

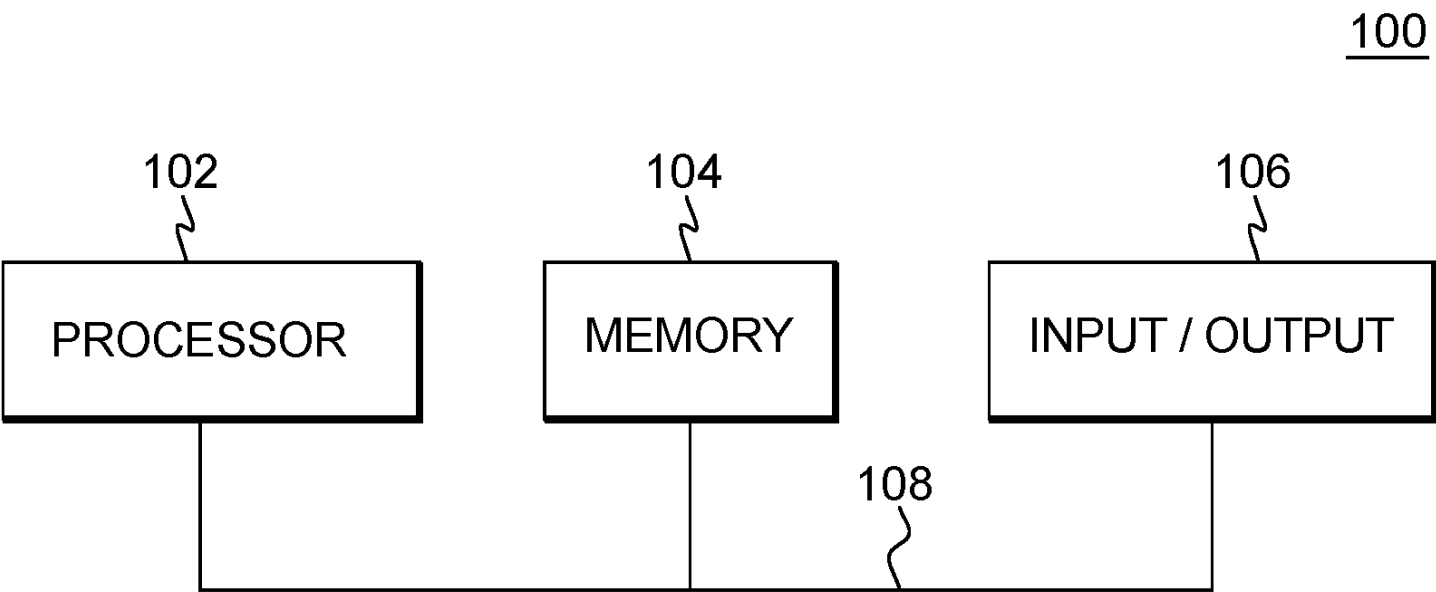


FIG. 1A

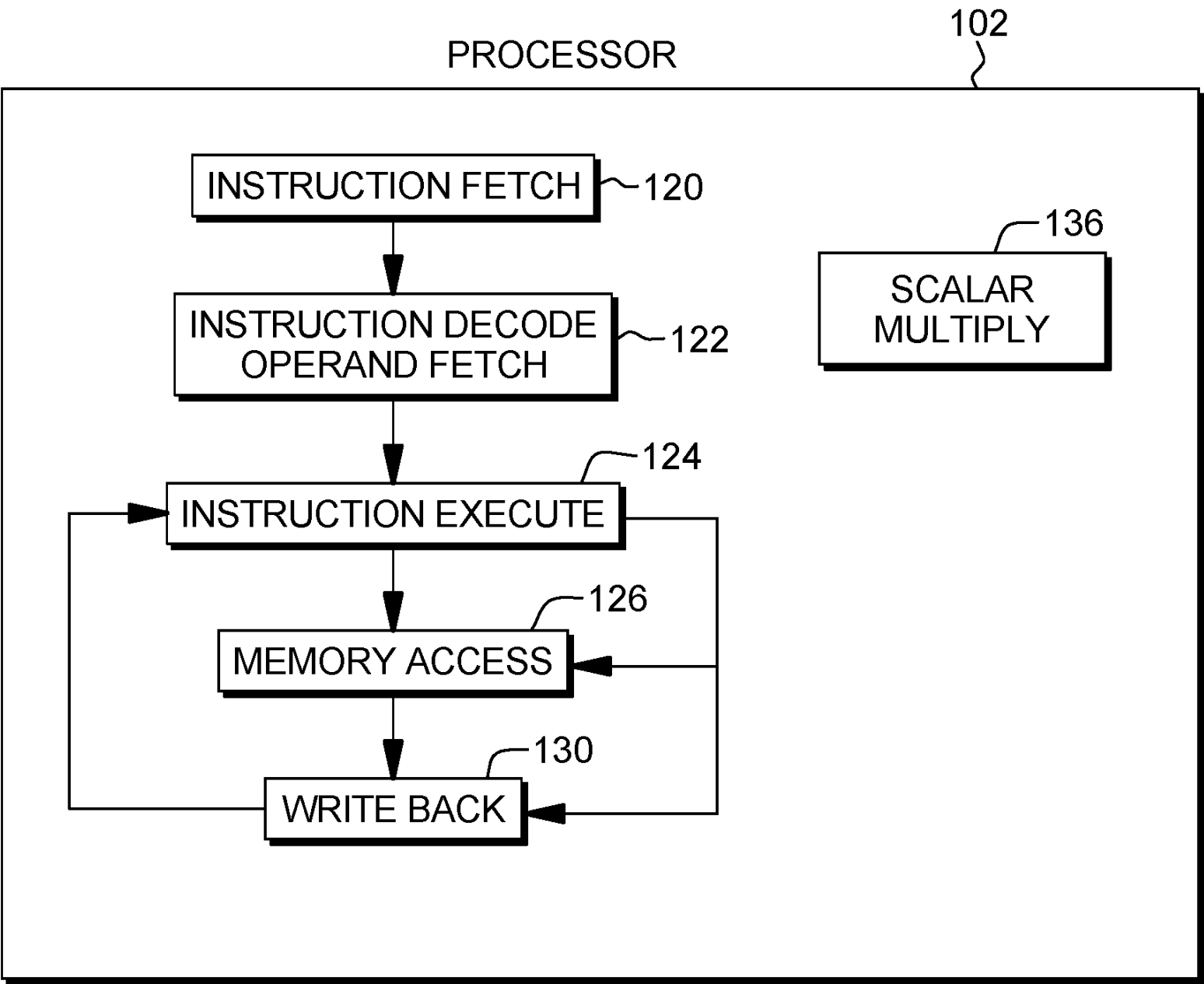


FIG. 1B

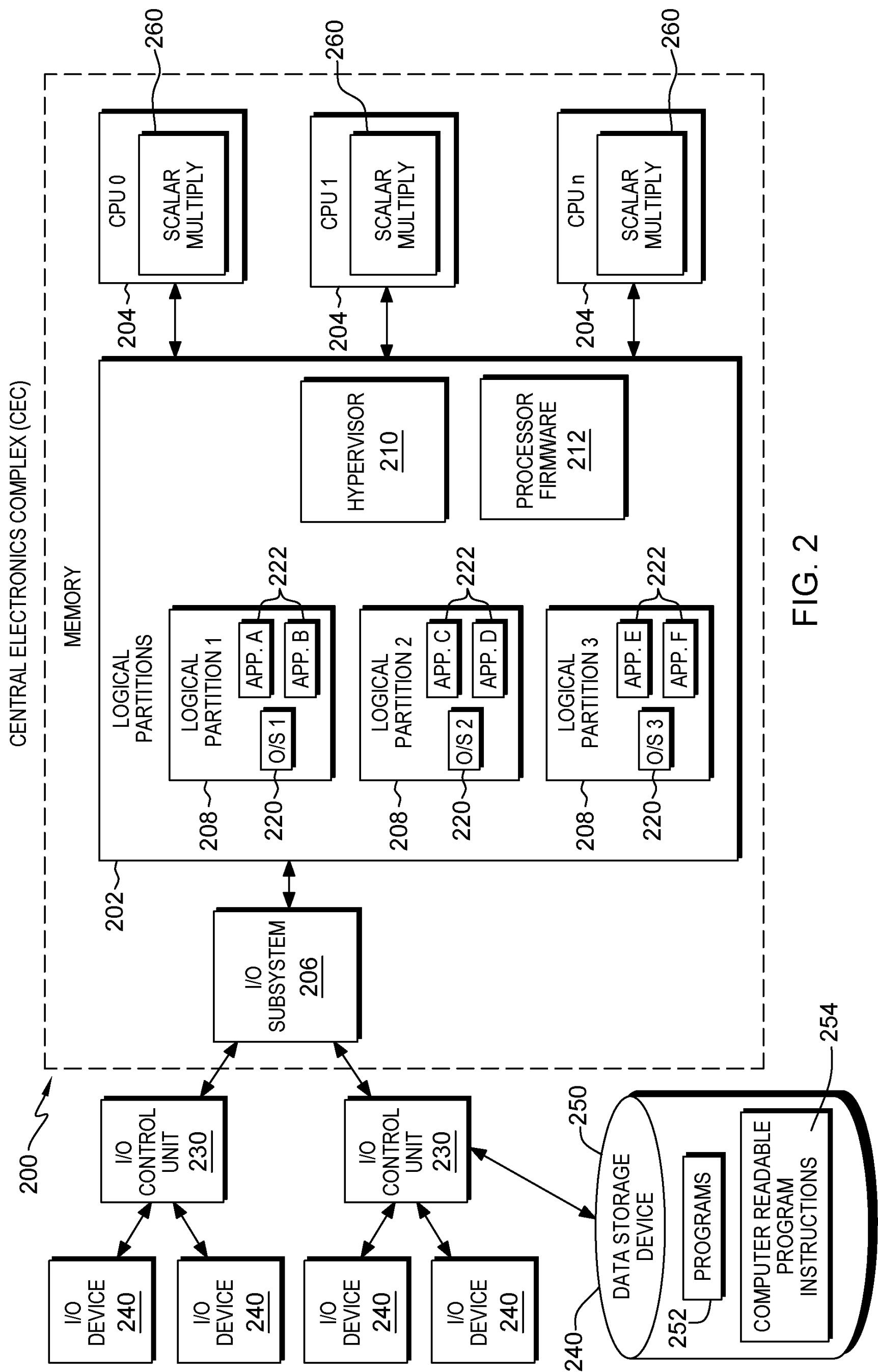


FIG. 2

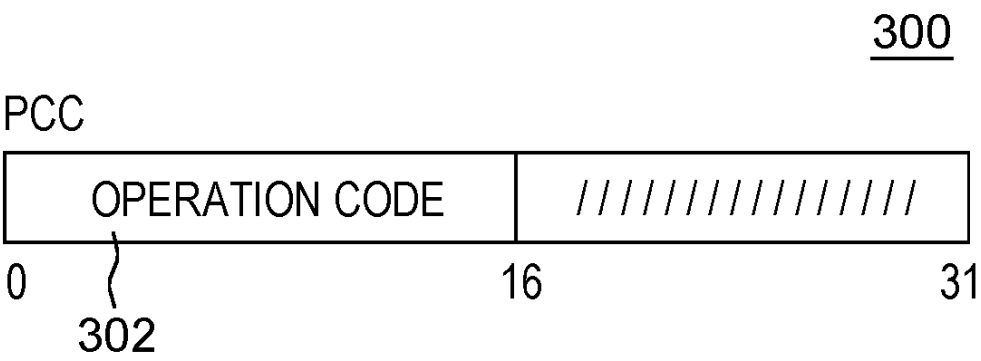


FIG. 3A

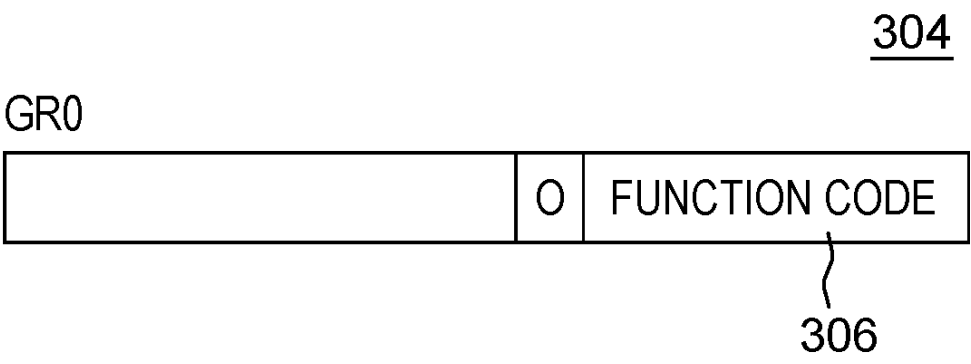


FIG. 3B

4/12

	Code	Function	Parm. Block Size (bytes)	Data Block Size (bytes)
310 ~	0	PCC-Query	16	-
312 ~	1	PCC-Compute-Last-Block-CMAC- Using-DEA	32	8
314 ~	2	PCC-Compute-Last-Block-CMAC- Using-TDEA-128	40	8
316 ~	3	PCC-Compute-Last-Block-CMAC- Using-TDEA-192	48	8
