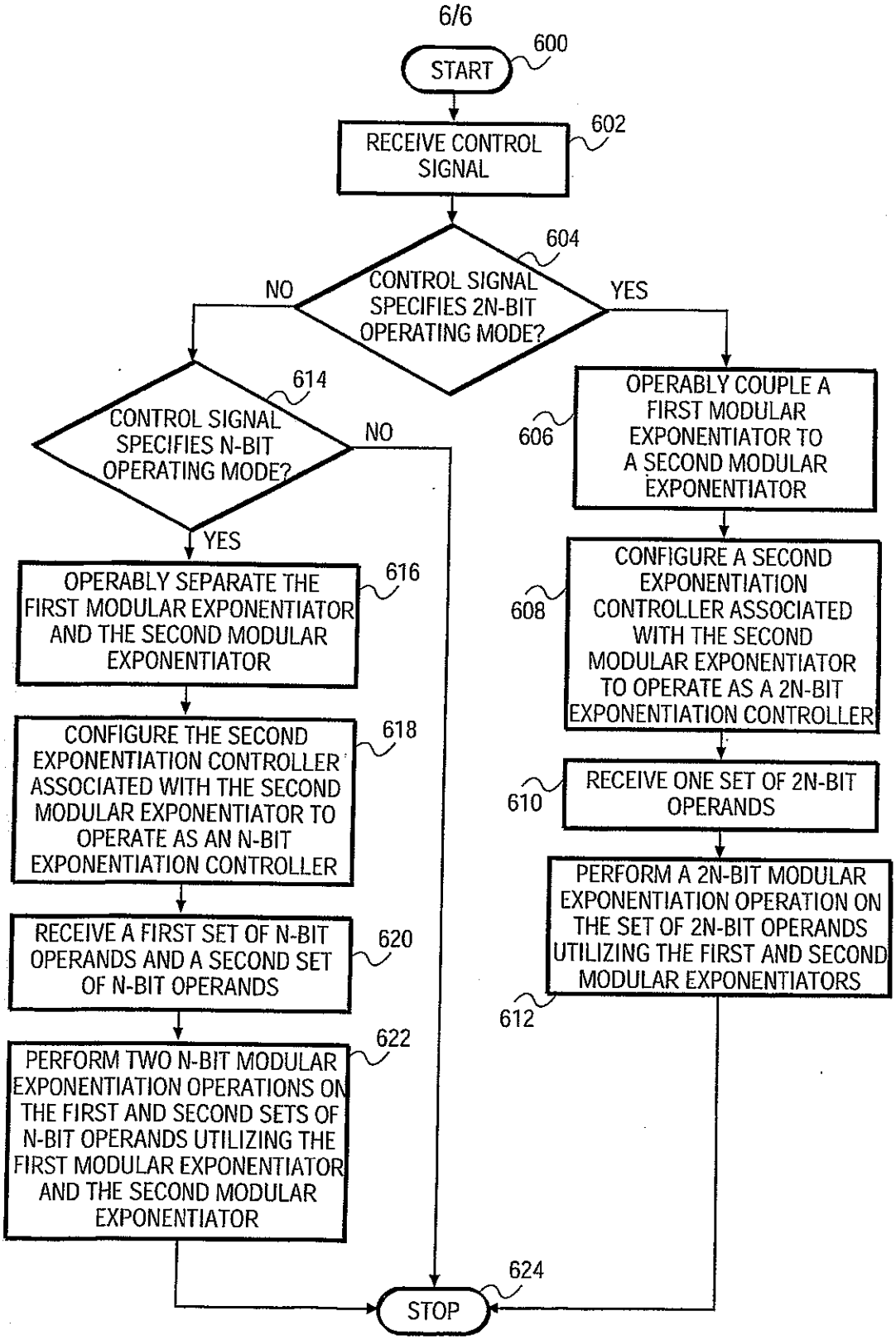

600
START
602
RECEIVE CONTROL SIGNAL
604
CONTROL SIGNAL SPECIFIES 2N-BIT OPERATING MODE?
NO
YES
614
CONTROL SIGNAL SPECIFIES N-BIT OPERATING MODE?
NO
YES
606
OPERABLY COUPLE A FIRST MODULAR EXPONENTIATOR TO A SECOND MODULAR EXPONENTIATOR
608
CONFIGURE A SECOND EXPONENTIATION CONTROLLER ASSOCIATED WITH THE SECOND MODULAR EXPONENTIATOR TO OPERATE AS A 2N-BIT EXPONENTIATION CONTROLLER
610
RECEIVE ONE SET OF 2N-BIT OPERANDS
612
PERFORM A 2N-BIT MODULAR EXPONENTIATION OPERATION ON THE SET OF 2N-BIT OPERANDS UTILIZING THE FIRST AND SECOND MODULAR EXPONENTIATORS
616
OPERABLY SEPARATE THE FIRST MODULAR EXPONENTIATOR AND THE SECOND MODULAR EXPONENTIATOR
618
CONFIGURE THE SECOND EXPONENTIATION CONTROLLER ASSOCIATED WITH THE SECOND MODULAR EXPONENTIATOR TO OPERATE AS AN N-BIT EXPONENTIATION CONTROLLER
620
RECEIVE A FIRST SET OF N-BIT OPERANDS AND A SECOND SET OF N-BIT OPERANDS
622
PERFORM TWO N-BIT MODULAR EXPONENTIATION OPERATIONS ON THE FIRST AND SECOND SETS OF N-BIT OPERANDS UTILIZING THE FIRST MODULAR EXPONENTIATOR AND THE SECOND MODULAR EXPONENTIATOR
624
STOP

FIG. 6