

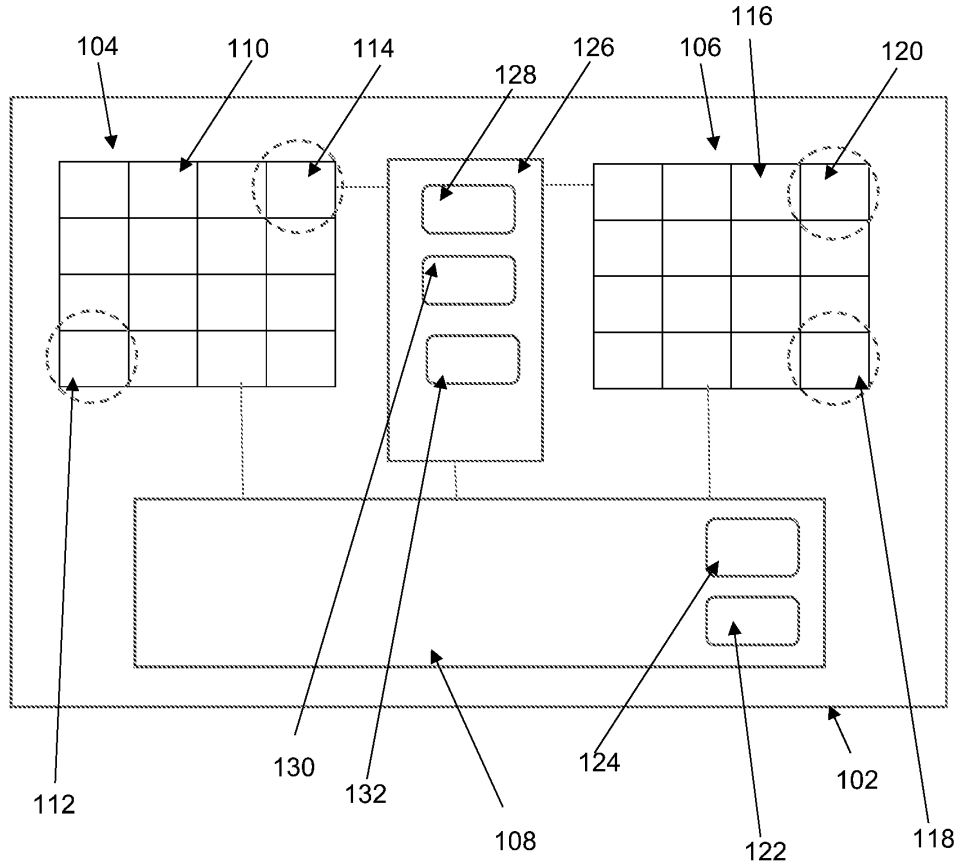


FIG. 1

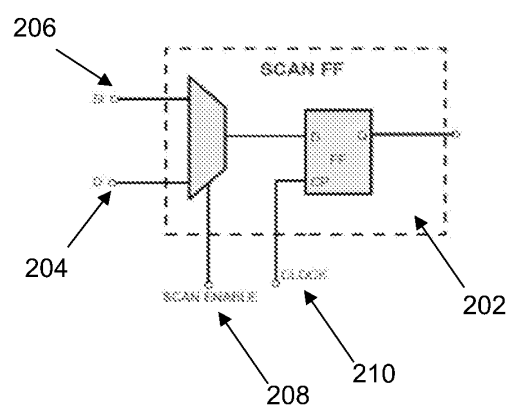


FIG. 2

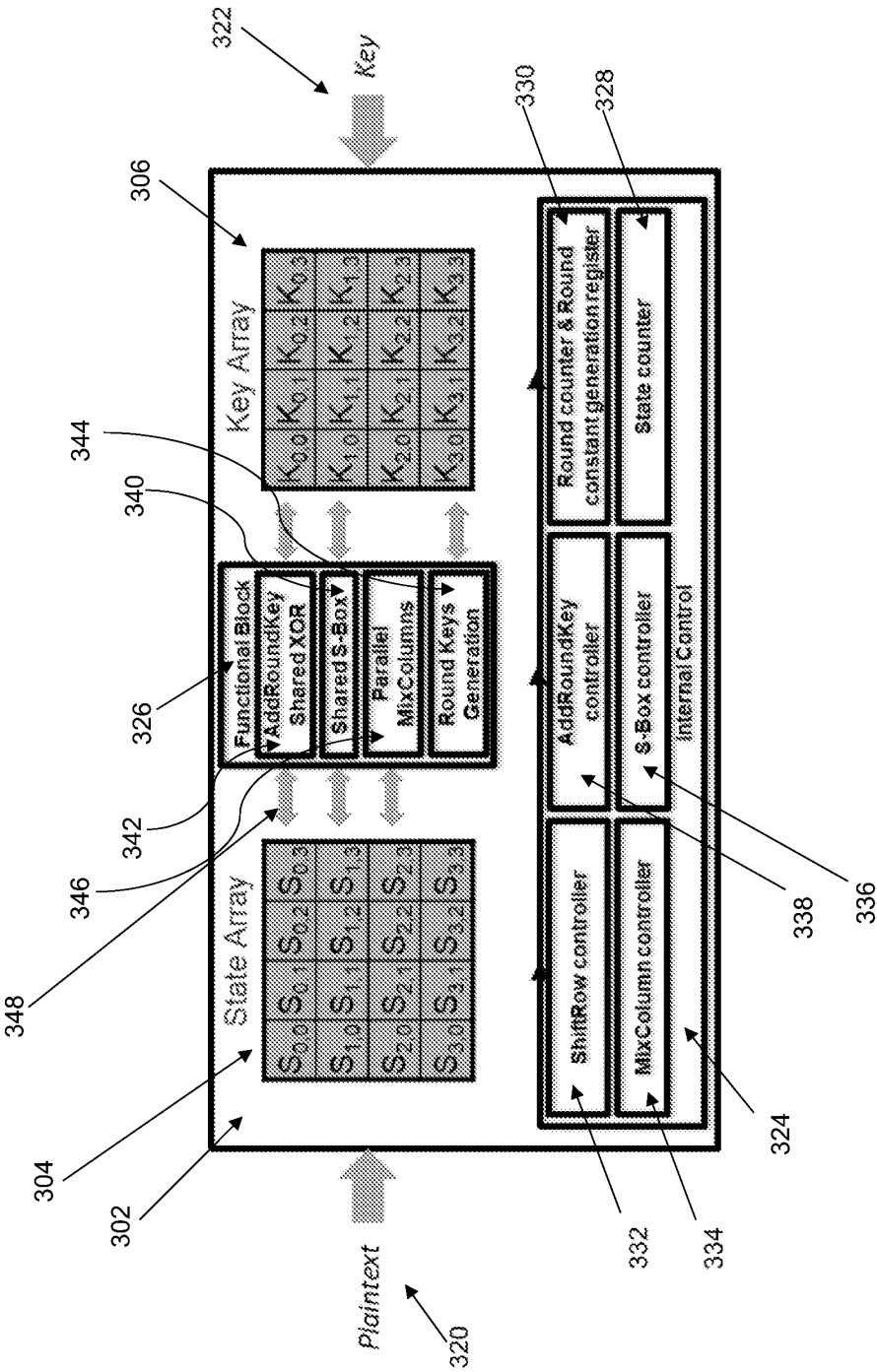


FIG. 3A

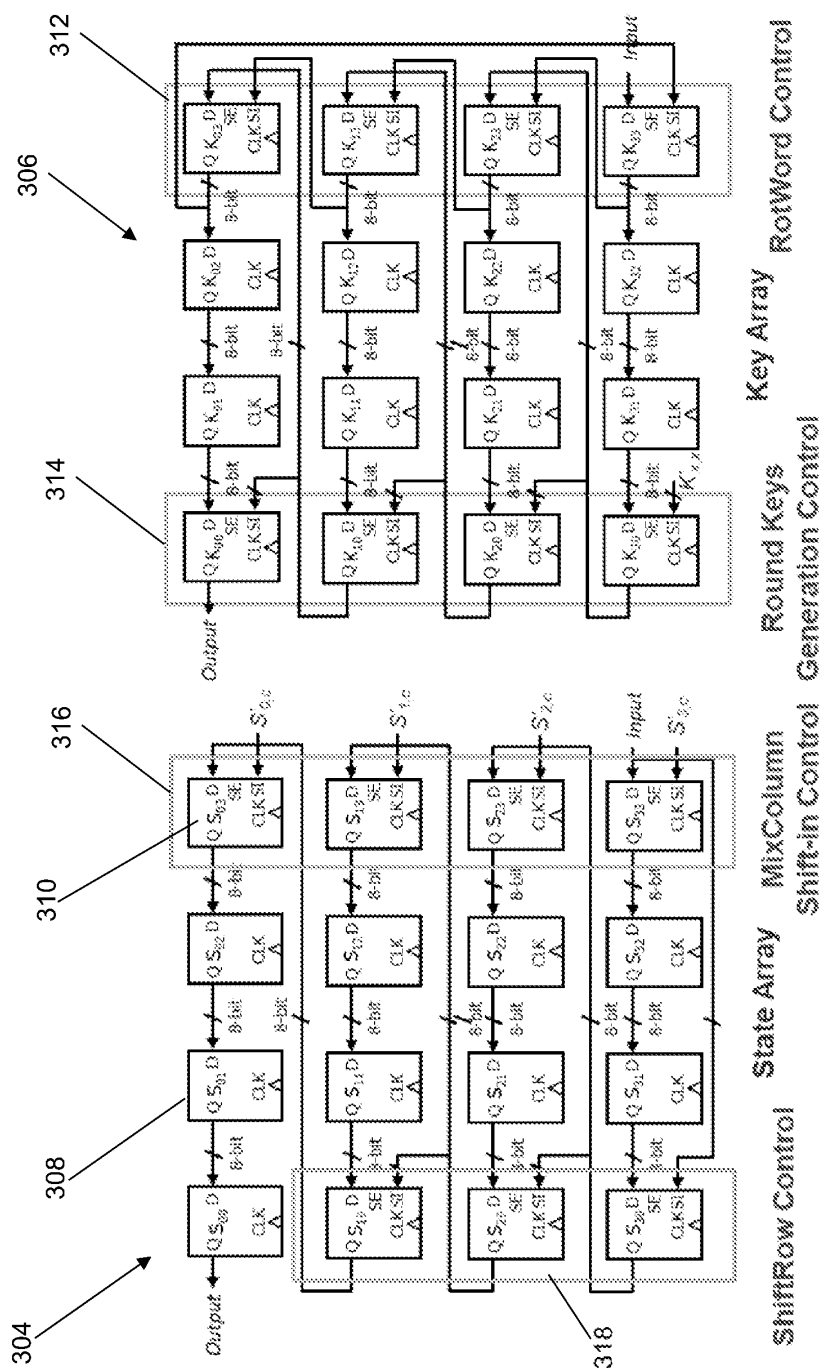


FIG. 3B

402

Round	Constant (RCon)	Round	Constant (RCon)
1	(01 00 00 00) ₁₆	6	(20 00 00 00) ₁₆
2	(02 00 00 00) ₁₆	7	(40 00 00 00) ₁₆
3	(04 00 00 00) ₁₆	8	(80 00 00 00) ₁₆
4	(08 00 00 00) ₁₆	9	(1B 00 00 00) ₁₆
5	(10 00 00 00) ₁₆	10	(36 00 00 00) ₁₆

FIG. 4A

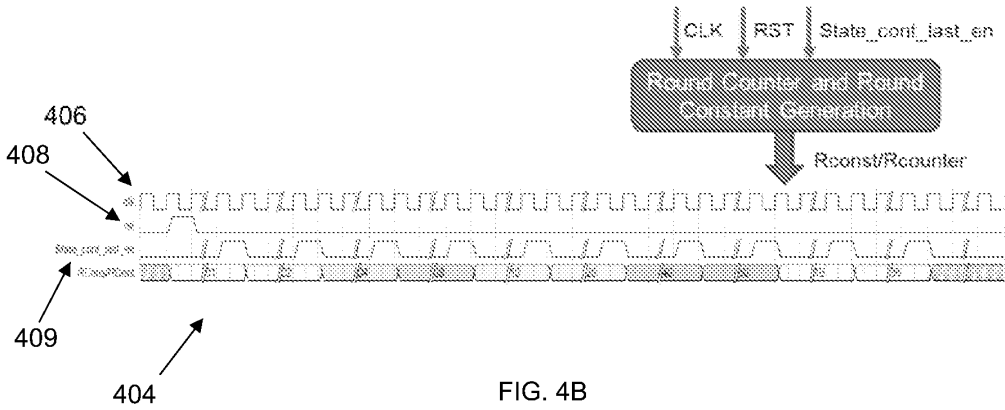


FIG. 4B

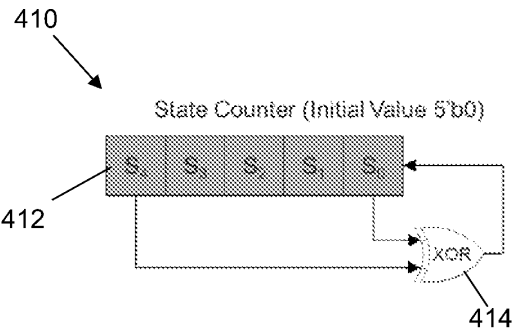


FIG. 4C

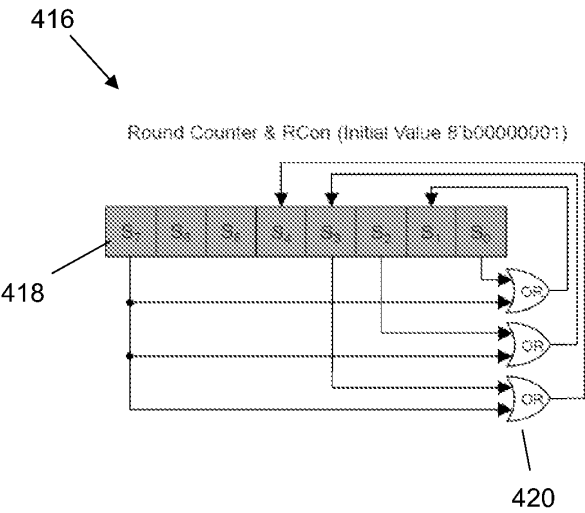


FIG. 4D

Cycle	Counter Value	Cycle	Counter Value
0	00000	11	00111
1	00001	12	01110
2	00010	13	11101
3	00101	14	11011
4	01010	15	10111
5	10101	16	01111
6	01011	17	11110
7	10110	18	11100
8	01100	19	11000
9	11001	20	10000
10	10011		

