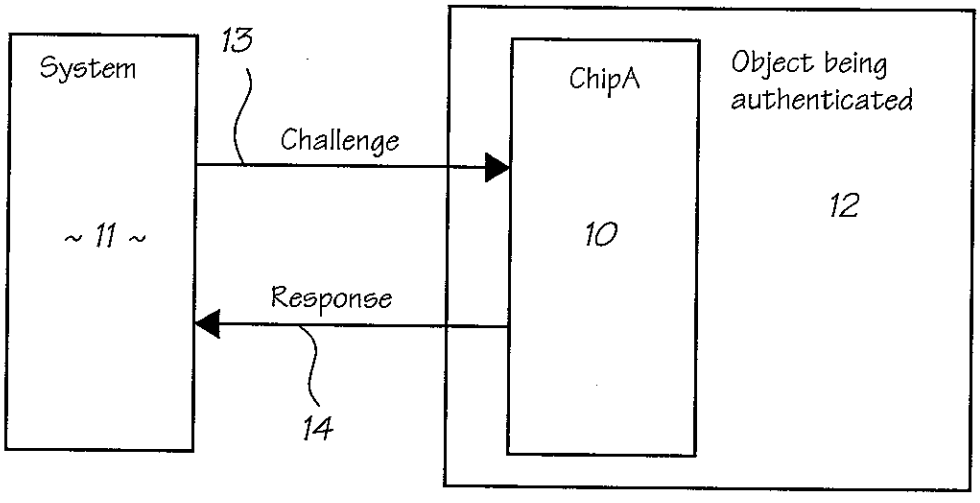

System
13
Challenge
~ 11 ~
Response
14
ChipA
10
Object being
authenticated
12

FIG. 1

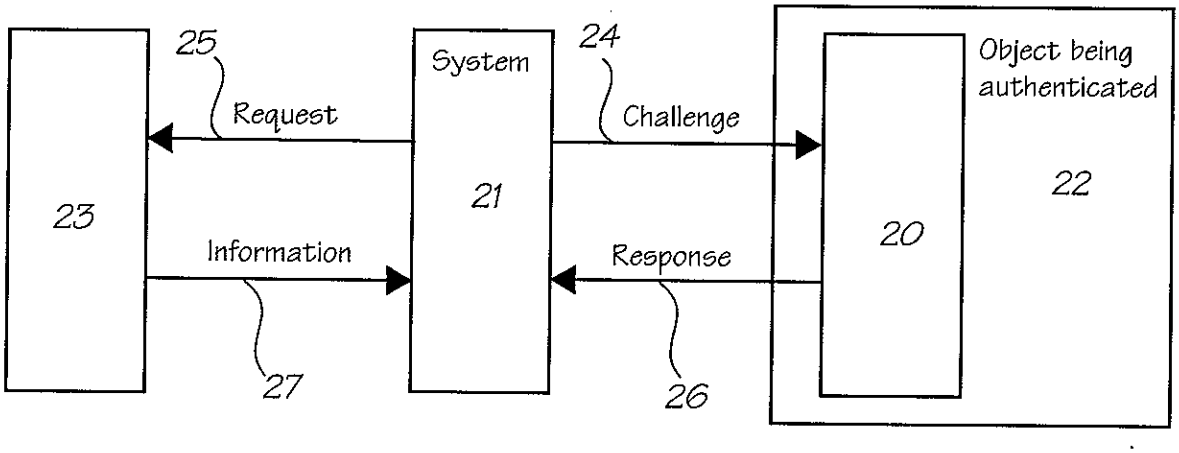

25
Request
23
Information
27
System
21
24
Challenge
Response
26
20
Object being
authenticated
22

FIG. 2

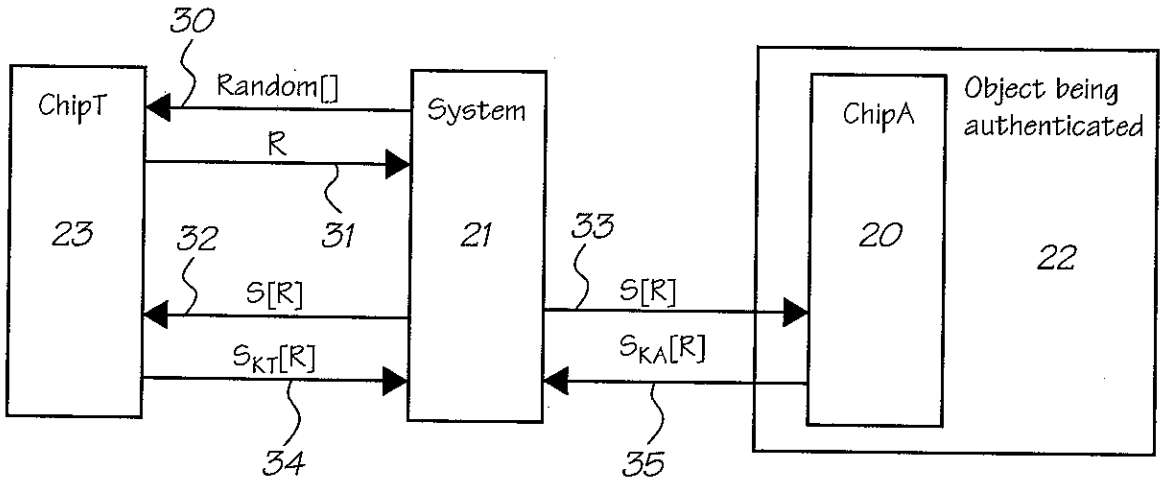

30
Random[]
ChipT
System
ChipA
Object being authenticated
R
23
31
21
20
22
32
33
S[R]
