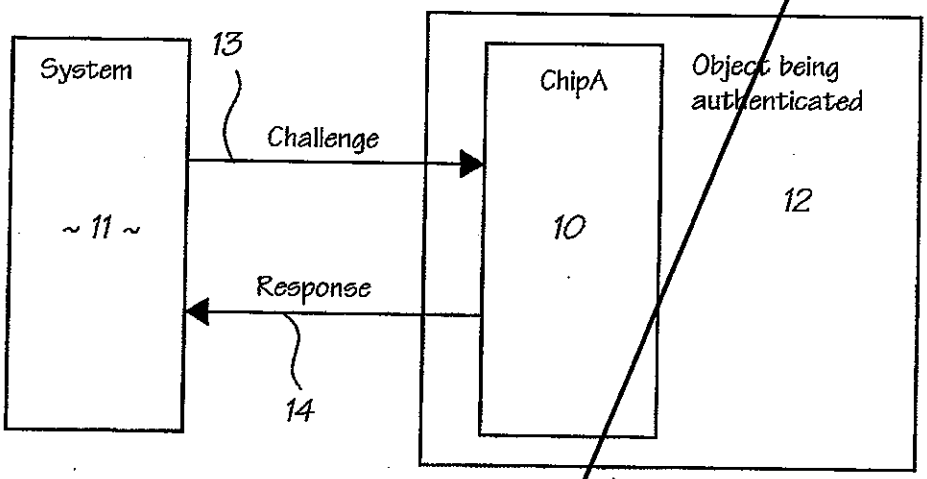

System
13
Challenge
~ 11 ~
Response
14
ChipA
10
Object being authenticated
12

FIG. 1

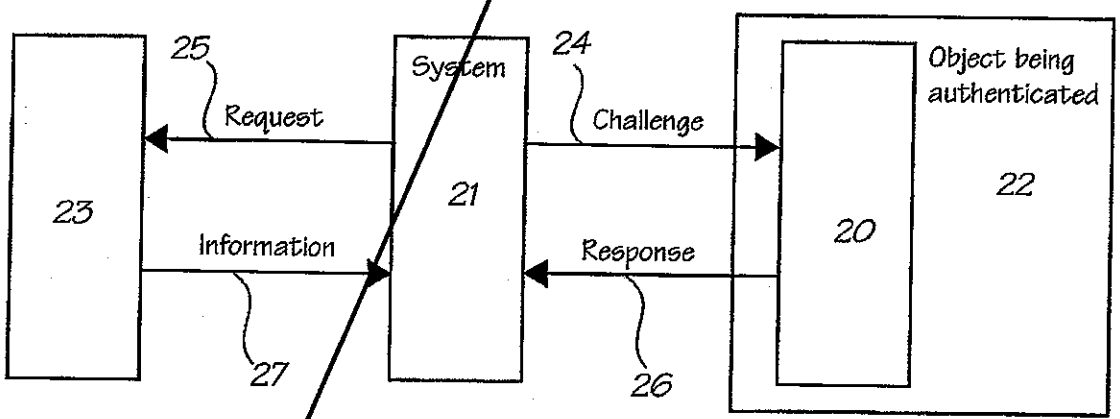

25
Request
23
Information
27
System
21
24
Challenge
Response
26
20
Object being authenticated
22

FIG. 2

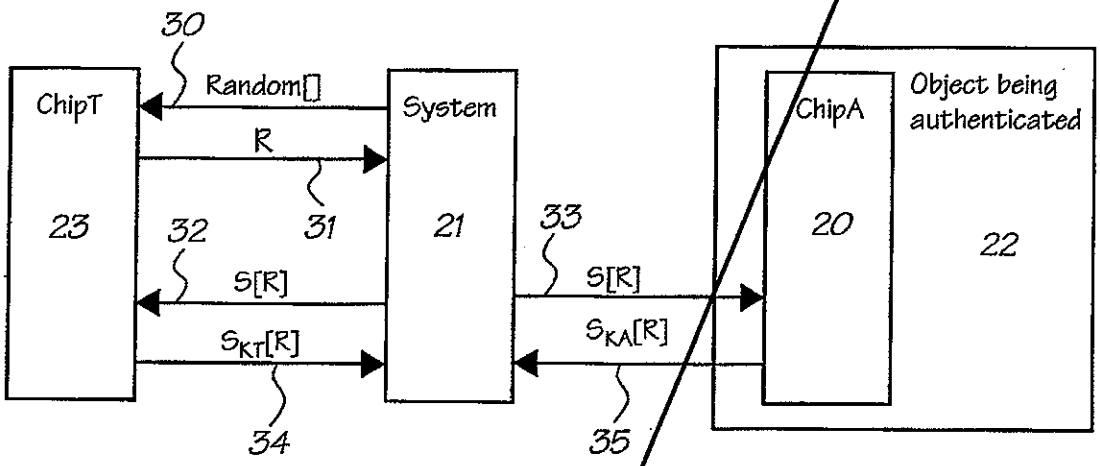

30
Random[]
ChipT
23
System
21
R
31
32
S[R]
$S_{KT}[R]$
34
33
S[R]
$S_{KA}[R]$
35
ChipA
20
Object being authenticated
22

FIG. 3

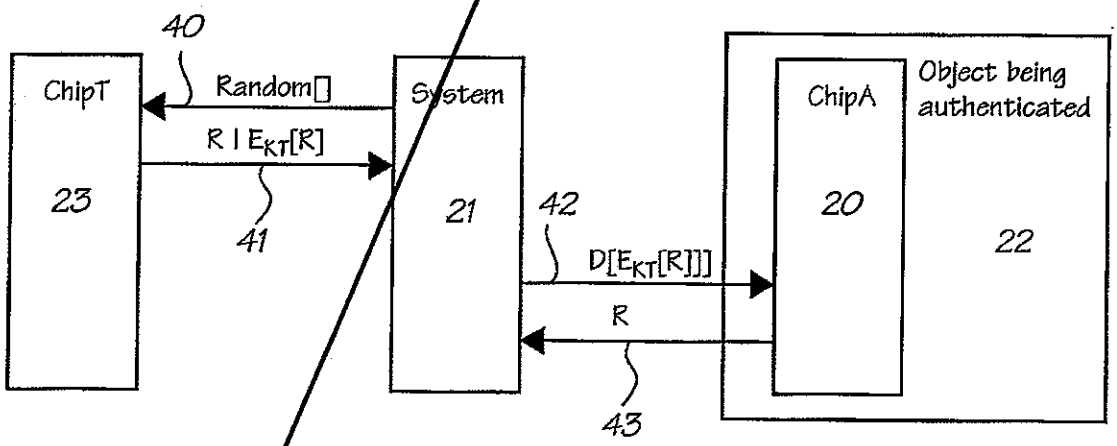

40
Random[]
ChipT
23
R | $E_{KT}[R]$
41
System
21
42
$D[E_{KT}[R]]$
R
43
ChipA
20
Object being authenticated
22

FIG. 4

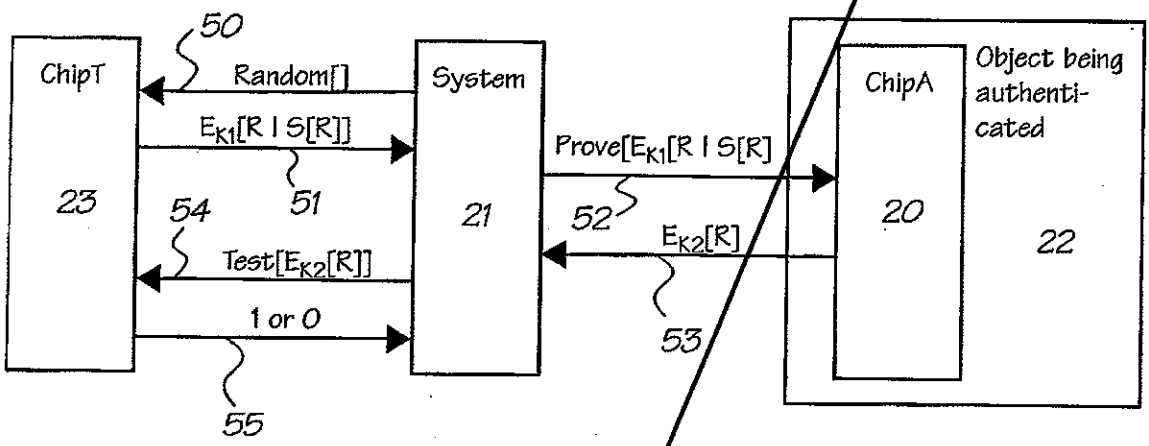

ChipT
23
50
Random[]
$E_{K1}[R \mid S[R]]$
51
54
$Test[E_{K2}[R]]$
1 or 0
55
System
21
$Prove[E_{K1}[R \mid S[R]$
52
$E_{K2}[R]$
53
ChipA
20
Object being authenti-cated
22