422



FIG. 4E

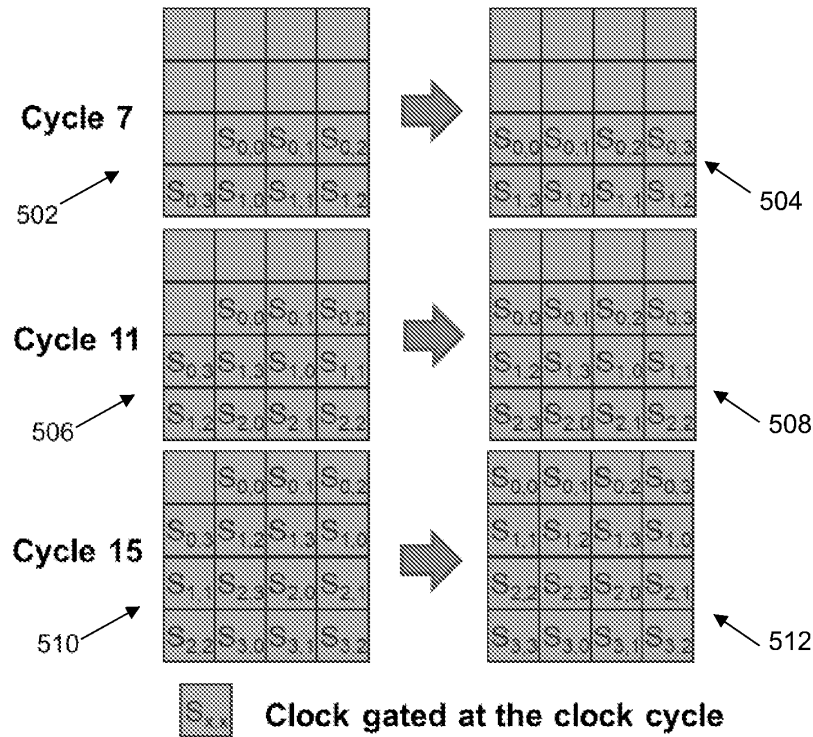


FIG. 5

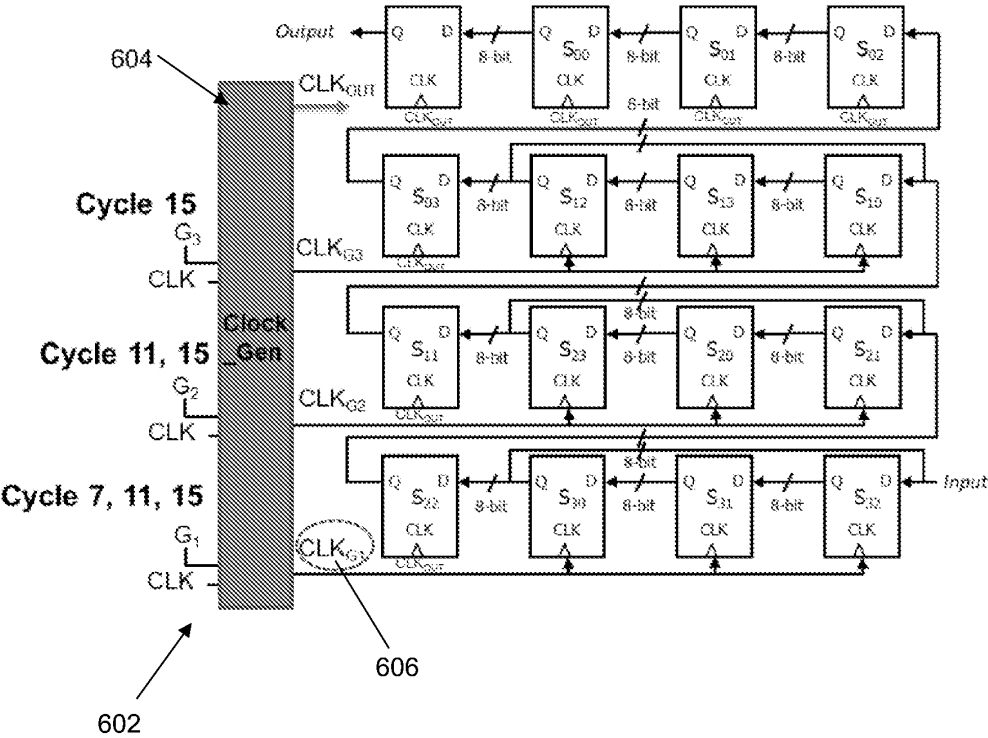


FIG. 6A

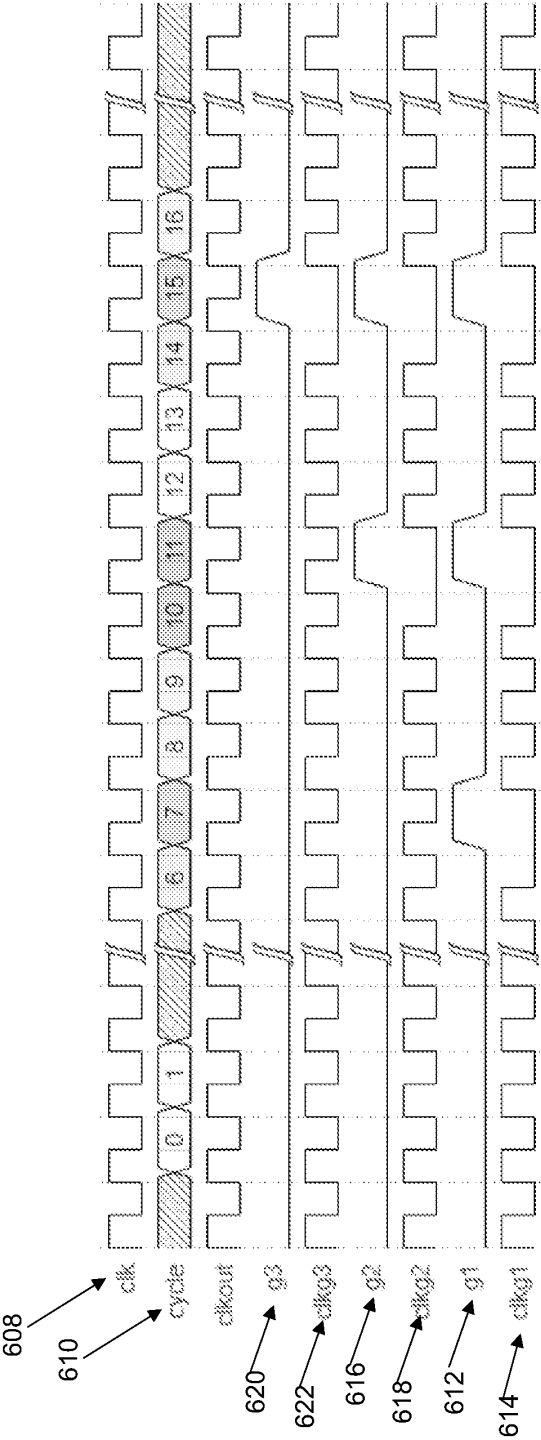


FIG. 6B

11/26

	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	eb	78
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	7e	c0
2	b7	fa	93	26	36	3f	f7	cc	24	a3	e5	f1	71	d8	31	13
3	04	c7	23	c3	18	96	05	9a	07	13	8c	e2	eb	27	c2	75
4	00	03	2c	1a	1b	6e	5a	a0	50	3b	36	b3	23	e3	2f	64
5	03	d1	50	ed	28	fc	b1	3b	6a	cb	b0	35	4a	4c	58	cf
6	00	ef	aa	fb	43	43	33	05	43	f9	02	7f	50	3c	9f	a8
7	51	a3	40	0f	92	3d	38	f5	bc	b5	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5c	97	44	17	ca	a7	7e	3d	64	5d	19	73
9	80	01	4f	dc	22	2a	90	08	4b	ee	b5	14	da	3e	0b	cf
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	ed	8d	d5	4e	a9	6c	b6	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	0f	48	03	f6	0a	e1	35	57	b9	66	c1	1d	9e
e	a1	f3	98	11	69	d9	8a	94	0b	1a	87	a5	ce	55	28	af
f	8c	a1	89	0d	bf	e6	42	68	41	99	24	0f	b0	54	5b	16

702

FIG. 7

12/26

804

$$\begin{aligned}
 S'_{0,c} &= ((02) \cdot S_{0,c}) \oplus ((03) \cdot S_{1,c}) \oplus S_{2,c} \oplus S_{3,c} \\
 S'_{1,c} &= S_{0,c} \oplus ((02) \cdot S_{1,c}) \oplus ((03) \cdot S_{2,c}) \oplus S_{3,c} \\
 S'_{2,c} &= S_{0,c} \oplus S_{1,c} \oplus ((02) \cdot S_{2,c}) \oplus ((03) \cdot S_{3,c}) \\
 S'_{3,c} &= ((03) \cdot S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus ((02) \cdot S_{3,c})
 \end{aligned}$$