S[R]
$S_{KT}[R]$
$S_{KA}[R]$
34
35

FIG. 3

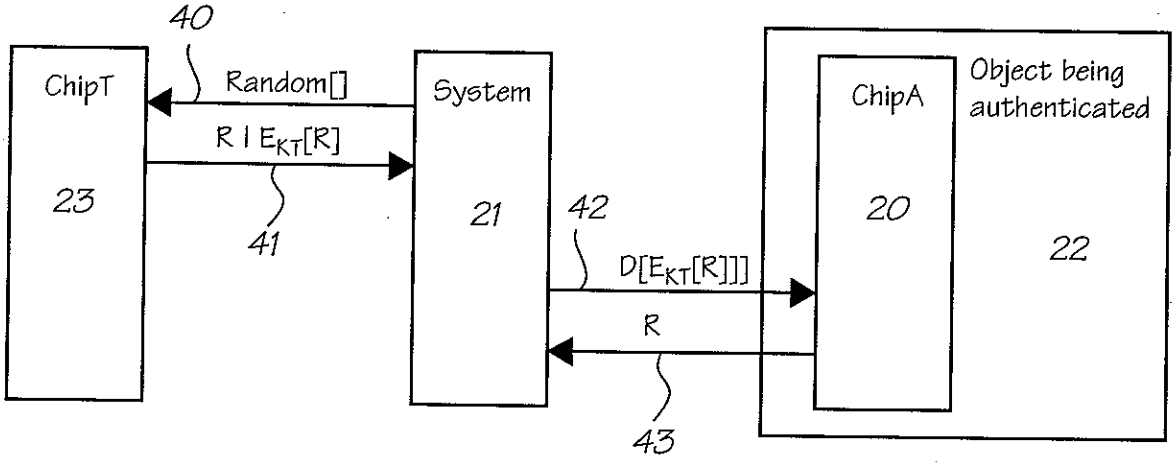

40
Random[]
ChipT
System
ChipA
Object being authenticated
R | $E_{KT}[R]$
23
21
20
22
41
42
$D[E_{KT}[R]]]$
R
43

FIG. 4

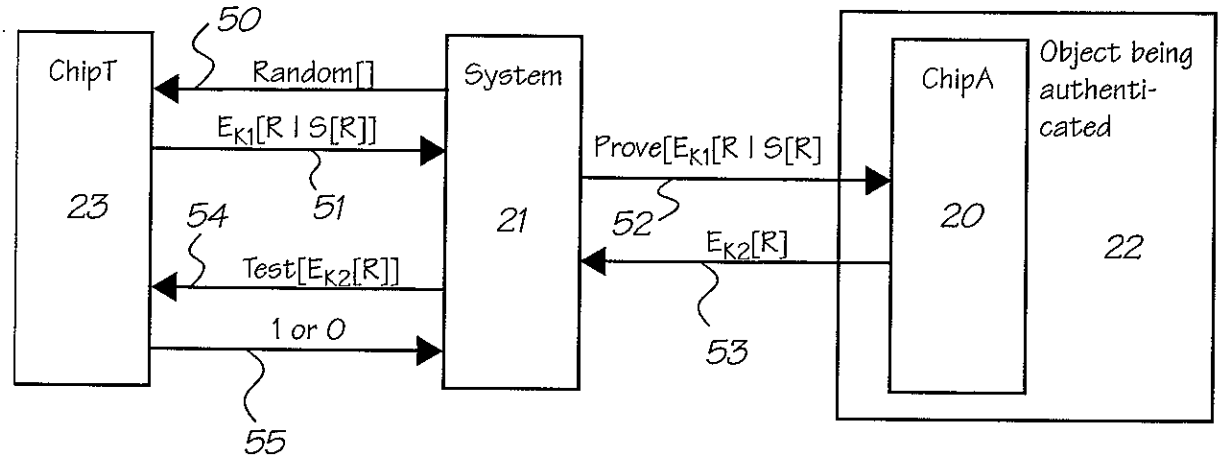

ChipT
23
50
Random[]
E_{K1}[R | S[R]]
51
54
Test[E_{K2}[R]]
1 or 0
55
System
21
Prove[E_{K1}[R | S[R]
52
E_{K2}[R]
53
ChipA
20
Object being authenti-cated
22