FIG. 5

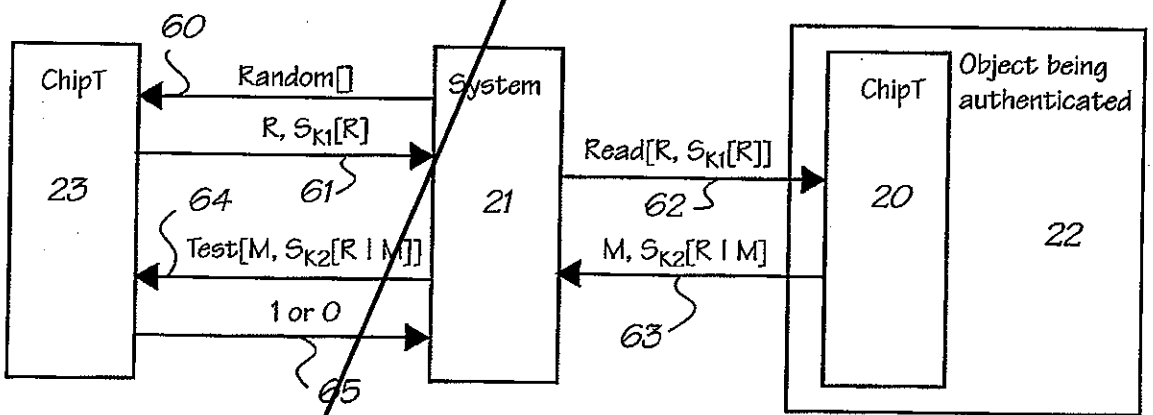

ChipT
23
60
Random[]
$R, S_{K1}[R]$
61
64
$Test[M, S_{K2}[R \mid M]]$
1 or 0
65
System
21
$Read[R, S_{K1}[R]]$
62
$M, S_{K2}[R \mid M]$
63
ChipT
20
Object being authenticated
22

FIG. 6

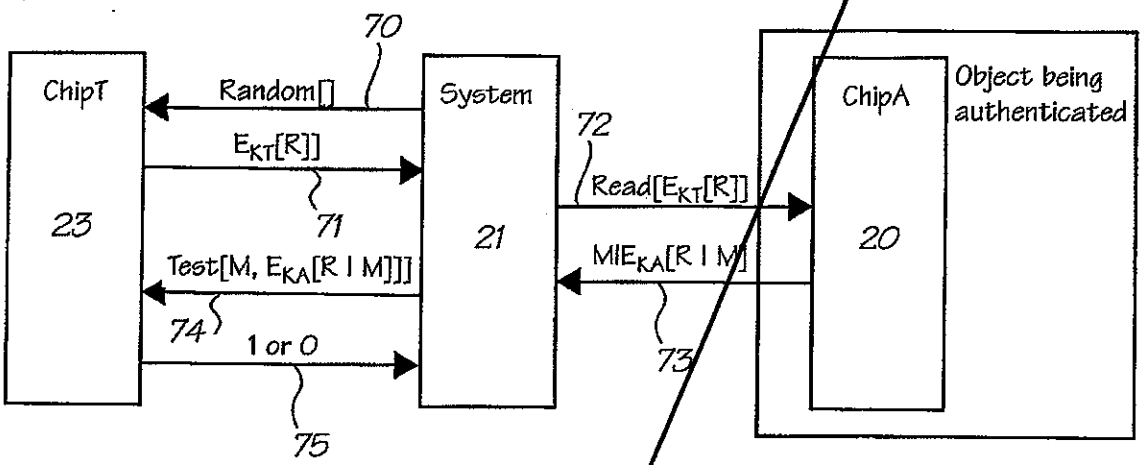

ChipT
23
Random[]
70
System
21
$E_{KT}[R]]$
71
Test[M, E_{KA}[R | M]]]
74
1 or 0
75
72
Read[E_{KT}[R]]
M|E_{KA}[R | M]
73
ChipA
20
Object being authenticated

FIG. 7

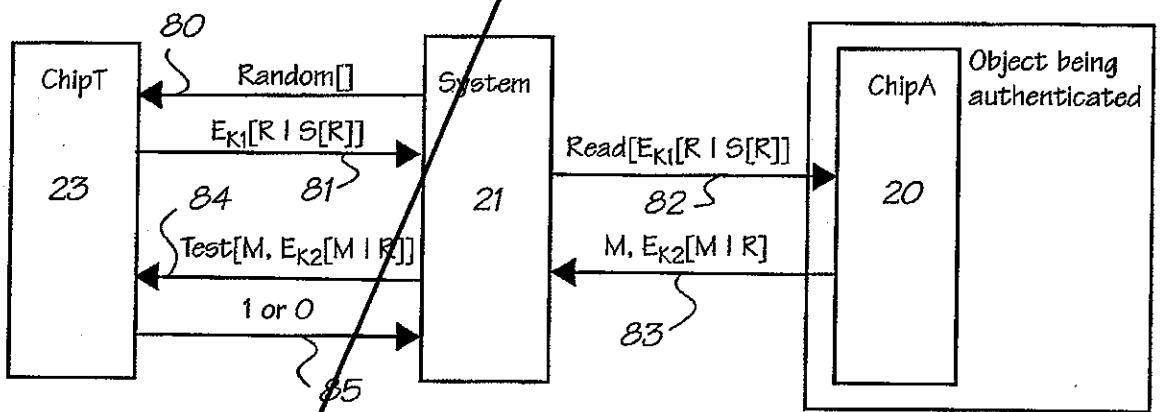

ChipT
23
80
Random[]
System
21
E_{K1}[R | S[R]]
81
84
Test[M, E_{K2}[M | R]]
1 or 0
85
Read[E_{K1}[R | S[R]]
82
M, E_{K2}[M | R]
83
ChipA
20
Object being authenticated