318 ~	9	PCC-Compute-Last-Block-CMAC- Using-Encrypted-DEA	56	8
320 ~	10	PCC-Compute-Last-Block-CMAC- Using-Encrypted-TDEA-128	64	8
322 ~	11	PCC-Compute-Last-Block-CMAC- Using-Encrypted-TDEA-192	72	8
324 ~	18	PCC-Compute-Last-Block-CMAC- Using-AES-128	56	16
326 ~	19	PCC-Compute-Last-Block-CMAC- Using-AES-192	64	16
328 ~	20	PCC-Compute-Last-Block-CMAC- Using-AES-256	72	16
330 ~	26	PCC-Compute-Last-Block-CMAC- Using-Encrypted-AES-128	88	16
332 ~	27	PCC-Compute-Last-Block-CMAC- Using-Encrypted-AES-192	96	16
334 ~	28	PCC-Compute-Last-Block-CMAC- Using-Encrypted-AES-256A	104	16
336 ~	50	PCC-Compute-XTS-Parameter- Using-AES-128	80	16
338 ~	52	PCC-Compute-XTS-Parameter- Using-AES-256	96	16
340 ~	58	PCC-Compute-XTS-Parameter- Using-Encrypted-AES-128	112	16
342 ~	60	PCC-Compute-XTS-Parameter- Using-Encrypted-AES-256	128	16
344 ~	64	PCC-Scalar-Multiply-P256	1480	-
346 ~	65	PCC-Scalar-Multiply-P384	1560	-
348 ~	66	PCC-Scalar-Multiply-P521	1720	-
350 ~	72	PCC-Scalar-Multiply-Ed25519	1480	-
352 ~	73	PCC-Scalar-Multiply-Ed448	1640	-