FIG. 5

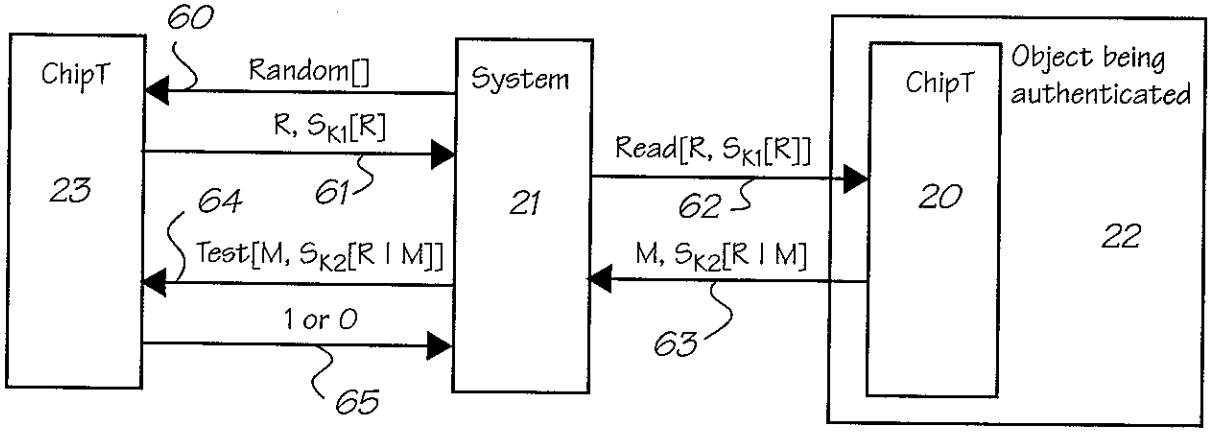

ChipT
23
60
Random[]
R, S_{K1}[R]
61
64
Test[M, S_{K2}[R | M]]
1 or 0
65
System
21
Read[R, S_{K1}[R]]
62
M, S_{K2}[R | M]
63
ChipT
20
Object being authenticated
22

FIG. 6

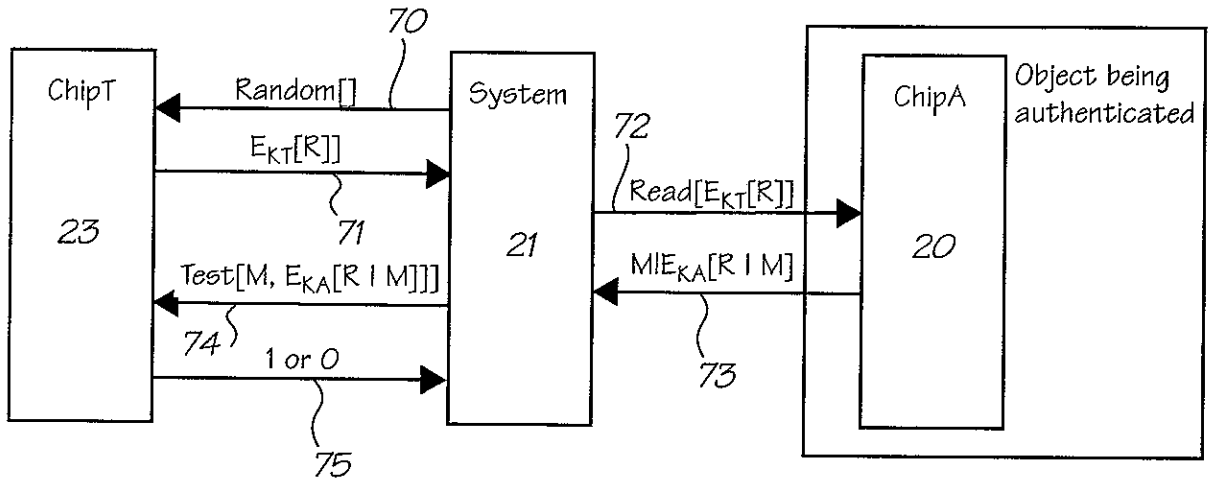

70
ChipT
Random[]
System
72
ChipA
Object being authenticated
$E_{KT}[R]]$
Read[$E_{KT}[R]$]
23
71
21
20
Test[M, $E_{KA}[R \mid M]$]]
M!$E_{KA}[R \mid M]$
74
1 or 0
73
75