FIG. 8

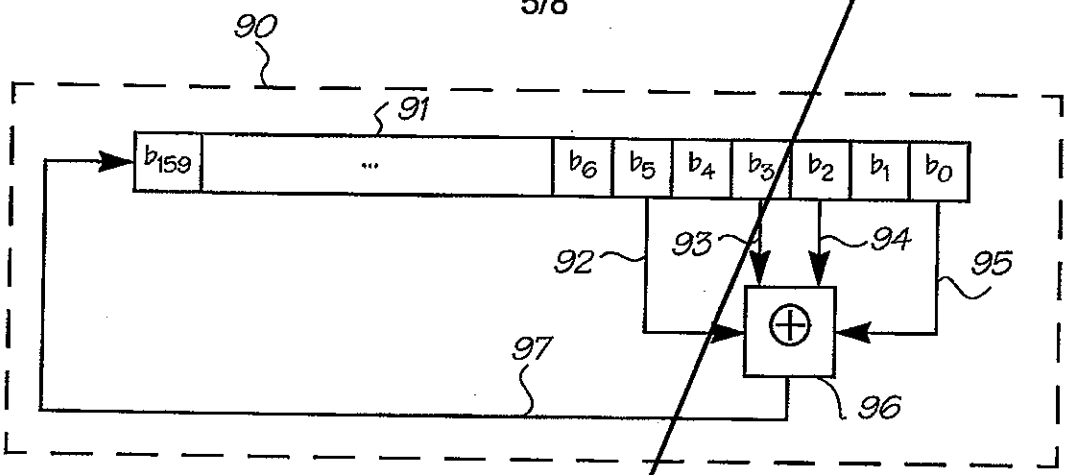


FIG. 9

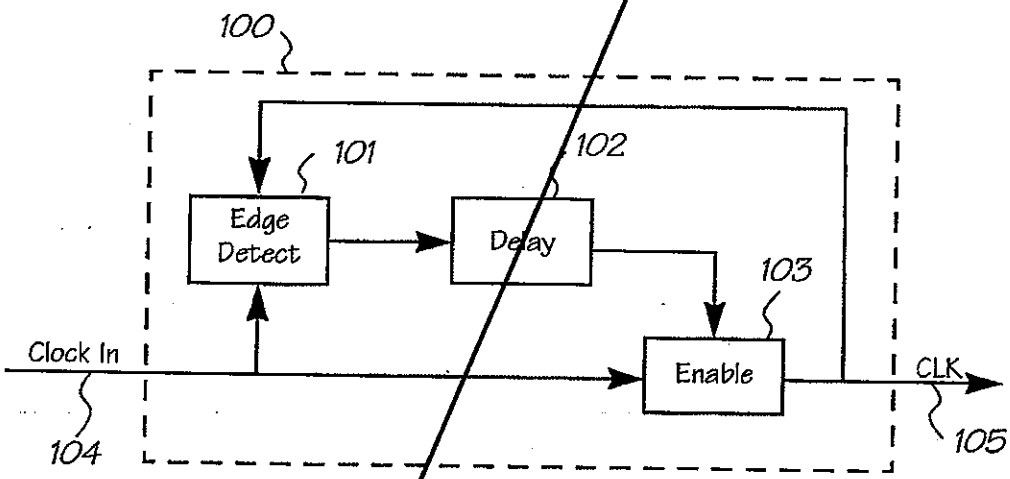


FIG. 10

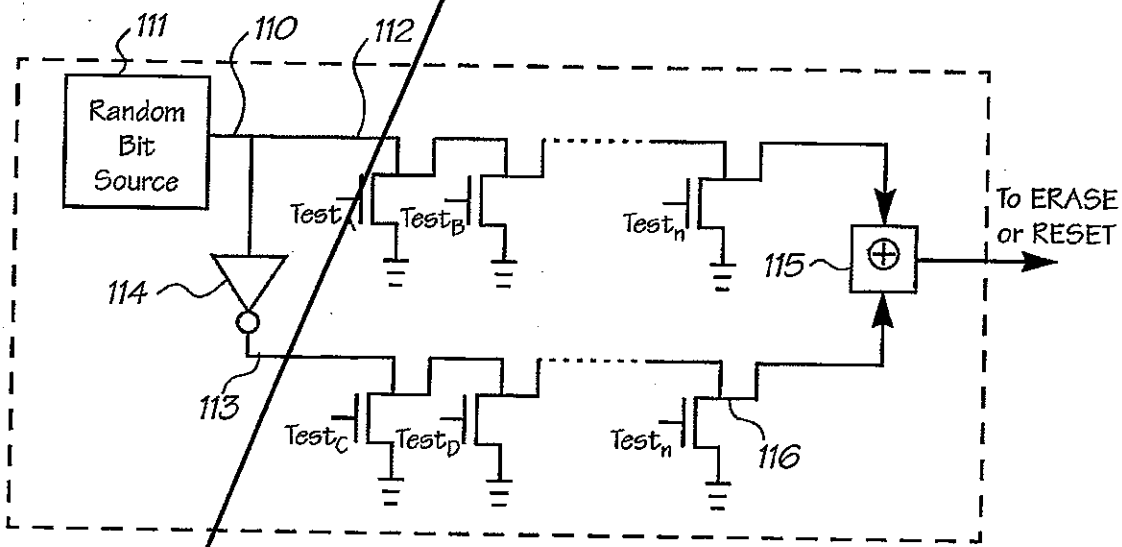


FIG. 11

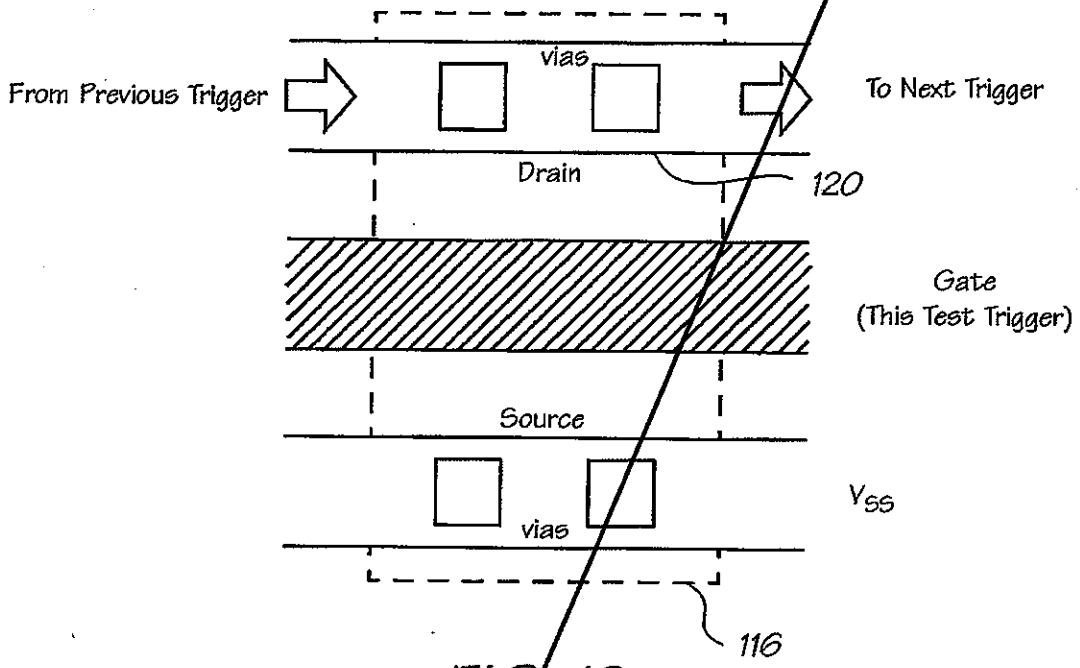

From Previous Trigger
vias
To Next Trigger
Drain
120
Gate
(This Test Trigger)
Source
V_{SS}
vias
116