FIG. 3C

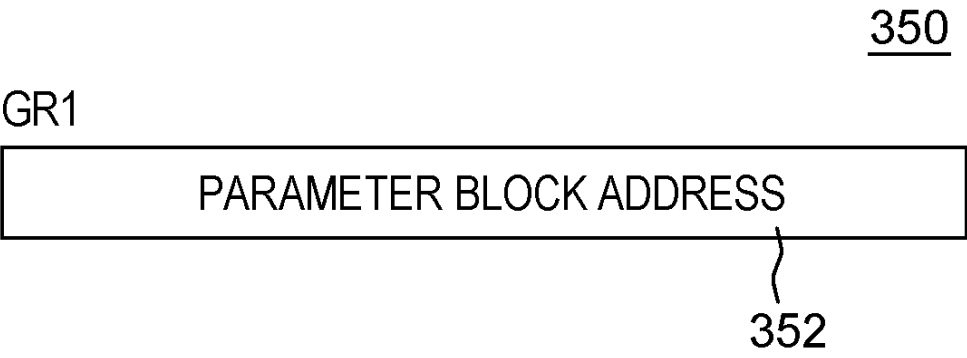
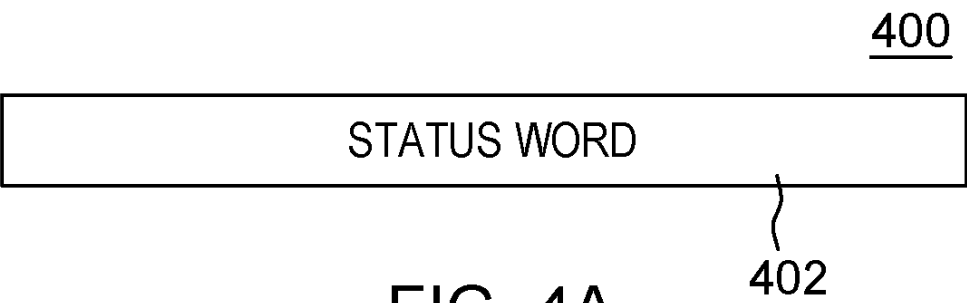


FIG. 3D



OFFSET		PCC -SCALAR-MULTIPLY- P256 AND Ed25519	
DEC	HEX		
00	00	RESULT X COMPONENT (Xr)	405
32	20	RESULT Y COMPONENT (Yr)	406
64	40	SOURCE X COMPONENT (Xs)	407
96	60	SOURCE Y COMPONENT (Ys)	408
128	80	SCALAR (d)	409
160	A0	RESERVED SAVE AREA	410
1480	5C8	0	63

FIG. 4B

OFFSET		PCC -SCALAR-MULTIPLY- P384	
DEC	HEX		
00	00	RESULT X COMPONENT (Xr)	413
48	30	RESULT Y COMPONENT (Yr)	414
96	60	SOURCE X COMPONENT (Xs)	415
144	90	SOURCE Y COMPONENT (Ys)	416
192	C0	SCALAR (d)	417
240	F0	RESERVED SAVE AREA	418
1560	618	0	63

FIG. 4C

OFFSET				<u>420</u>
DEC	HEX	PCC -SCALAR-MULTIPLY- P521		
00	00	RESULT X COMPONENT (Xr)	<u>421</u>	
80	50	RESULT Y COMPONENT (Yr)	<u>422</u>	
160	A0	SOURCE X COMPONENT (Xs)	<u>423</u>	
240	F0	SOURCE Y COMPONENT (Ys)	<u>424</u>	
320	140	SCALAR (d)		
400	190	RESERVED SAVE AREA	<u>425</u>	
1720	6B8	0	32	63

FIG. 4D

OFFSET				<u>426</u>
DEC	HEX	PCC -SCALAR-MULTIPLY- Ed448		
00	00	RESULT X COMPONENT (Xr)	<u>427</u>	
64	40	RESULT Y COMPONENT (Yr)	<u>428</u>	
128	80	SOURCE X COMPONENT (Xs)	<u>429</u>	
192	C0	SOURCE Y COMPONENT (Ys)	<u>430</u>	
256	100	SCALAR (d)	<u>431</u>	
320	140	RESERVED SAVE AREA	<u>432</u>	
1640	668	0	32	63