802

FIG. 8A

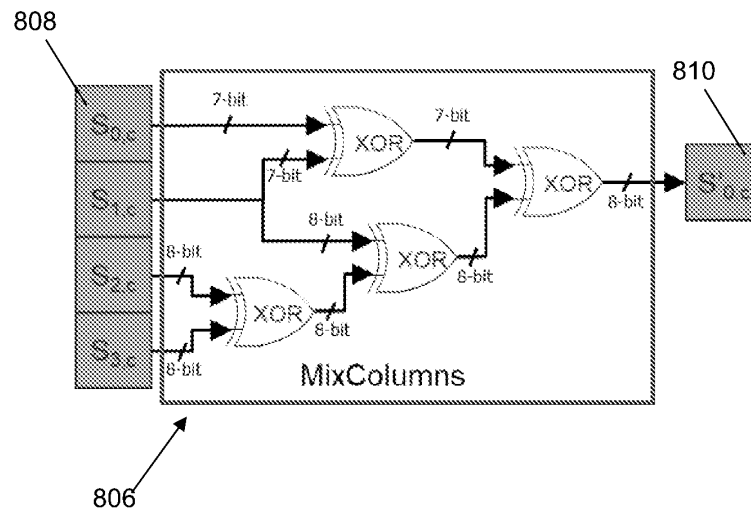


FIG. 8B

13/26

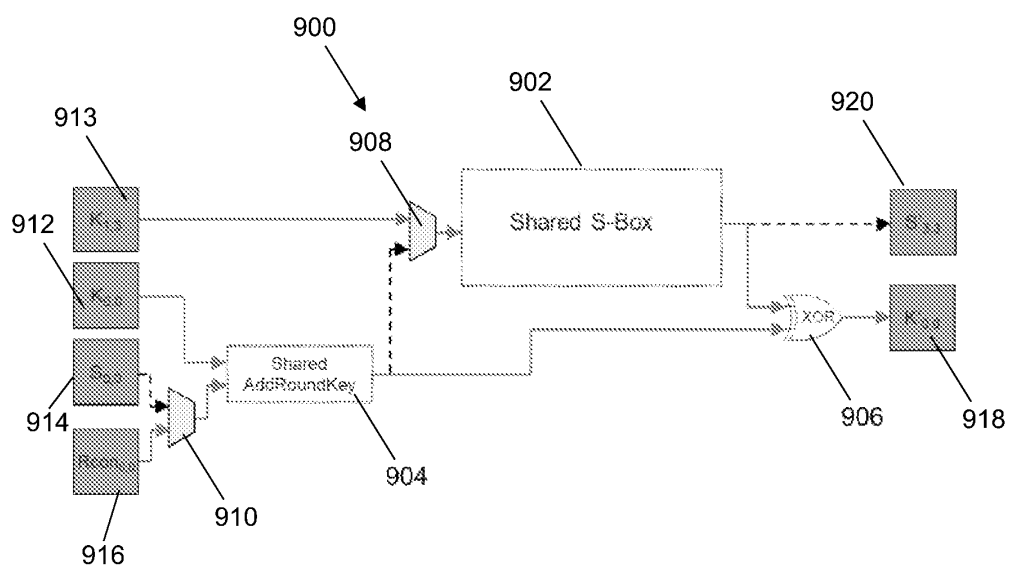


FIG. 9A