FIG. 12

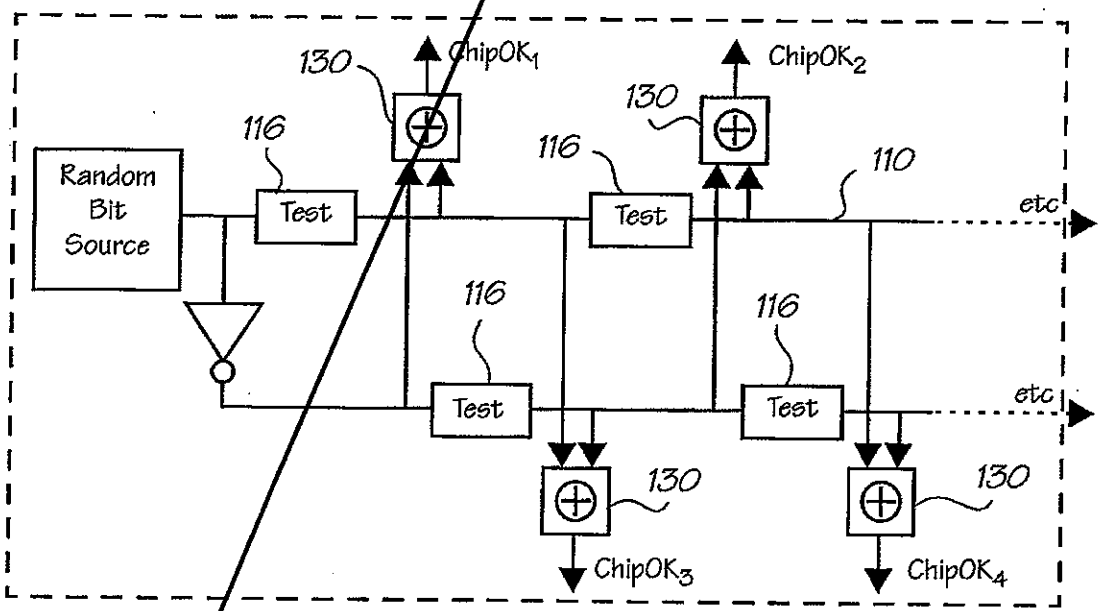

130
ChipOK1
ChipOK2
130
116
116
110
Random Bit Source
Test
Test
etc
116
116
Test
Test
etc
130
130
ChipOK3
ChipOK4

FIG. 13

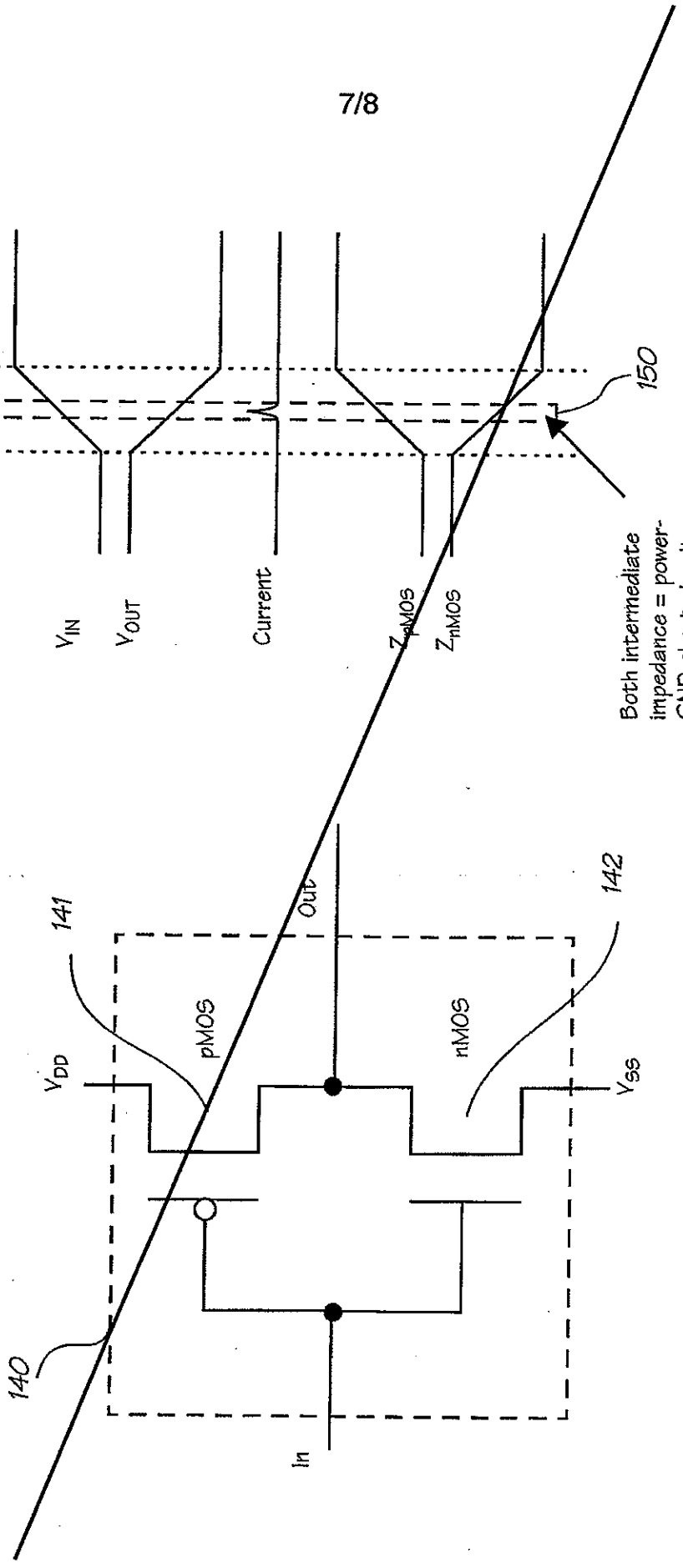

140
141
142
pMOS
nMOS
V_{DD}
V_{SS}
In
Out
V_{IN}
V_{OUT}
Current
Z_{pMOS}
Z_{nMOS}
Start of transition
End of transition
150
Both intermediate impedance = power-GND short circuit