FIG. 4E

8/12

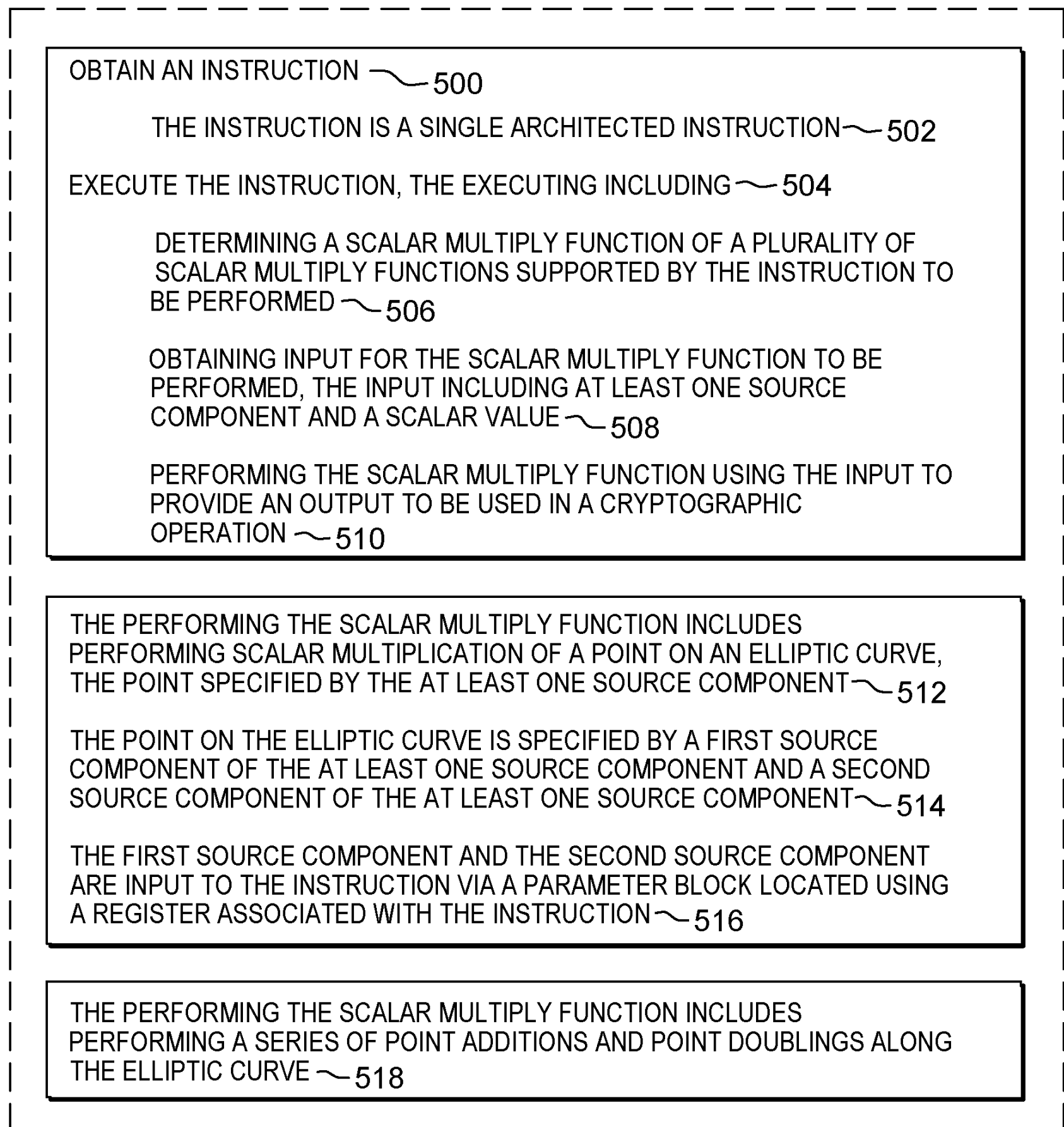


FIG. 5A

9/12

THE PERFORMING THE SCALAR MULTIPLY FUNCTION INCLUDES USING THE FOLLOWING EQUATION: $(X_r, Y_r) = d * (X_s, Y_s)$, IN WHICH X_s AND Y_s ARE THE AT LEAST ONE SOURCE COMPONENT AND ARE COORDINATES OF A POINT ON AN ELLIPTIC CURVE, d IS THE SCALAR VALUE, $*$ IS SCALAR MULTIPLY, AND X_r AND Y_r ARE RESULTING COORDINATES OF THE SCALAR MULTIPLY FUNCTION, THE RESULTING COORDINATES BEING THE OUTPUT ~ 520

d INCLUDES A PLURALITY OF BITS WHICH ARE SCANNED FROM ONE BIT (e.g., A MOST SIGNIFICANT BIT OF d) TO ANOTHER BIT (e.g., A LEAST SIGNIFICANT BIT OF d) ~ 522

THE PERFORMING THE SCALAR MULTIPLY FUNCTION FURTHER INCLUDES FOR A BIT OF THE PLURALITY OF BITS OF d EQUAL TO A SELECT VALUE, A POINT ADDITION OCCURS, AND AFTER EACH BIT IS SCANNED, A POINT DOUBLING OCCURS ~ 524