FIG. 7

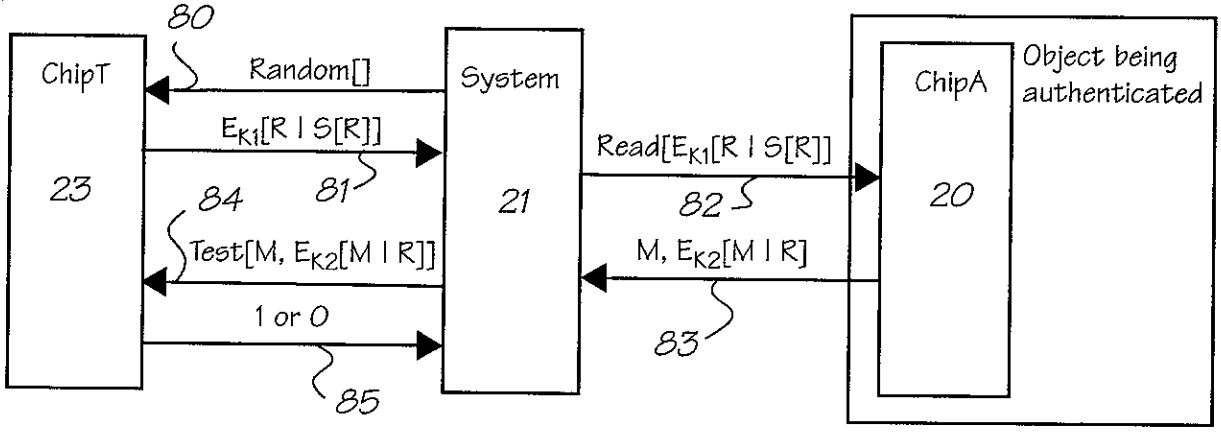

80
ChipT
Random[]
System
ChipA
Object being authenticated
$E_{K1}[R \mid S[R]]$
Read[$E_{K1}[R \mid S[R]]$
23
84
81
21
82
20
Test[M, $E_{K2}[M \mid R]$]
M, $E_{K2}[M \mid R]$
1 or 0
83
85