FIG. 14

FIG. 15

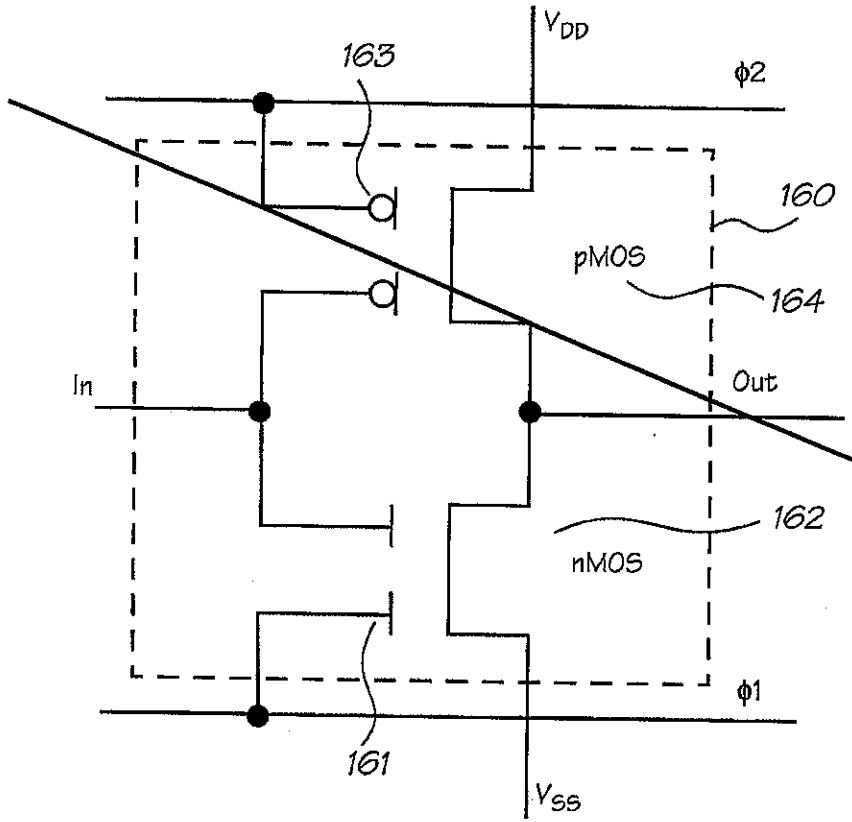

V_{DD}
163
$\phi 2$
160
pMOS
164
In
Out
162
nMOS
$\phi 1$
161
V_{SS}

FIG. 16

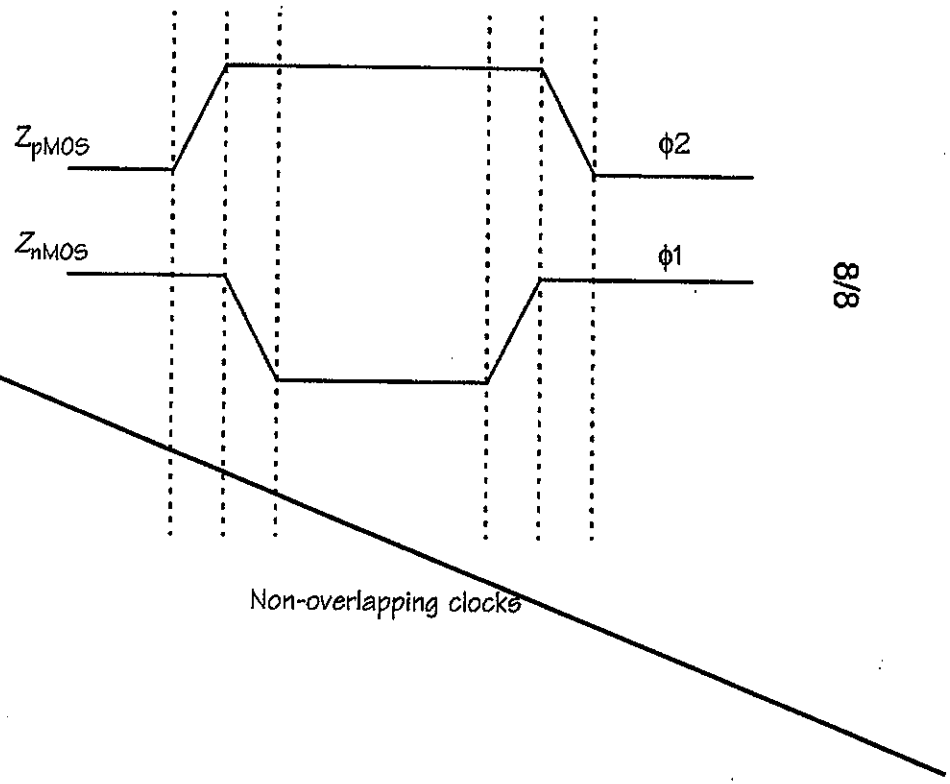

Z_{pMOS}
$\phi 2$
Z_{nMOS}
$\phi 1$
Non-overlapping clocks

FIG. 17

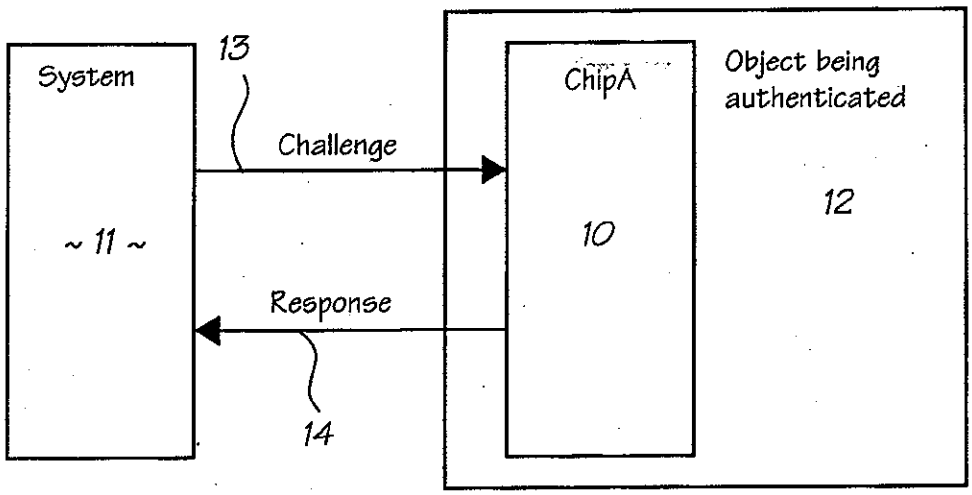

System
13
Challenge
~ 11 ~
Response
14
ChipA
10
Object being authenticated
12

FIG. 1

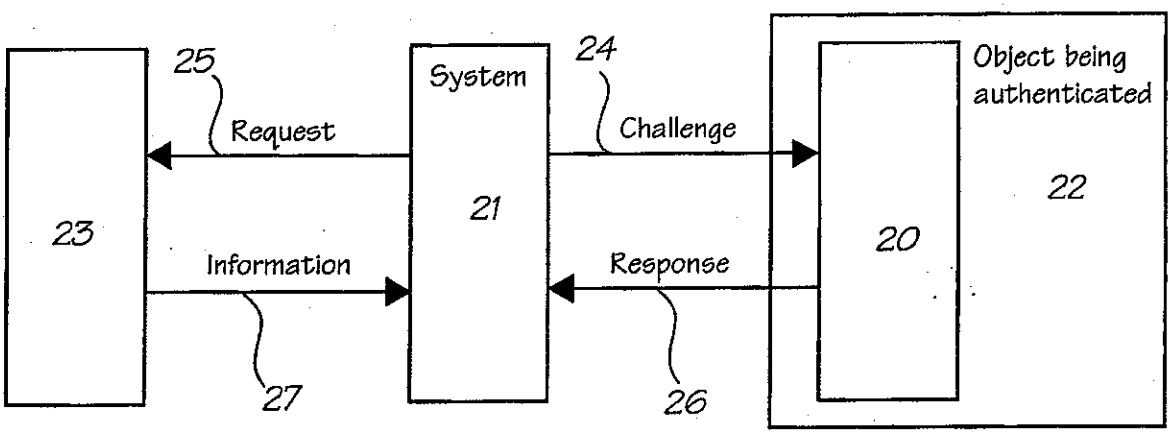

25
Request
23
Information
27
System
21
24
Challenge
Response
26
20
Object being authenticated
22

FIG. 2

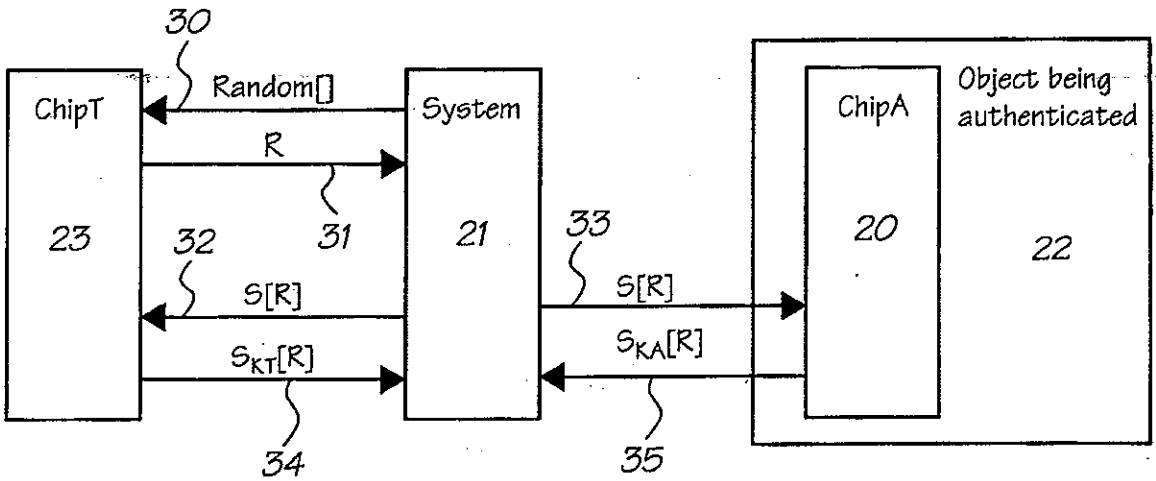

30
Random[]
ChipT
23
System
21
R
31
32
S[R]
$S_{KT}[R]$
34
33
S[R]
$S_{KA}[R]$
35
ChipA
20
Object being authenticated
22

FIG. 3

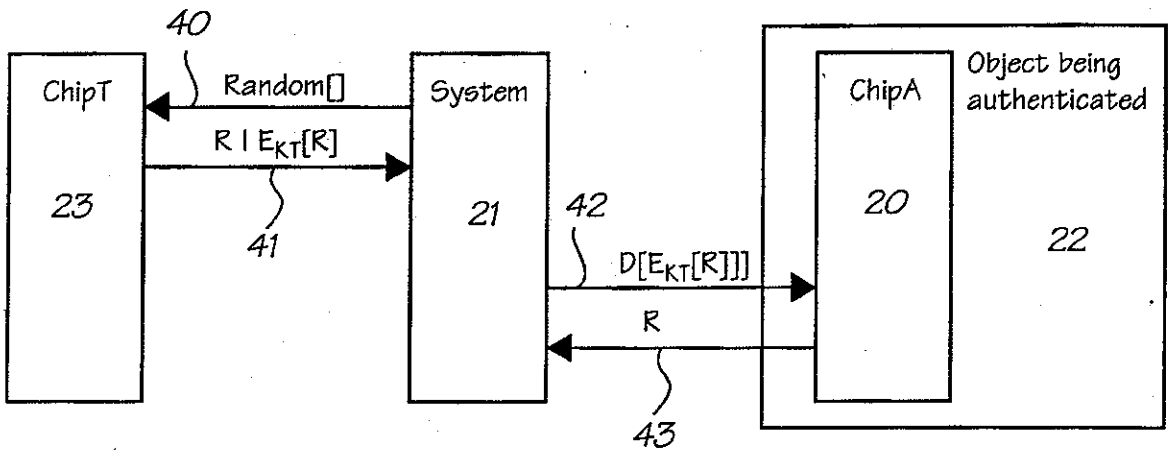

40
Random[]
ChipT
23
R | $E_{KT}[R]$
41
System
21
42
$D[E_{KT}[R]]]$
R
43
ChipA
20
Object being authenticated
22

FIG. 4

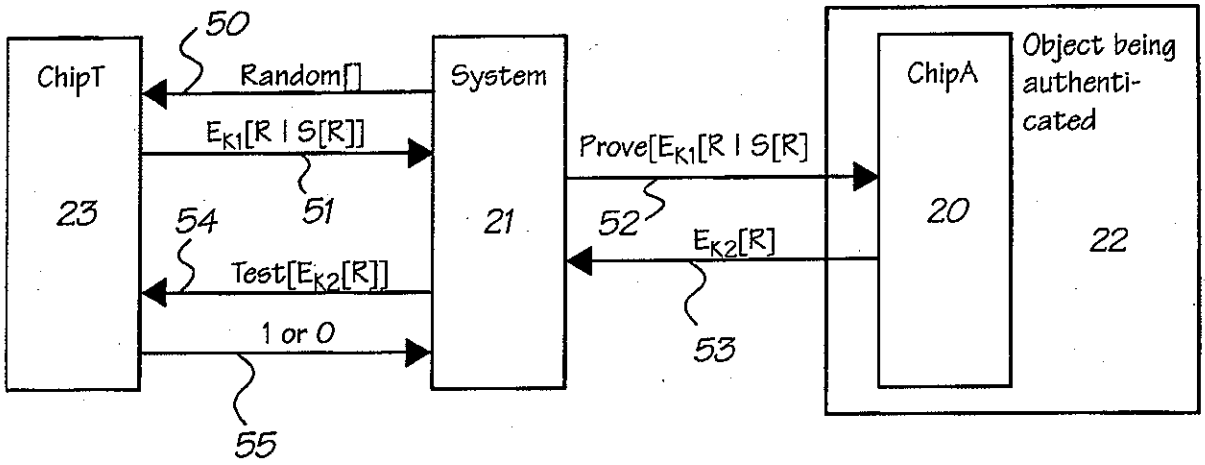

ChipT
23
50
Random[]
$E_{K1}[R \mid S[R]]$
51
54
Test[$E_{K2}[R]$]
1 or 0
55
System
21
Prove[$E_{K1}[R \mid S[R]$
52
$E_{K2}[R]$
53
ChipA
20
Object being authenti-cated
22