THE PLURALITY OF SCALAR MULTIPLY FUNCTIONS INCLUDES A PLURALITY OF SCALAR MULTIPLY FUNCTIONS FOR A PLURALITY OF ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM FUNCTIONS FOR A PLURALITY OF PRIMES ~ 526

THE PLURALITY OF SCALAR MULTIPLY FUNCTIONS INCLUDES A PLURALITY OF SCALAR MULTIPLY FUNCTIONS FOR A PLURALITY OF EDWARDS-CURVE DIGITAL SIGNATURE ALGORITHM FUNCTIONS FOR A PLURALITY OF PRIMES ~ 528

FIG. 5B

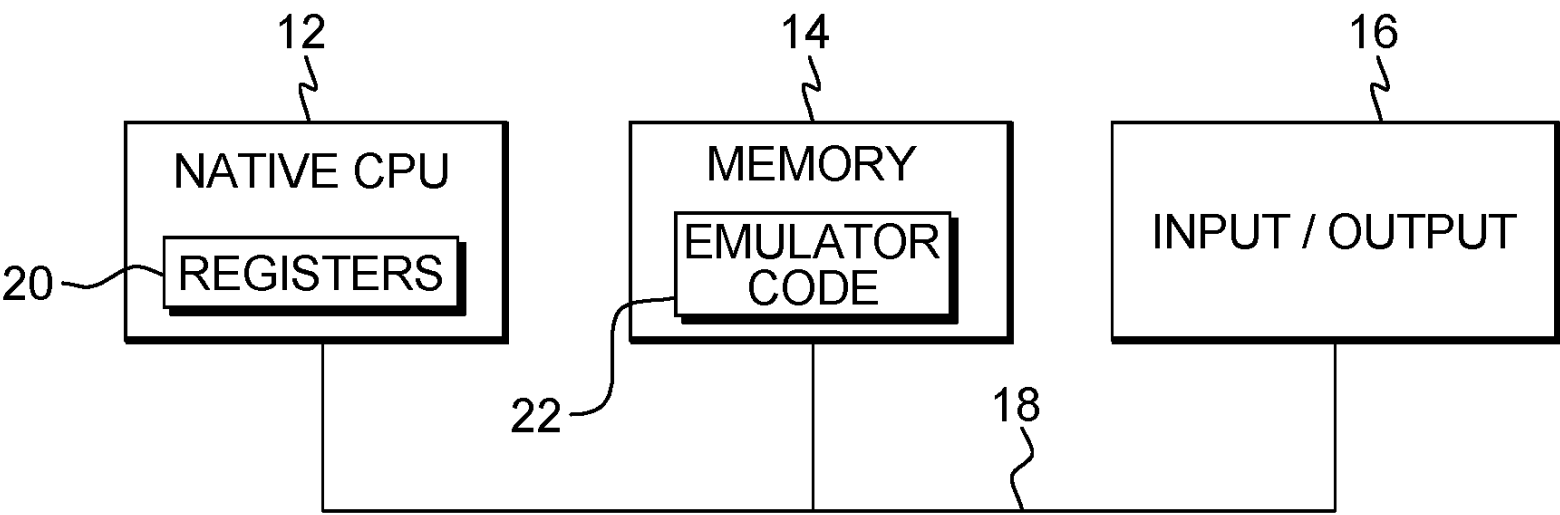


FIG. 6A

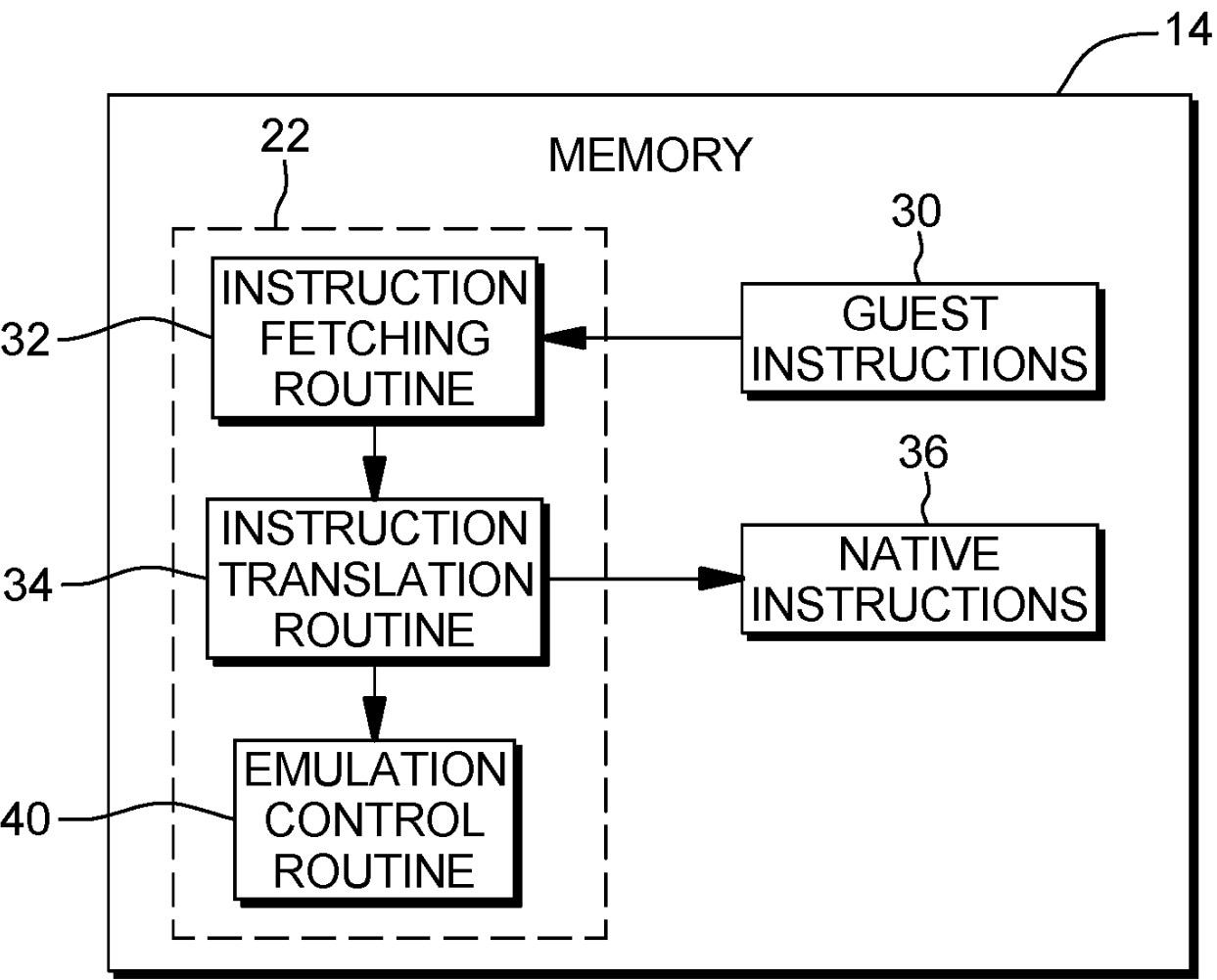


FIG. 6B

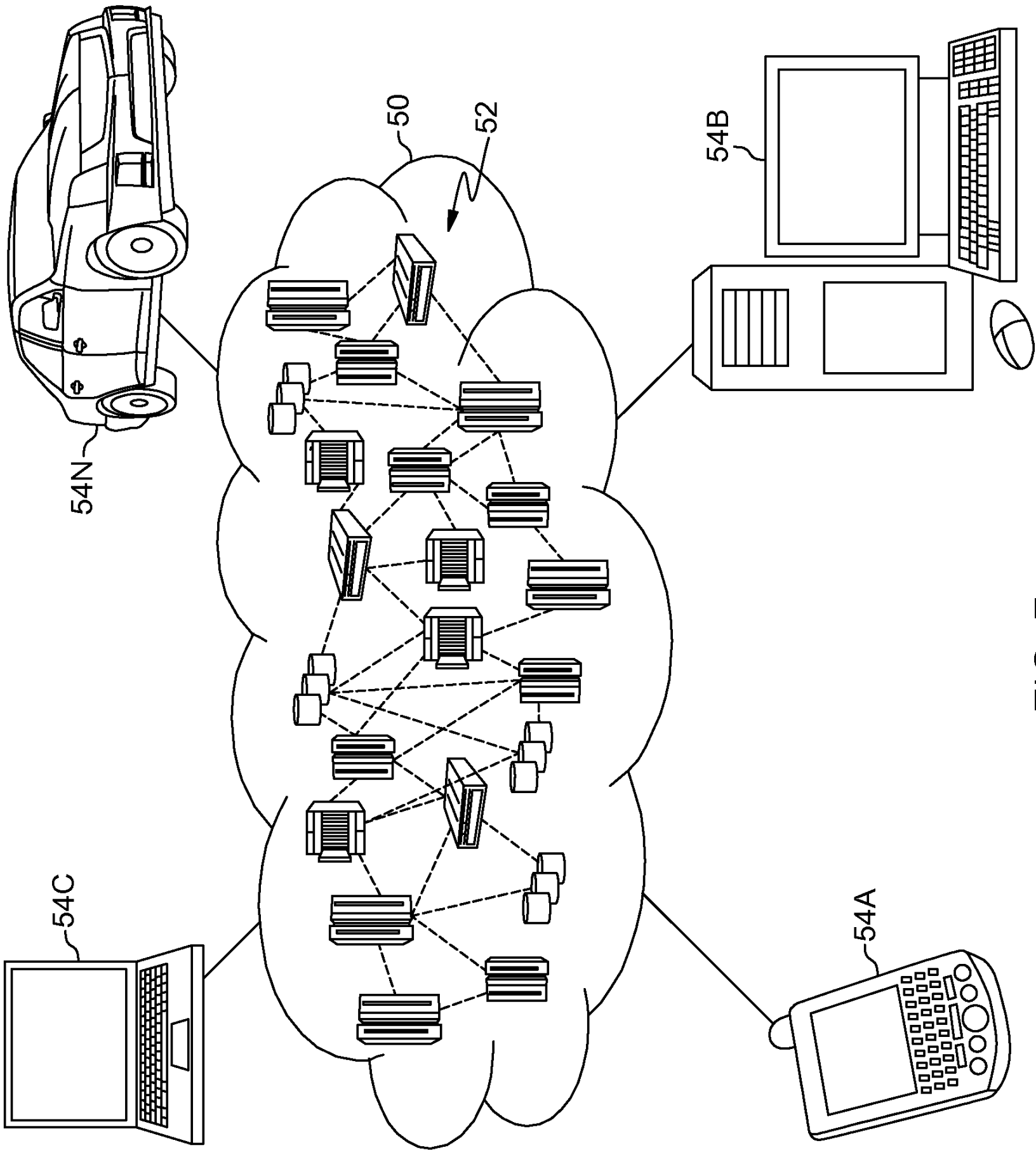


FIG. 7

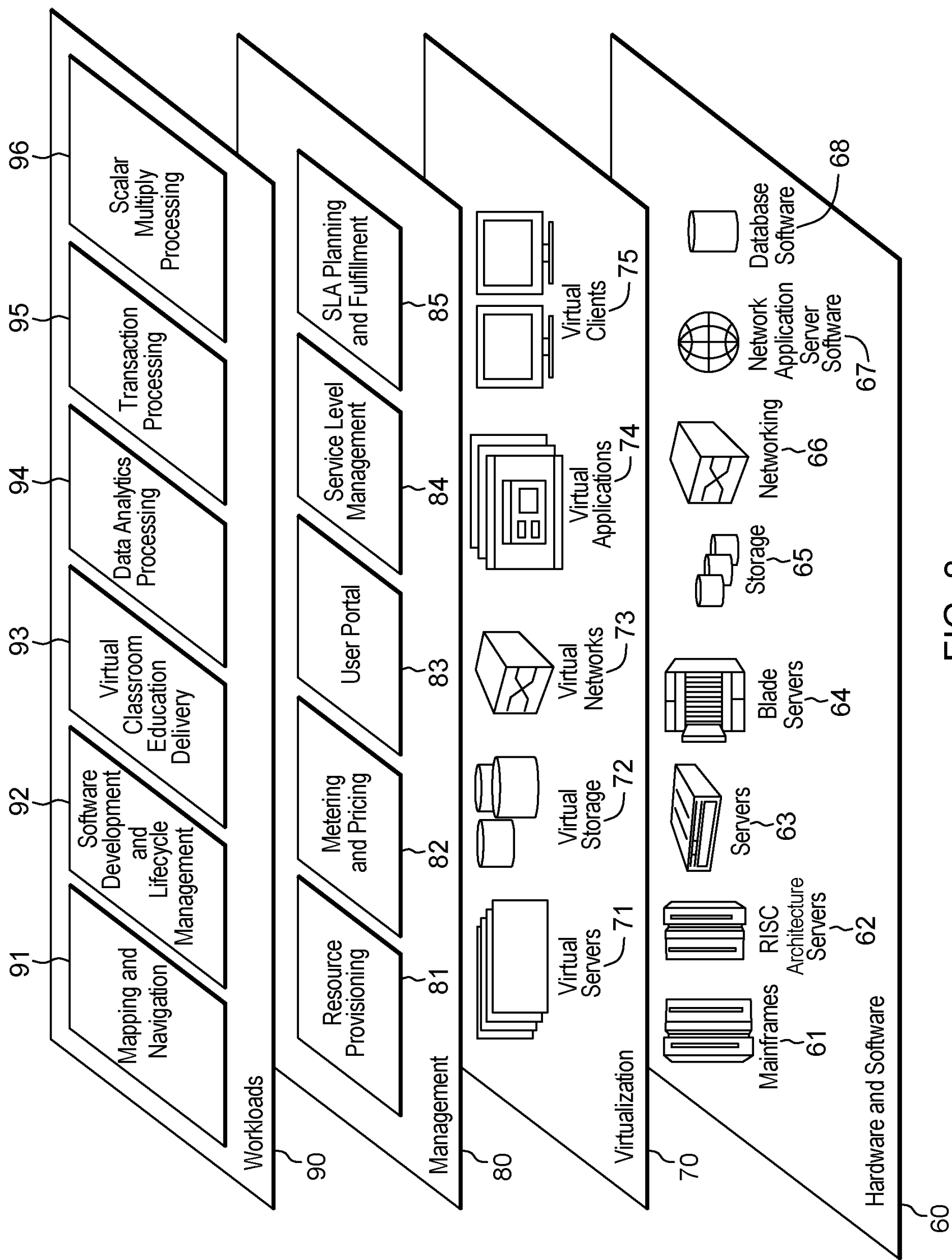


FIG. 8