FIG. 8

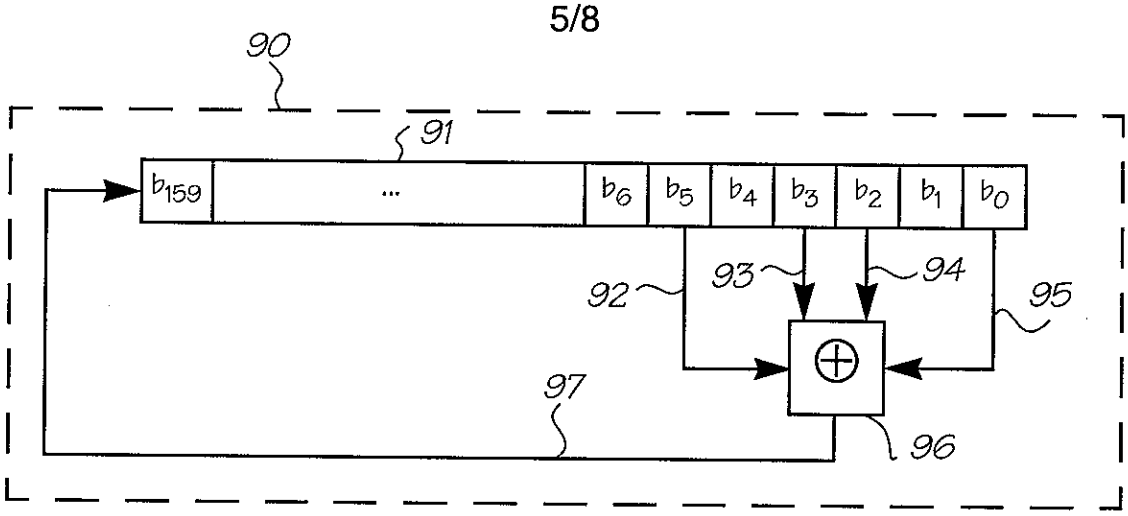


FIG. 9

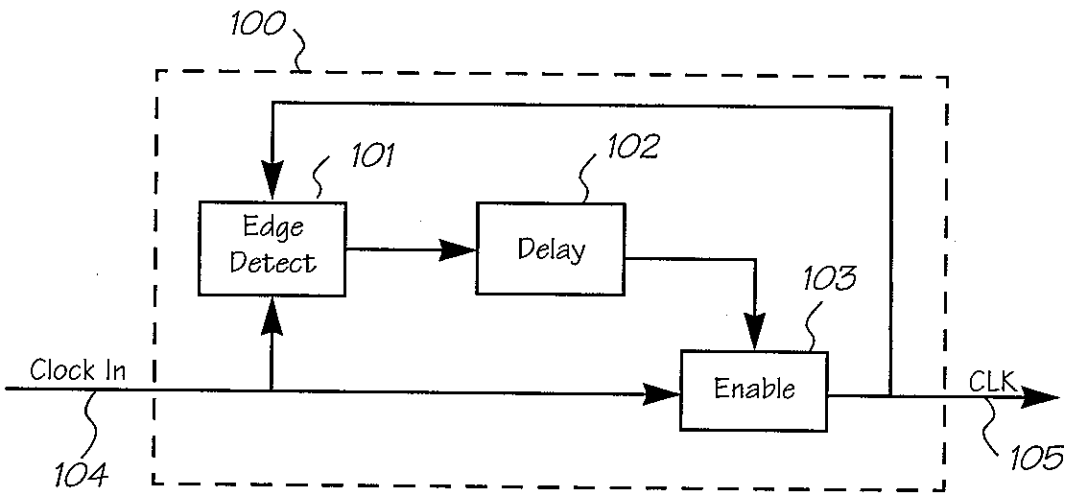


FIG. 10

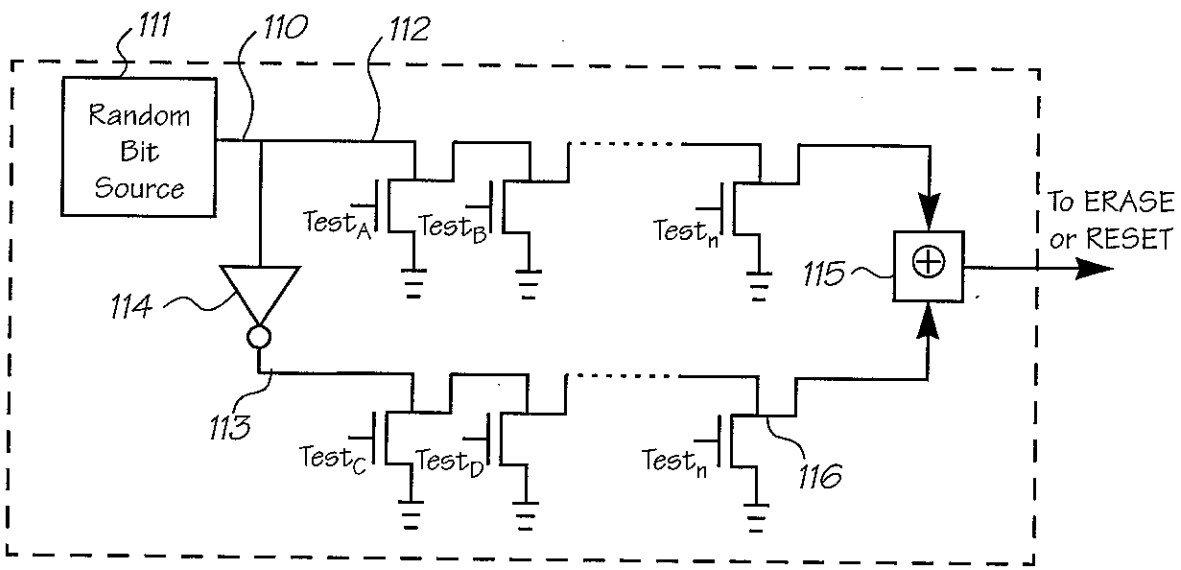