FIG. 5

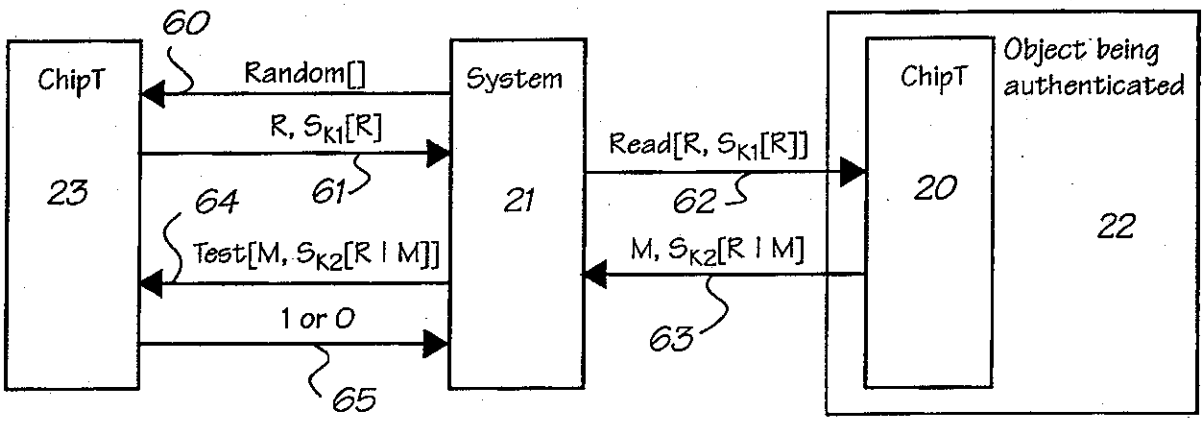

ChipT
23
60
Random[]
R, $S_{K1}[R]$
61
64
Test[M, $S_{K2}[R \mid M]$]
1 or 0
65
System
21
Read[R, $S_{K1}[R]$]
62
M, $S_{K2}[R \mid M]$
63
ChipT
20
Object being authenticated
22

FIG. 6

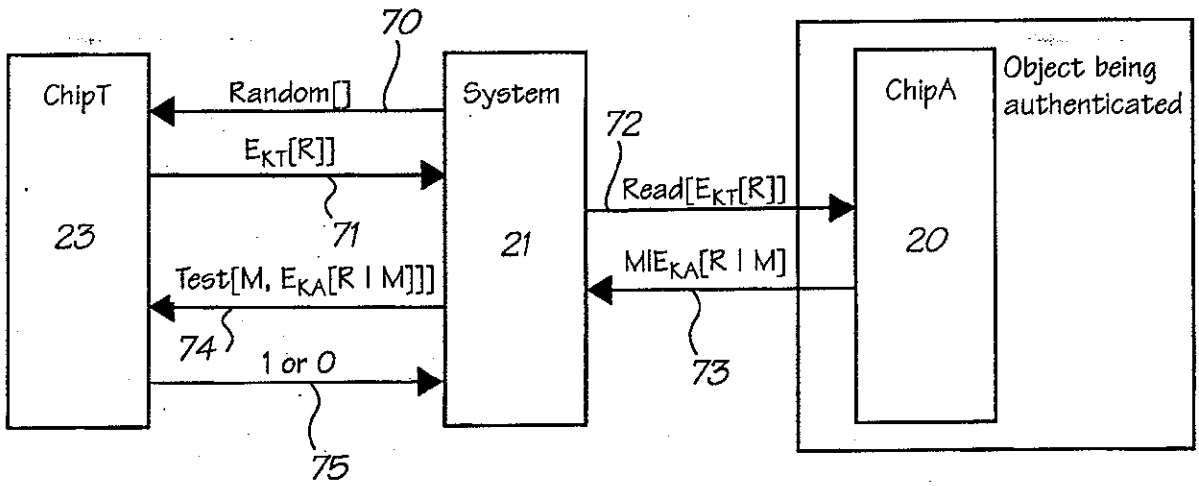

70
ChipT
Random[]
System
72
ChipA
Object being authenticated
$E_{KT}[R]]$
Read[$E_{KT}[R]$]
23
71
21
20
Test[M, $E_{KA}[R \mid M]$]]
MI$E_{KA}[R \mid M]$
74
1 or 0
73
75

FIG. 7

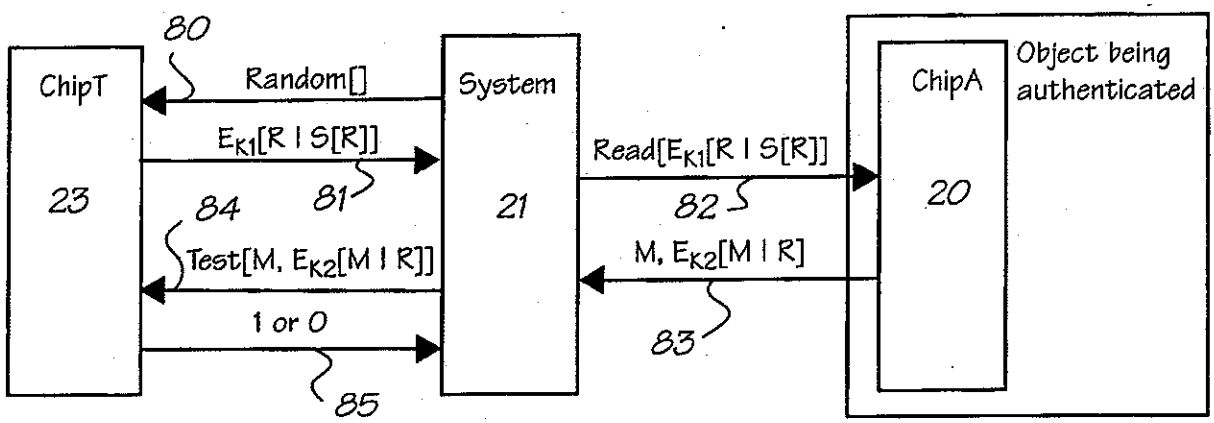

80
ChipT
Random[]
System
ChipA
Object being authenticated
$E_{K1}[R \mid S[R]]$
Read[$E_{K1}[R \mid S[R]]$
23
84
81
21
82
20
Test[M, $E_{K2}[M \mid R]$]
M, $E_{K2}[M \mid R]$
1 or 0
83
85