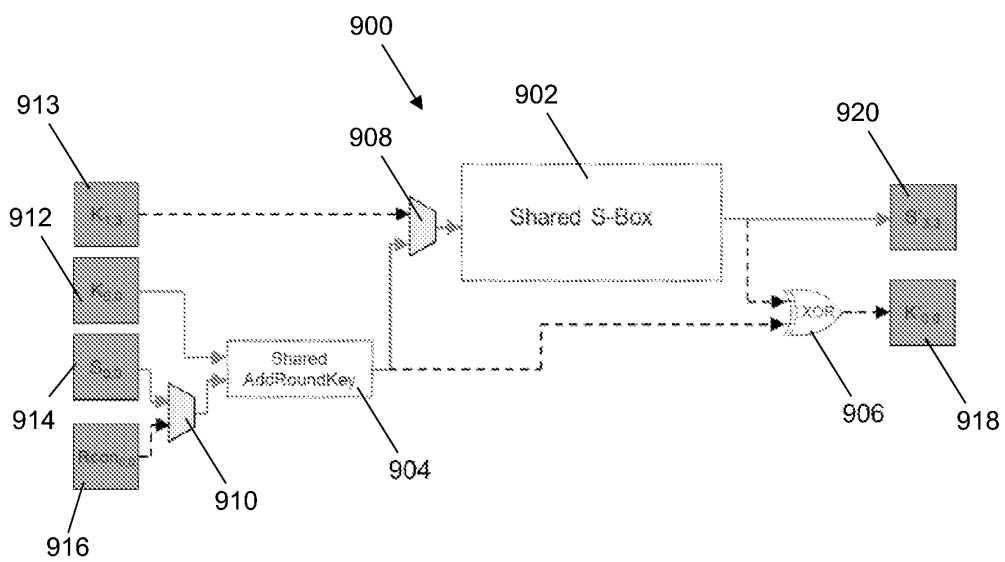


FIG. 9B

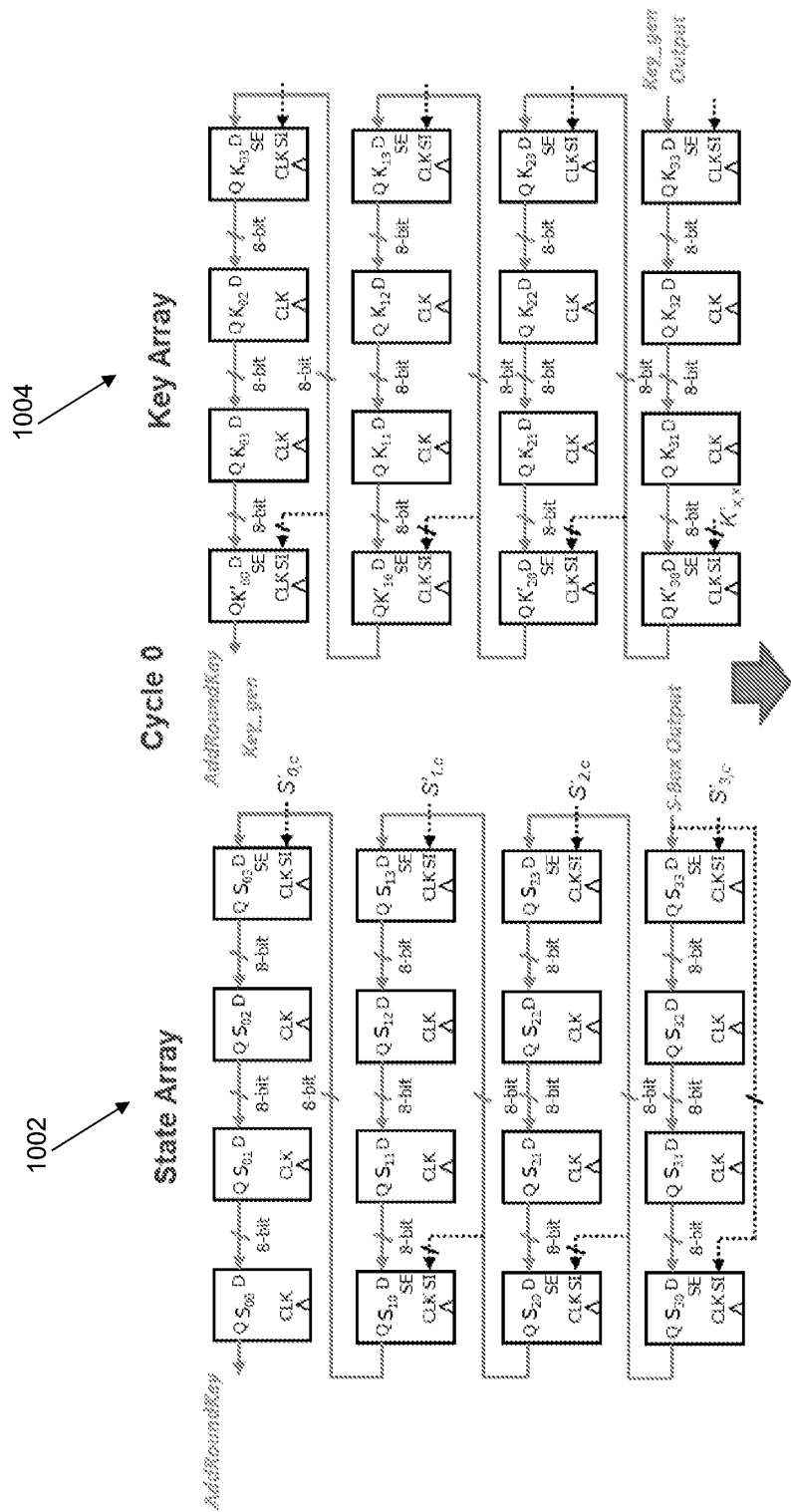


FIG. 10A

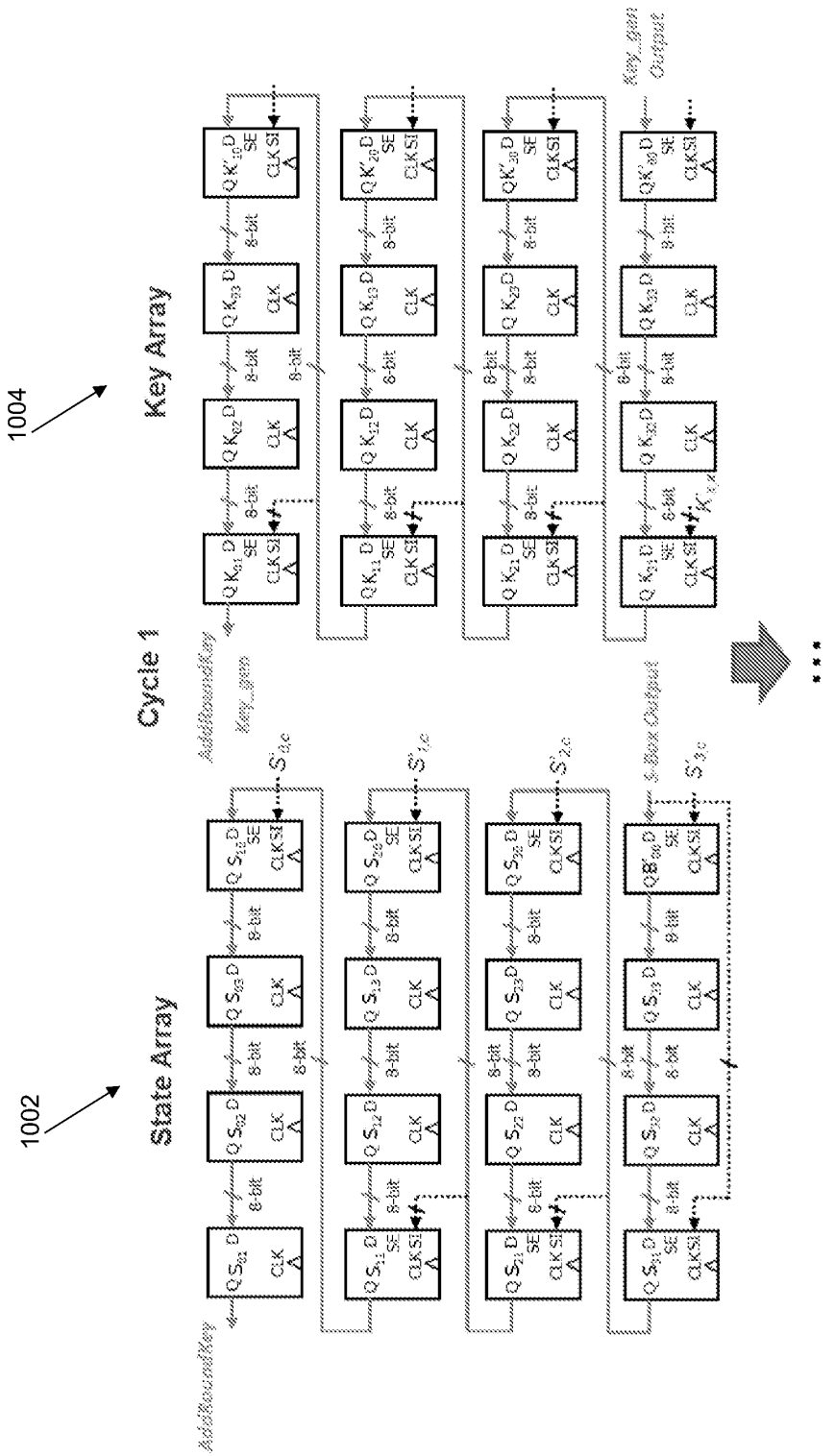