FIG. 11

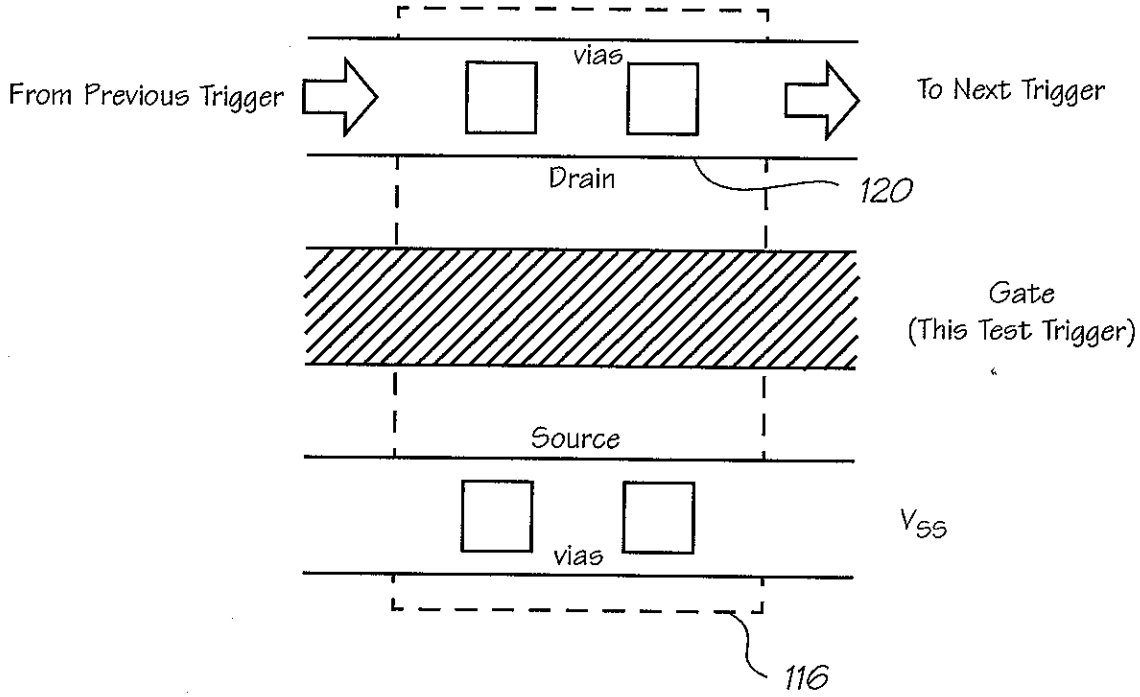

From Previous Trigger
vias
To Next Trigger
Drain
120
Gate
(This Test Trigger)
Source
V_{SS}
vias
116