FIG. 8

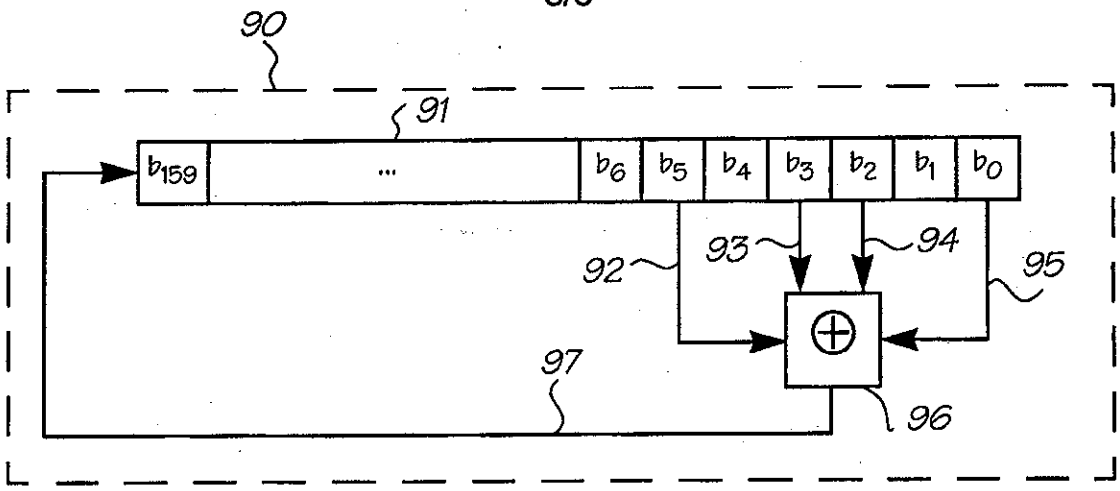


FIG. 9

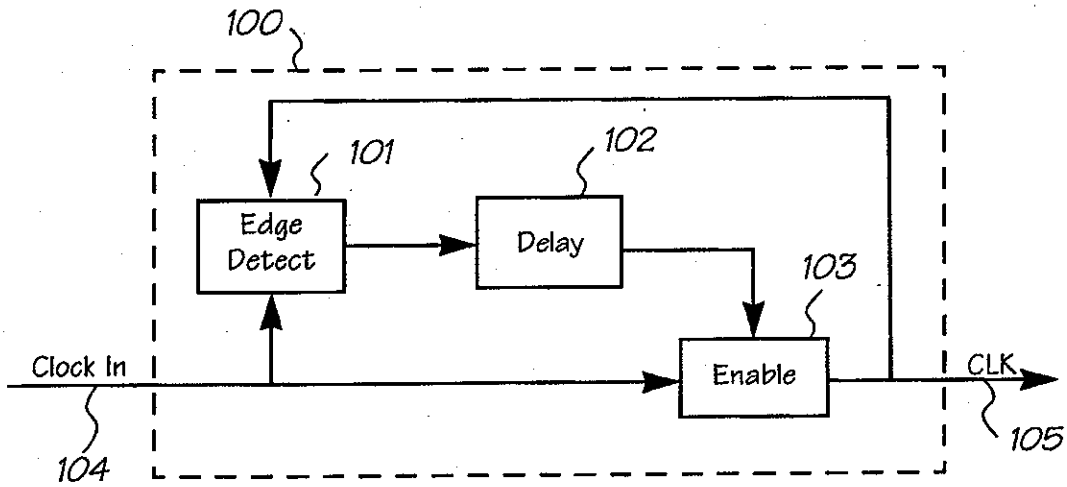


FIG. 10

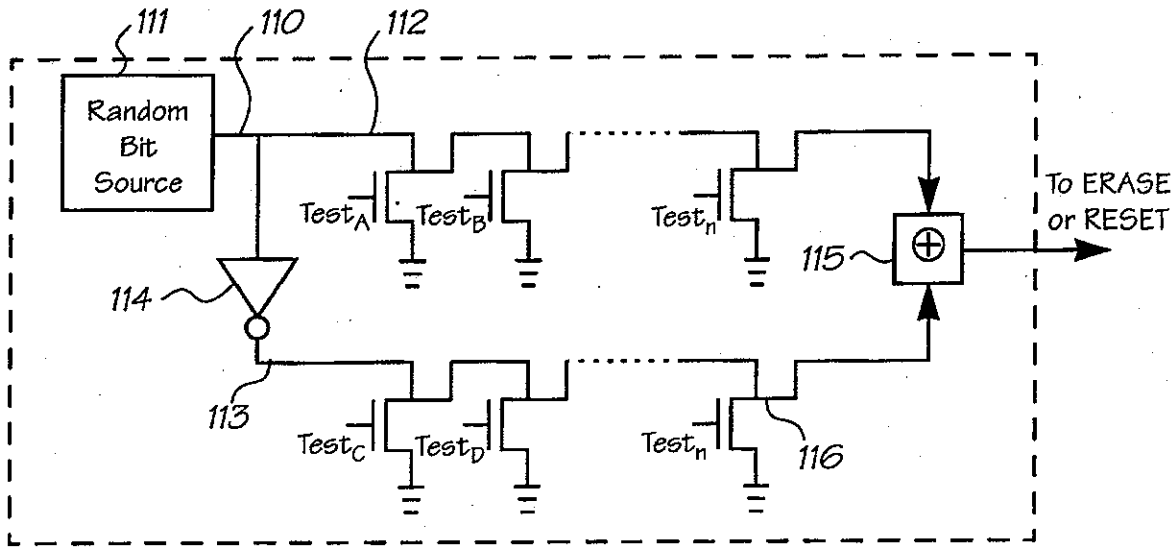


FIG. 11

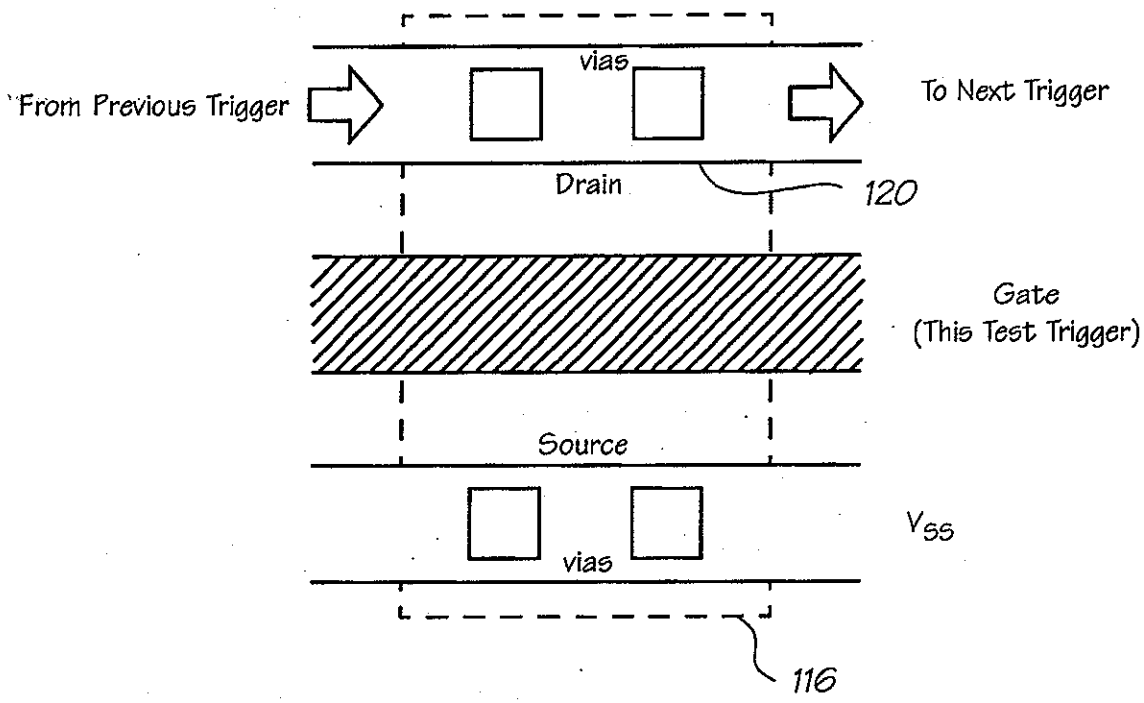

From Previous Trigger
vias
To Next Trigger
Drain
120
Gate
(This Test Trigger)
Source
V_{SS}
vias
116

FIG. 12

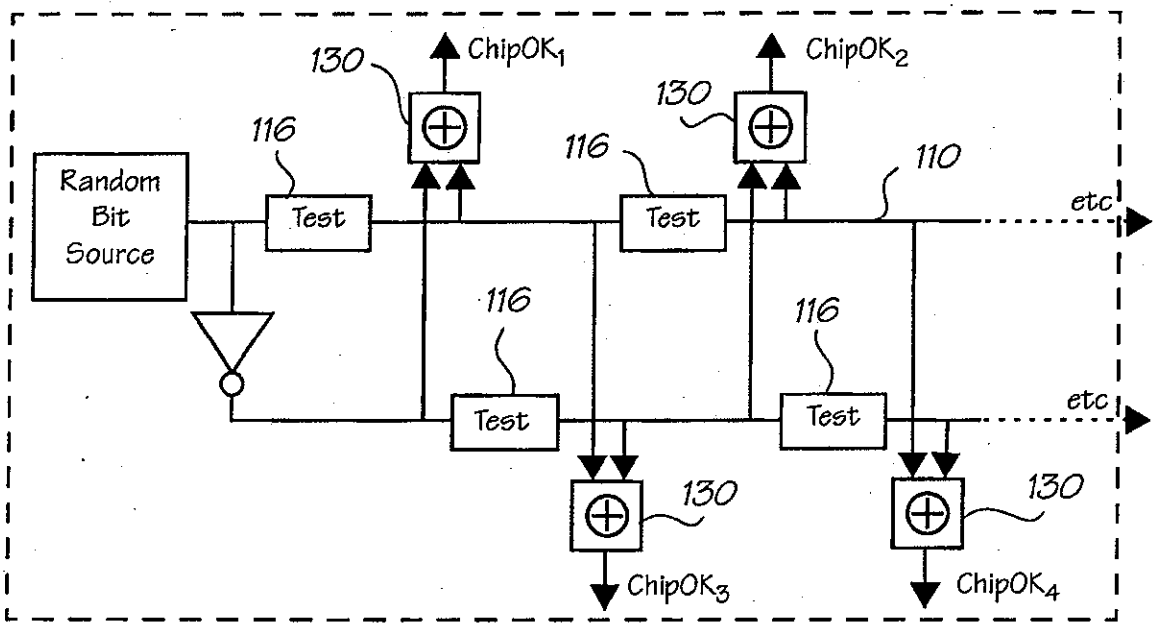

Random Bit Source
Test
Test
Test
Test
116
116
116
116
130
130
130
130
$ChipOK_1$
$ChipOK_2$
$ChipOK_3$
$ChipOK_4$
110
etc
etc