FIG. 10B

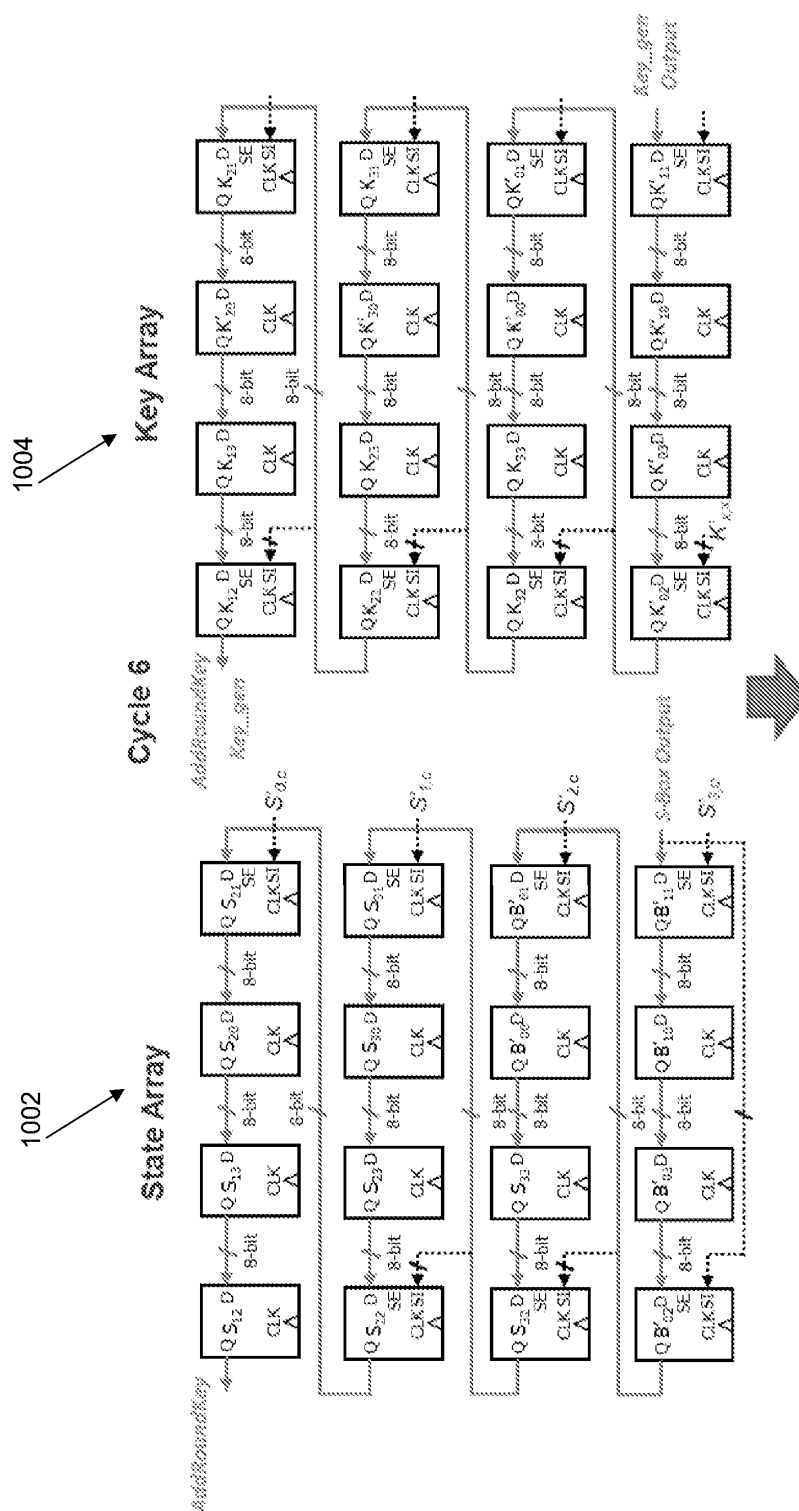


FIG. 11A

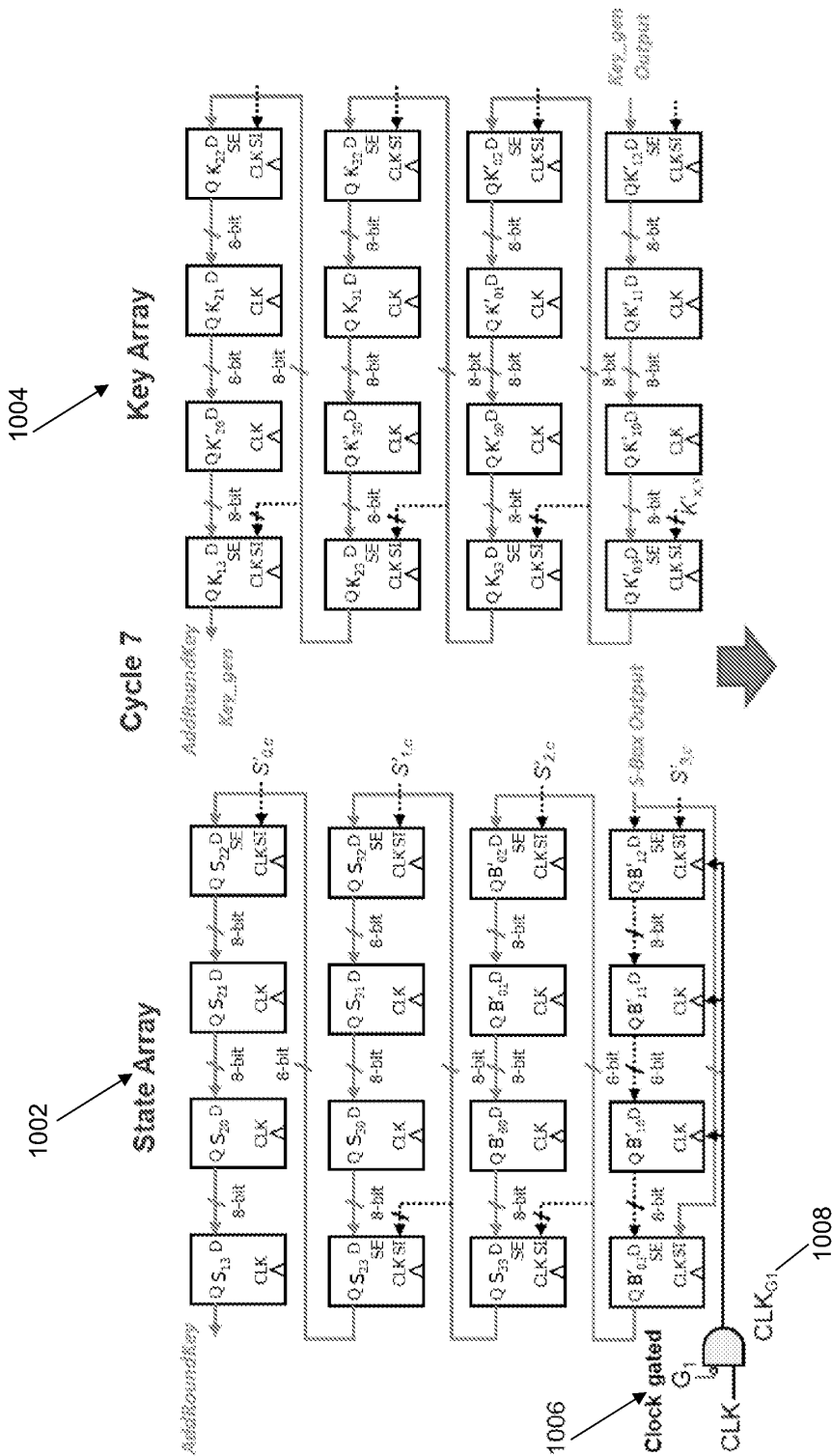


FIG. 11B

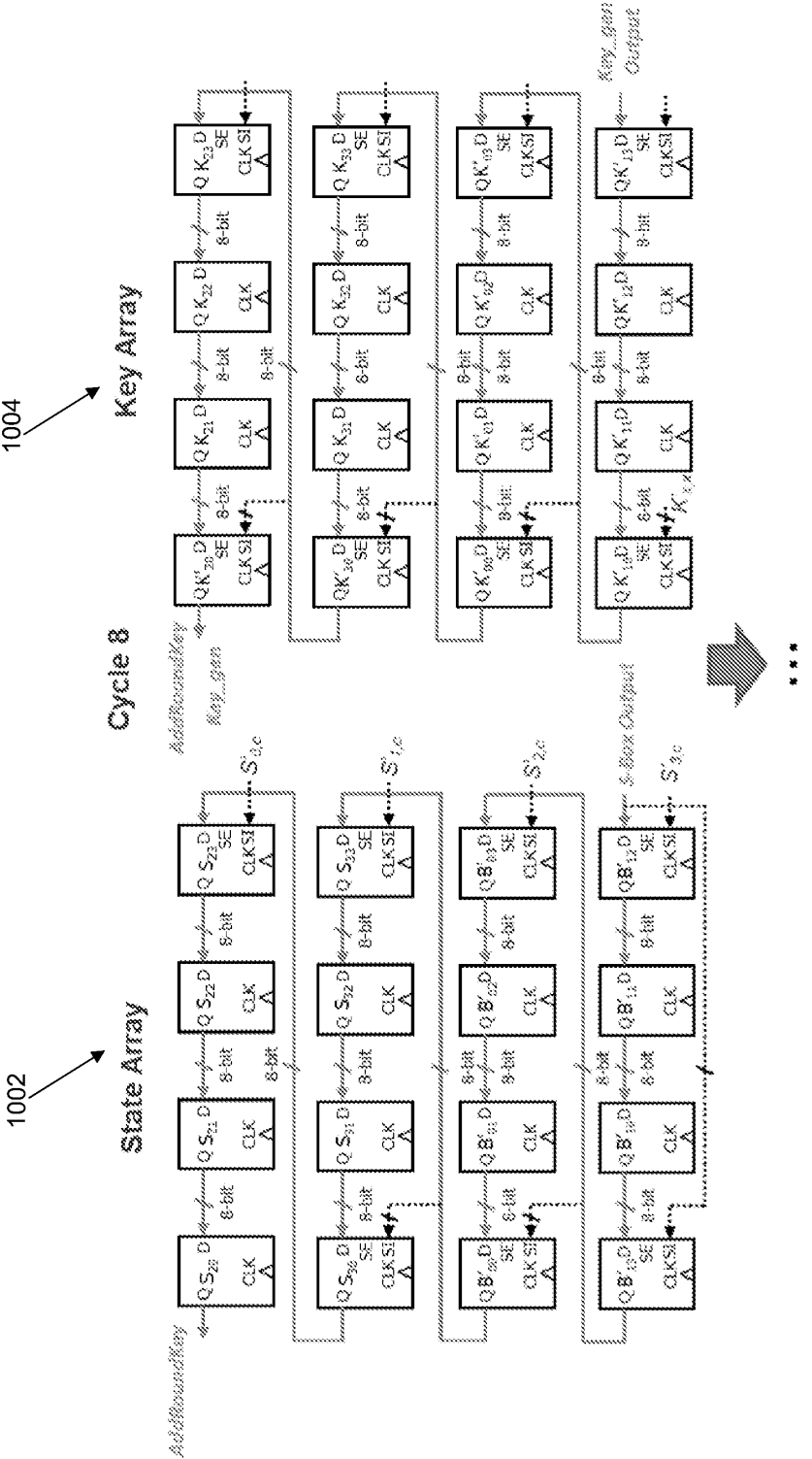