FIG. 12

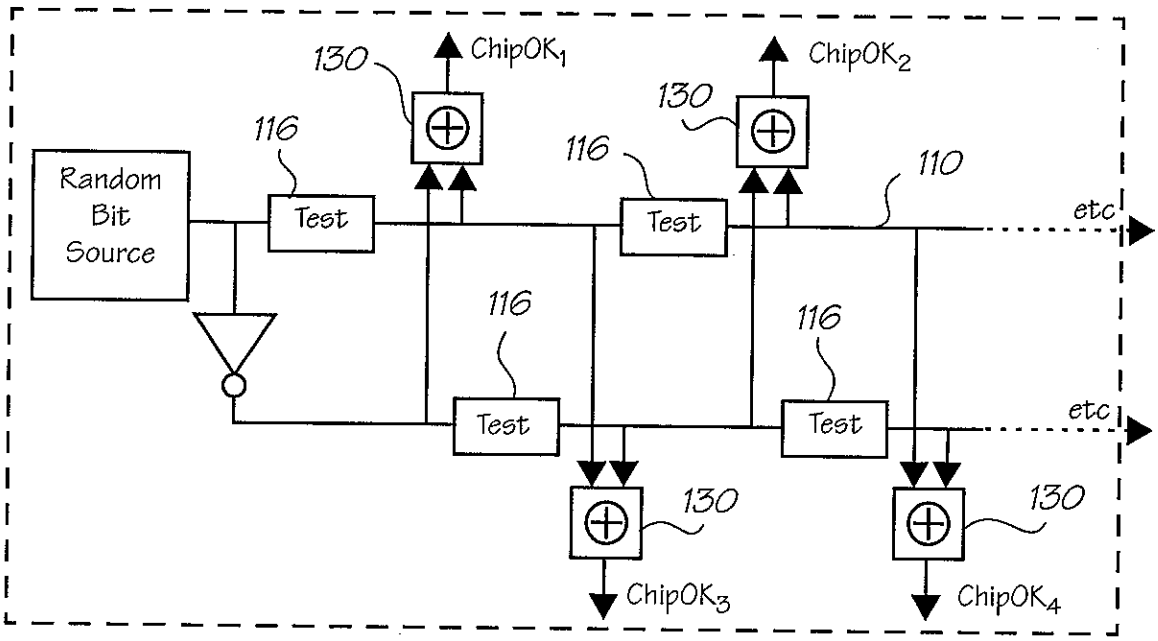

130
ChipOK1
130
ChipOK2
116
116
110
Random
Bit
Source
Test
Test
etc
116
116
Test
Test
etc
130
130
ChipOK3
ChipOK4

FIG. 13

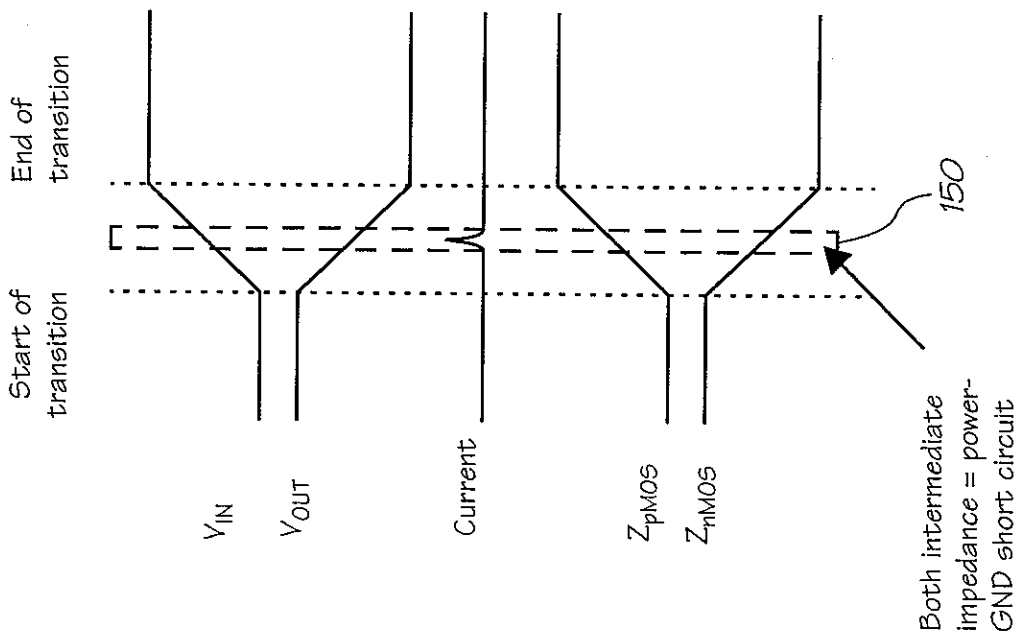

Start of transition
End of transition
V_{IN}
V_{OUT}
Current
Z_{pMOS}
Z_{nMOS}
150
Both intermediate impedance = power-GND short circuit