FIG. 13

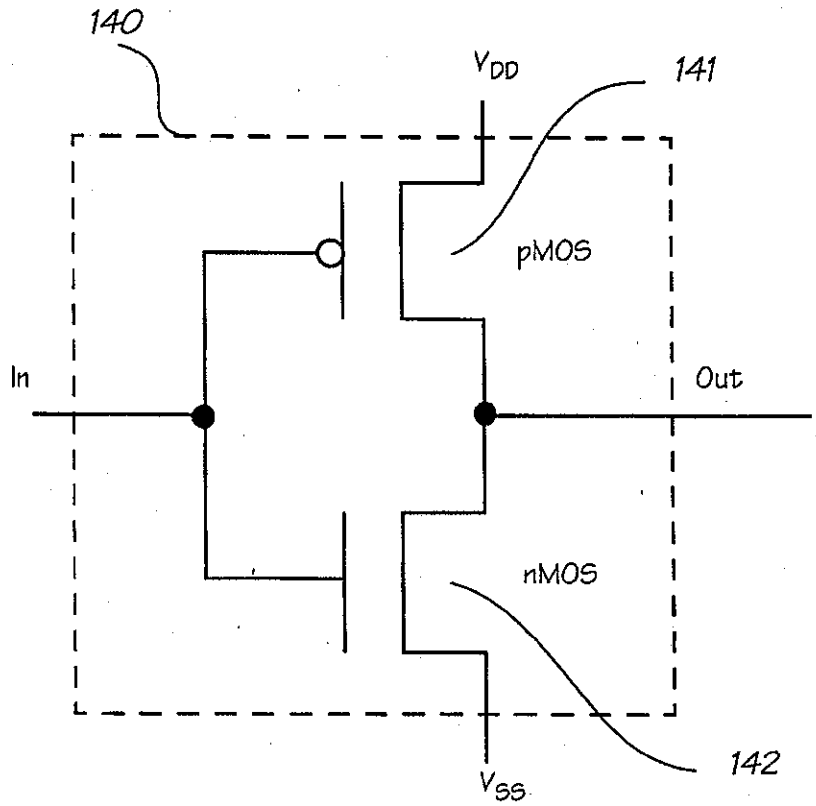

140
V_{DD}
141
pMOS
In
Out
nMOS
142
V_{SS}

FIG. 14

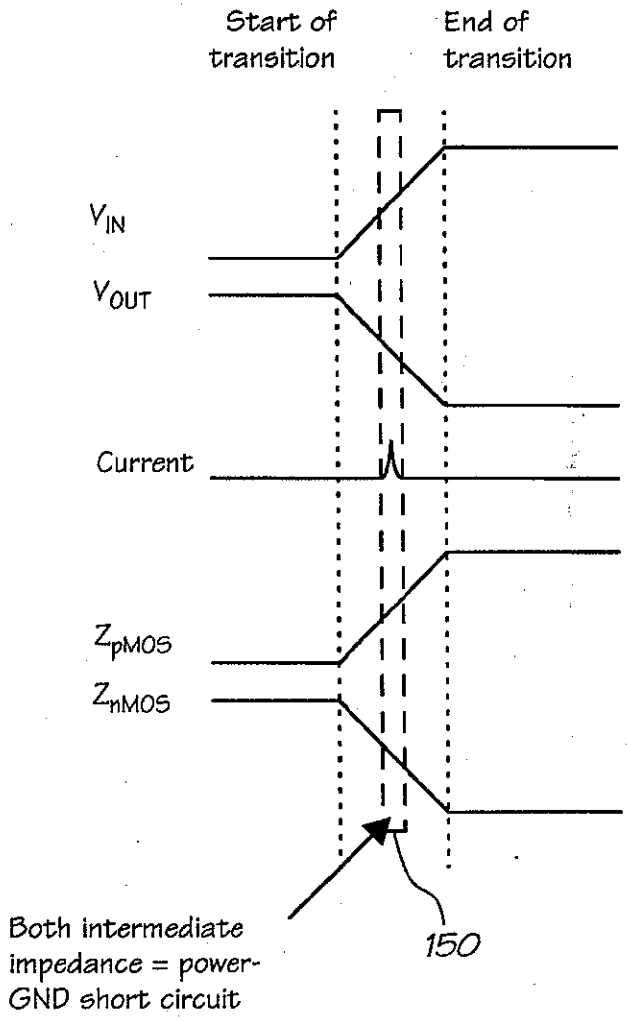

Start of transition
End of transition
V_{IN}
V_{OUT}
Current
Z_{pMOS}
Z_{nMOS}
Both intermediate impedance = power-GND short circuit
150

FIG. 15

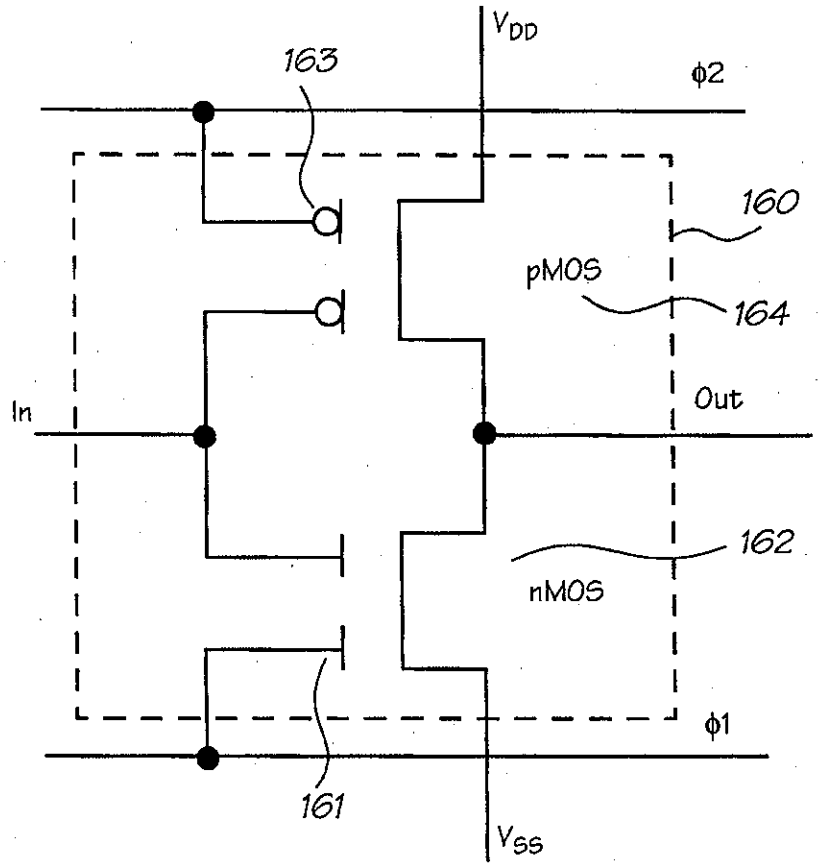
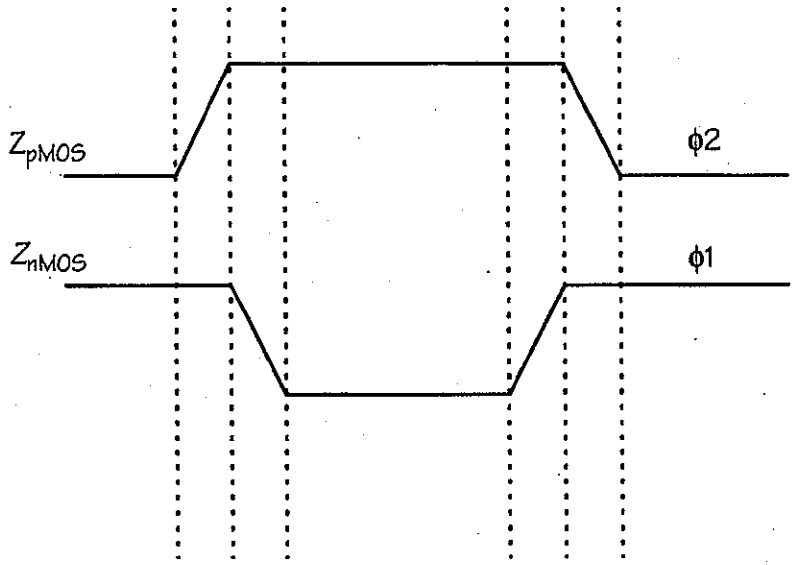


FIG. 16



Non-overlapping clocks

FIG. 17