FIG. 11C

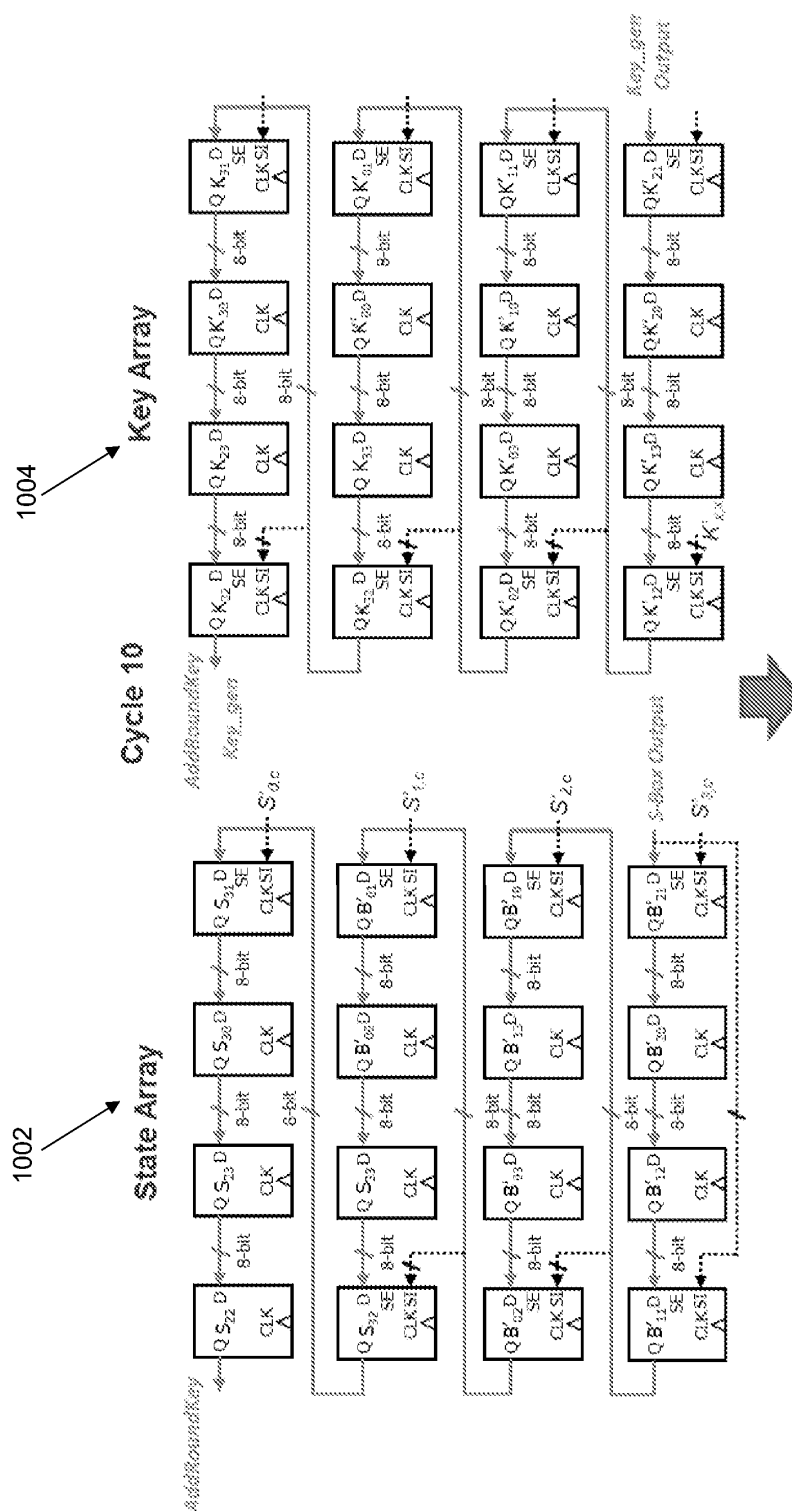


FIG. 12A

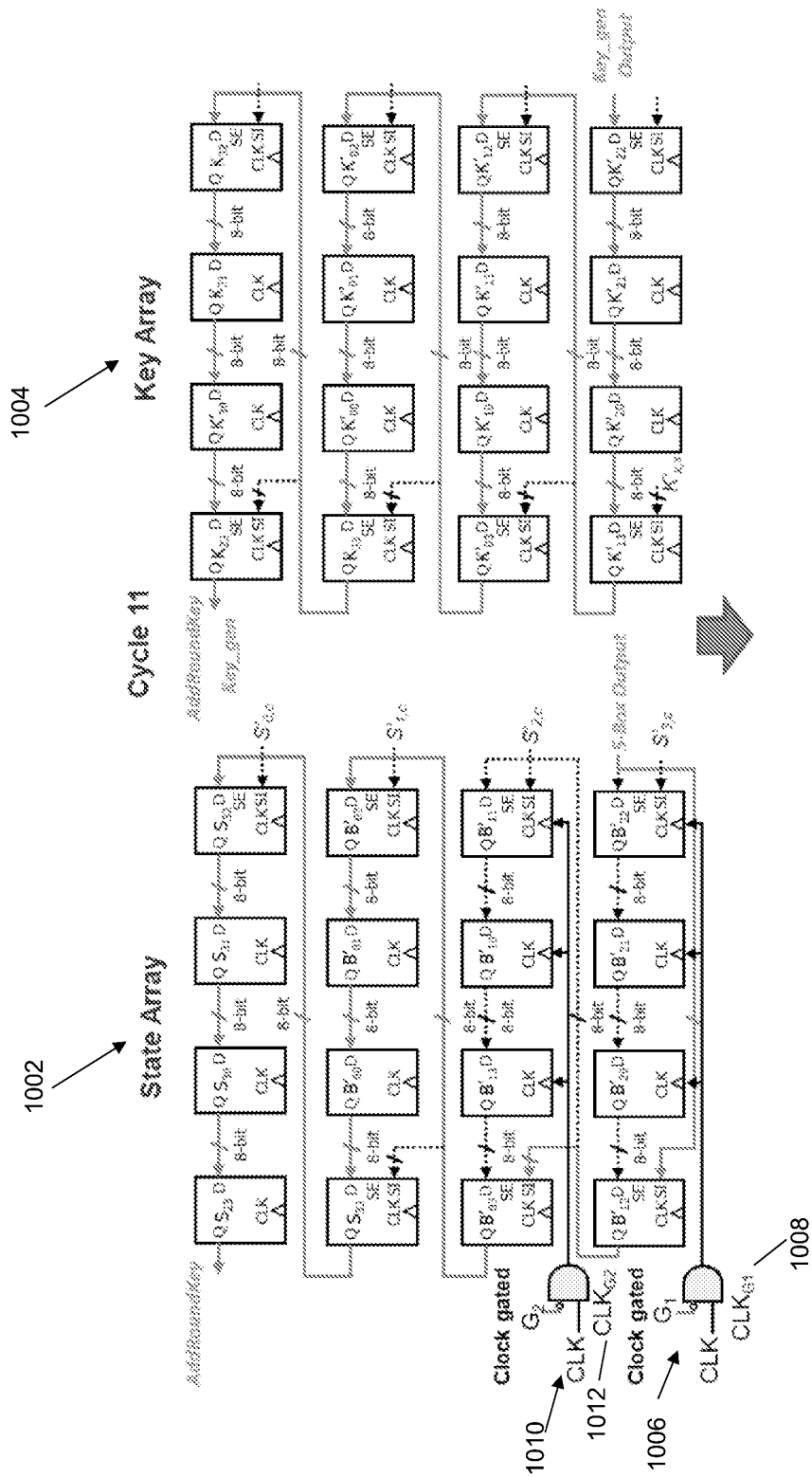


FIG. 12B