FIG. 15

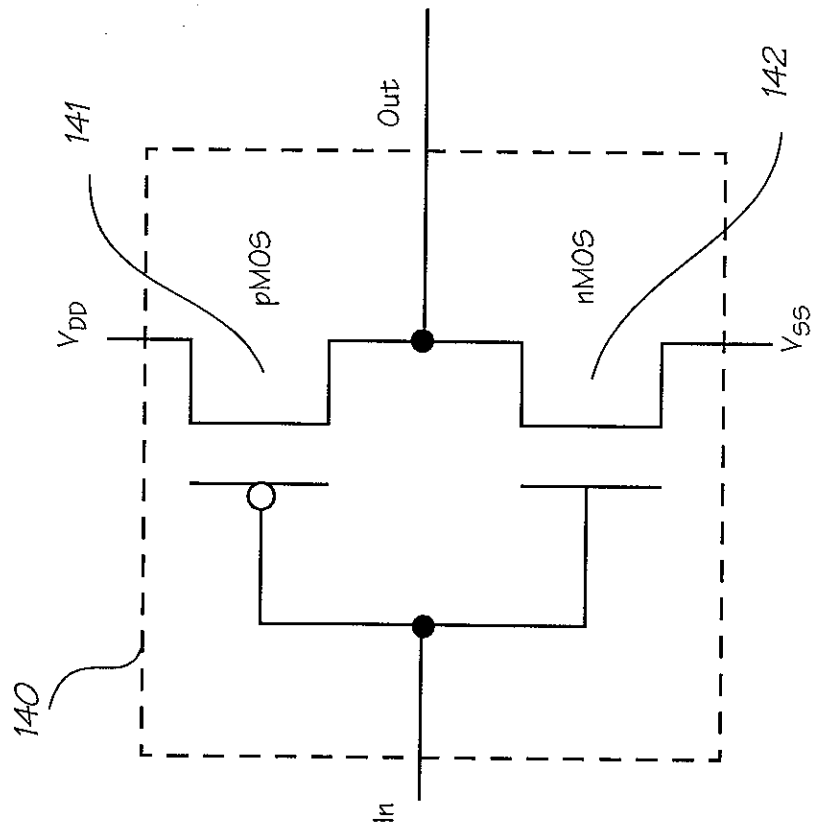

140
141
142
V_{DD}
V_{SS}
pMOS
nMOS
Out
In

FIG. 14

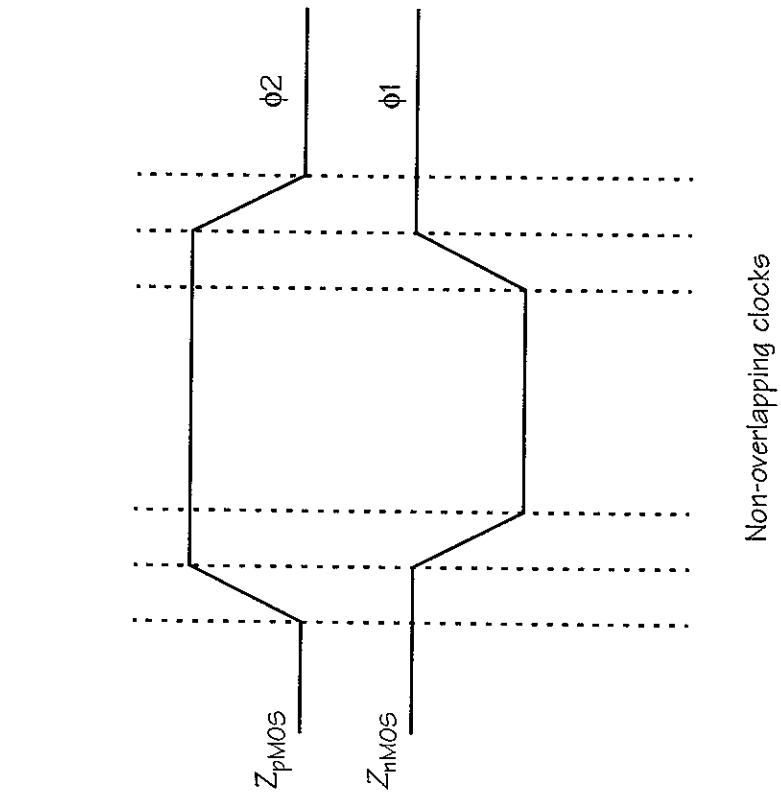

ϕ2
ϕ1
Z_{pMOS}
Z_{nMOS}
Non-overlapping clocks

FIG. 17

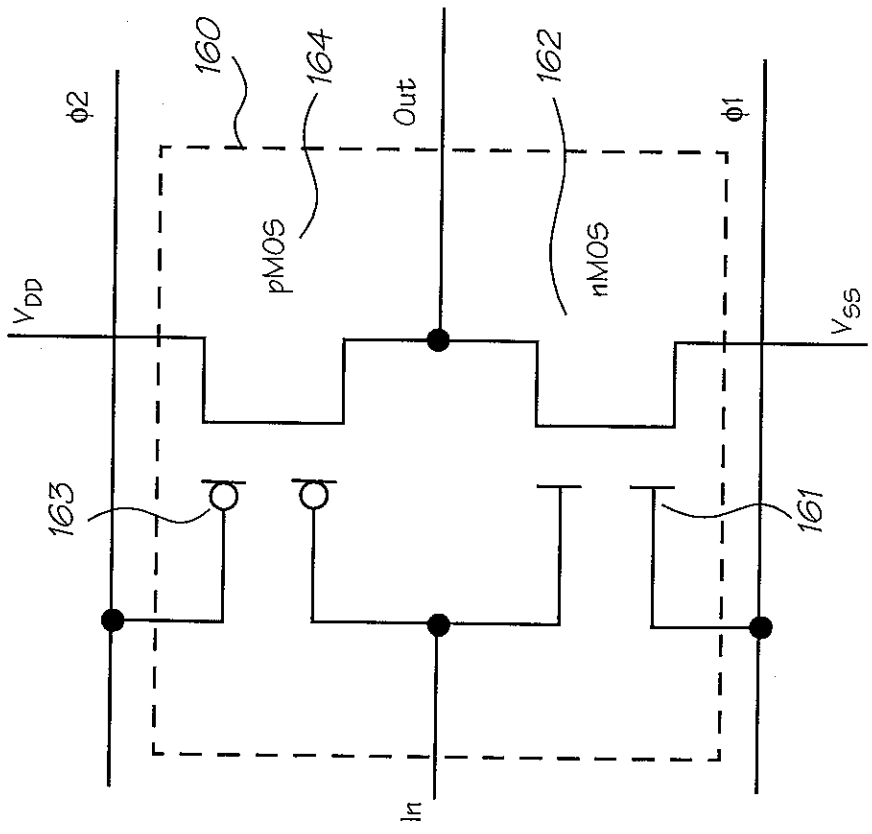

160
164
162
ϕ2
ϕ1
Out
pMOS
nMOS
V_{DD}
V_{SS}
163
161
In

FIG. 16