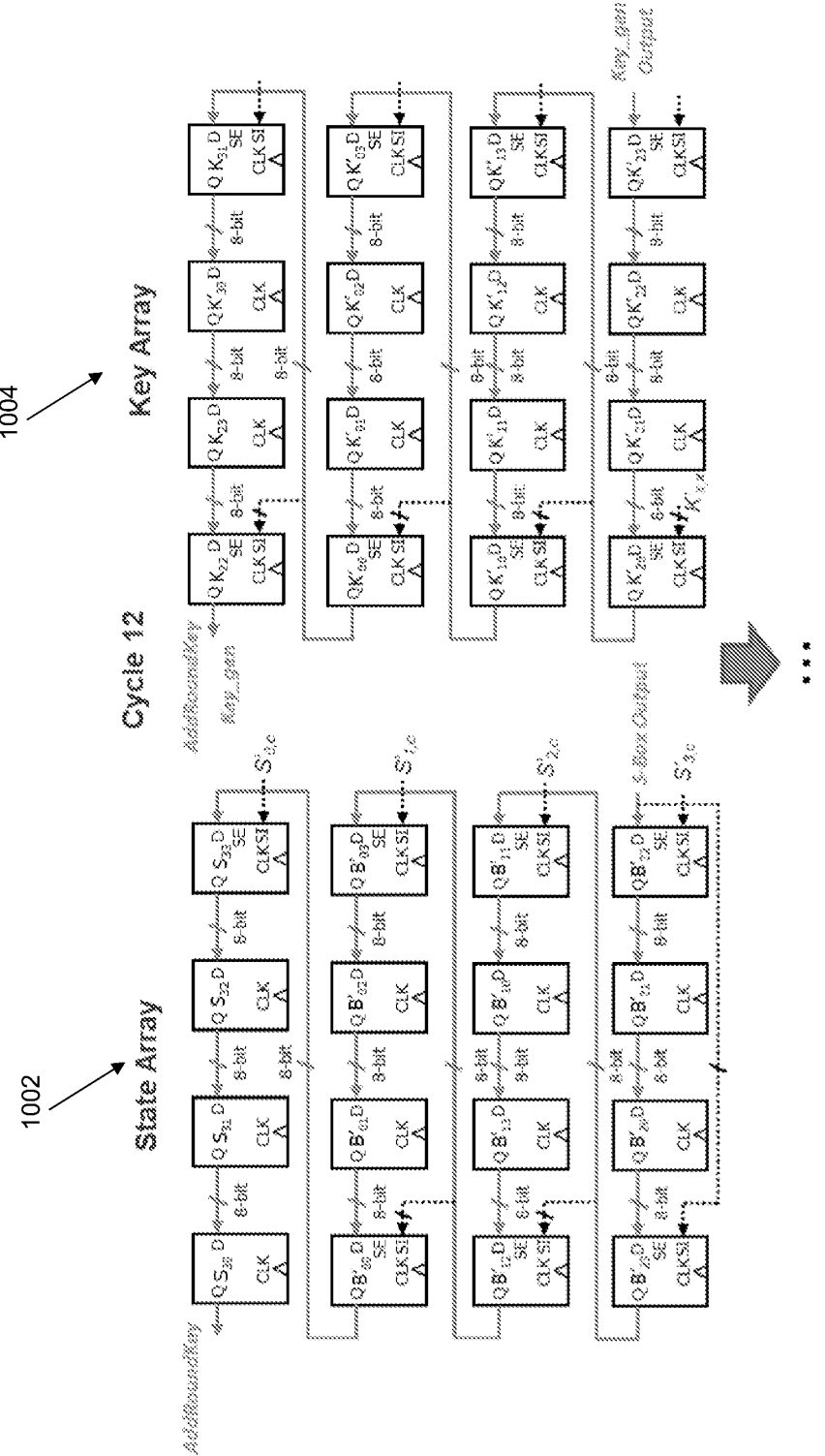


FIG. 12C

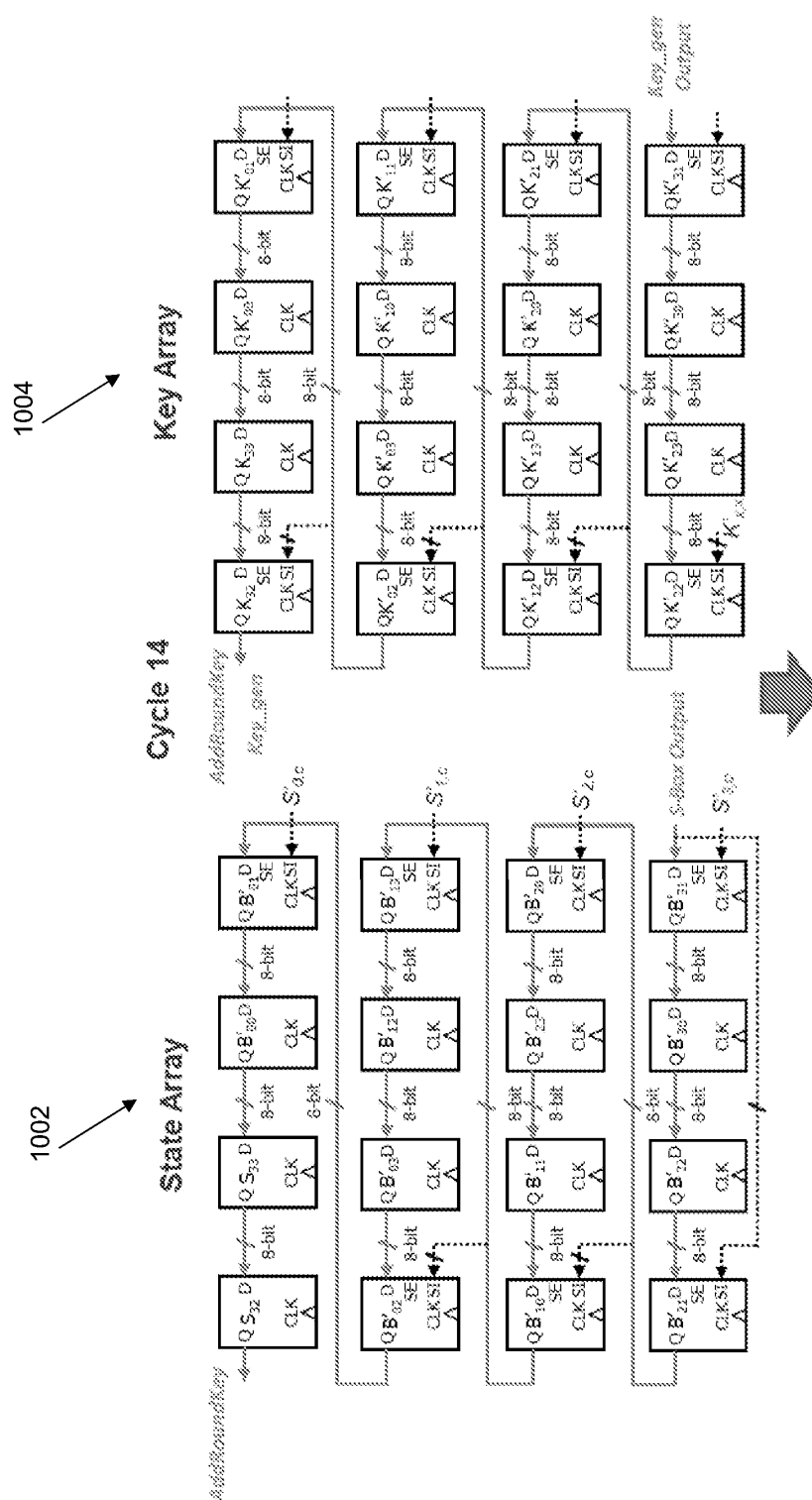
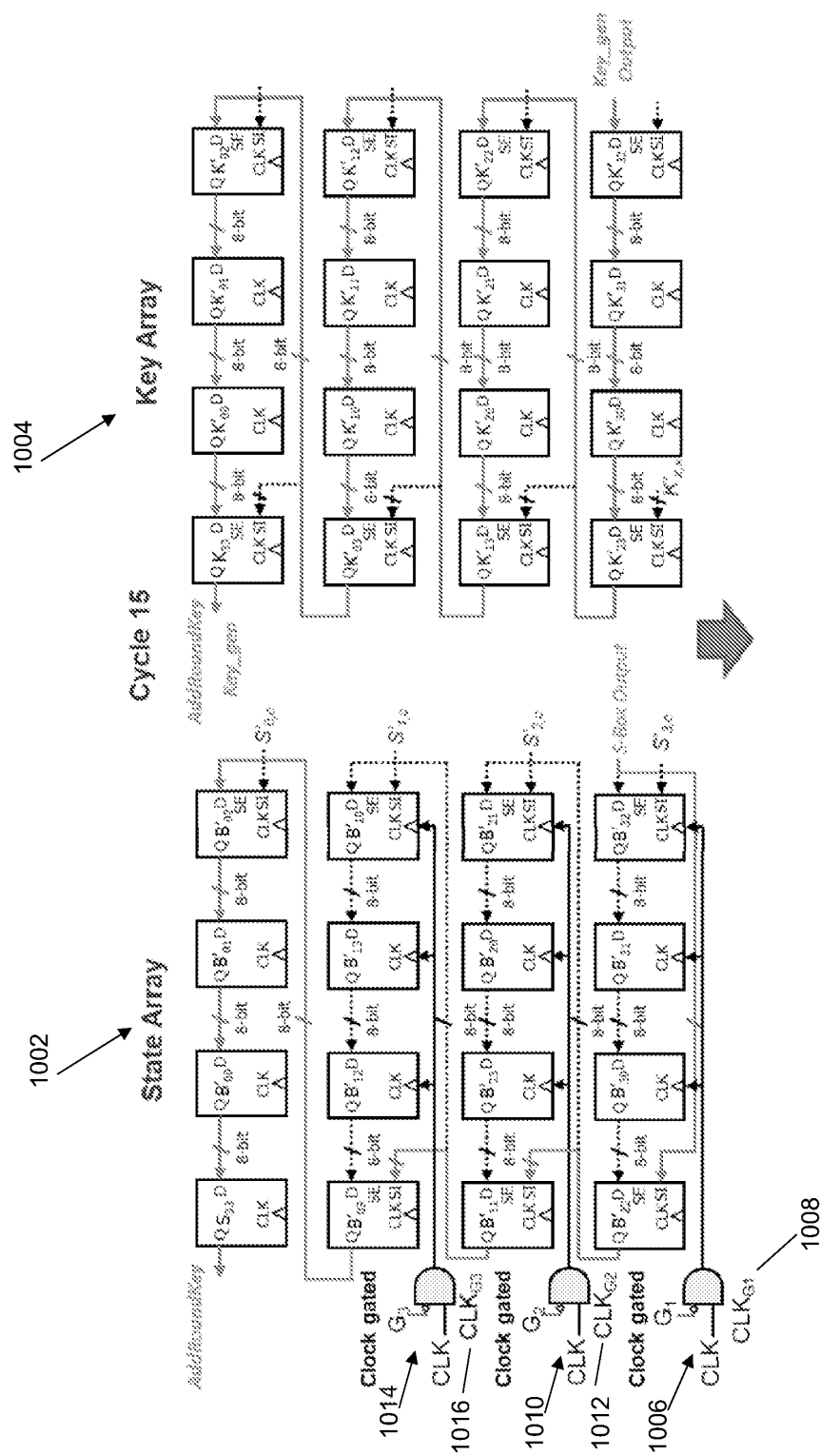


FIG. 13A



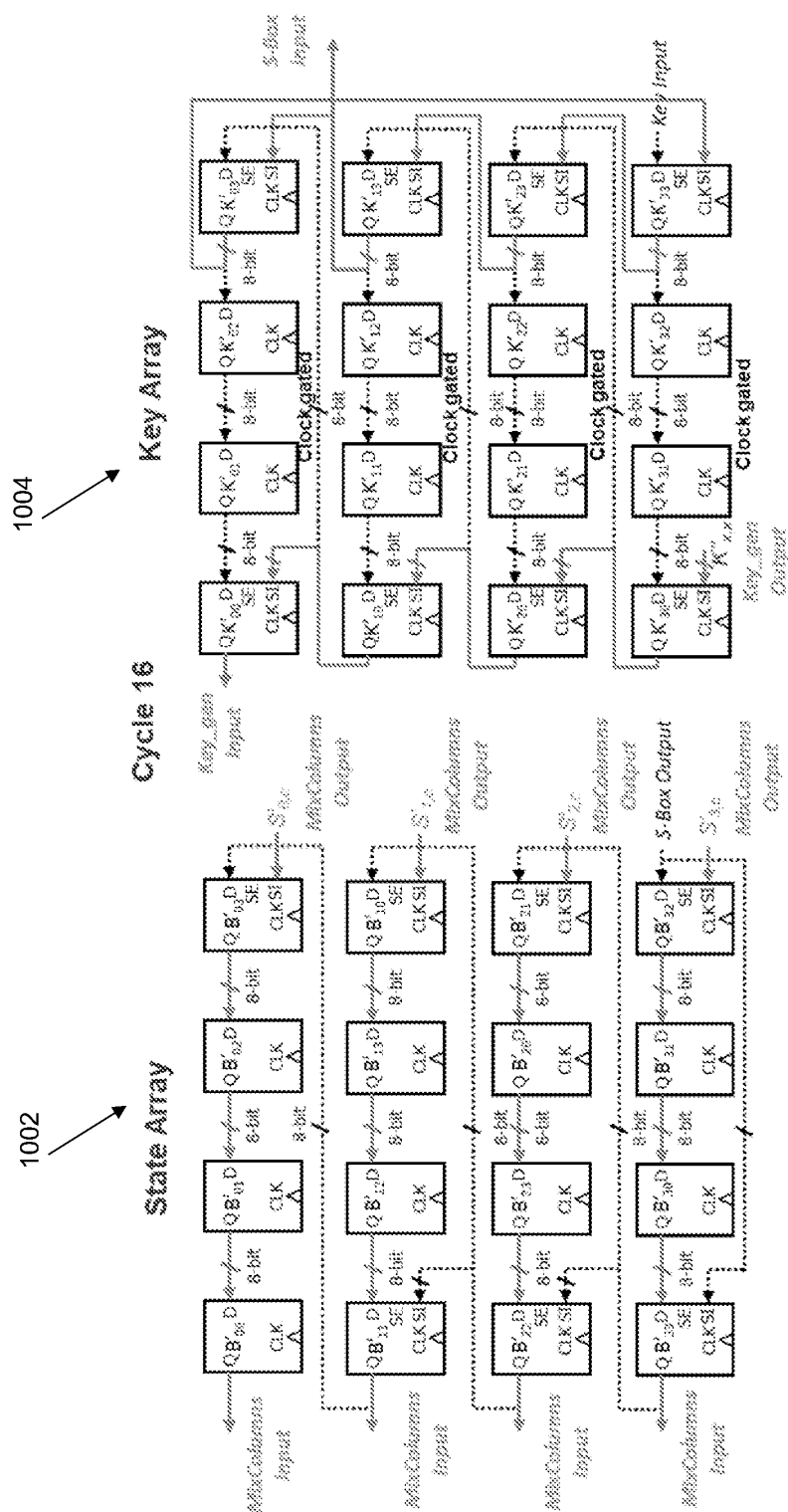


FIG. 13C

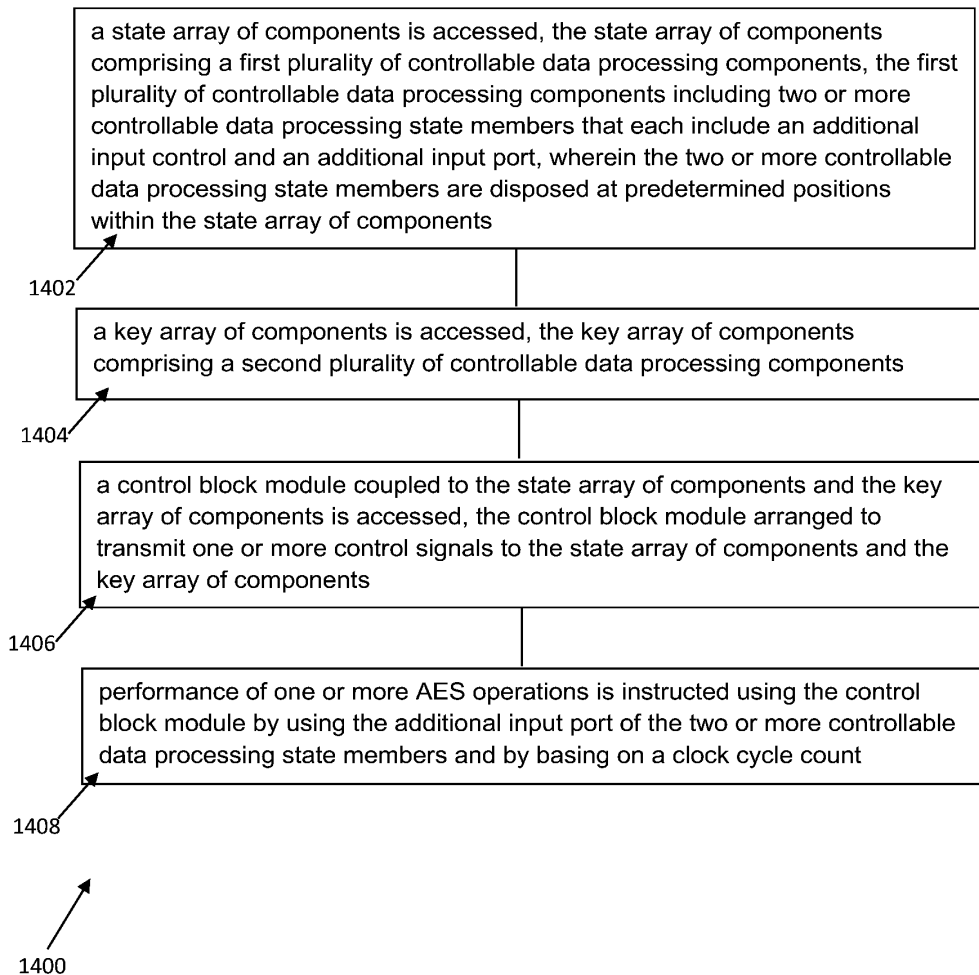


FIG. 14