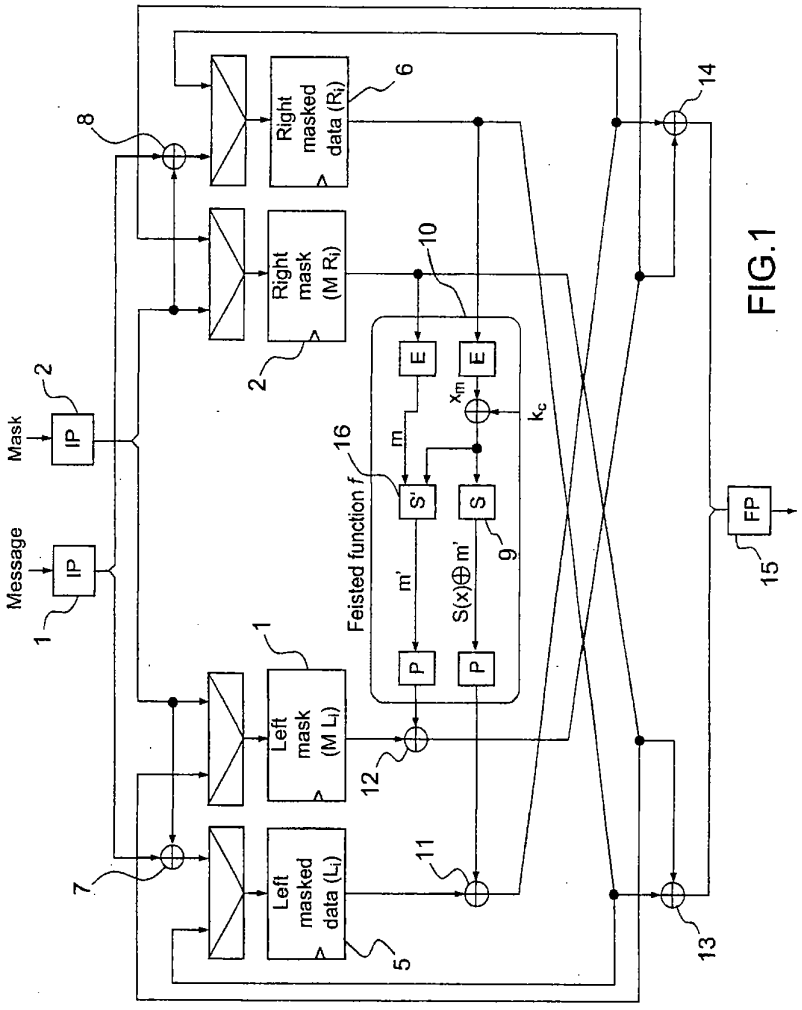
Mask
Message
IP
IP
1
2
Left masked data (L_i)
Left mask ($M L_i$)
Right mask ($M R_i$)
Right masked data (R_i)
5
1
2
6
7
8
10
11
12
13
14
15
FP
Feisted function f
16
E
E
S'
S
P
P
m
m'
x_m
k_c
S(x)⊕ m'
g

FIG.1

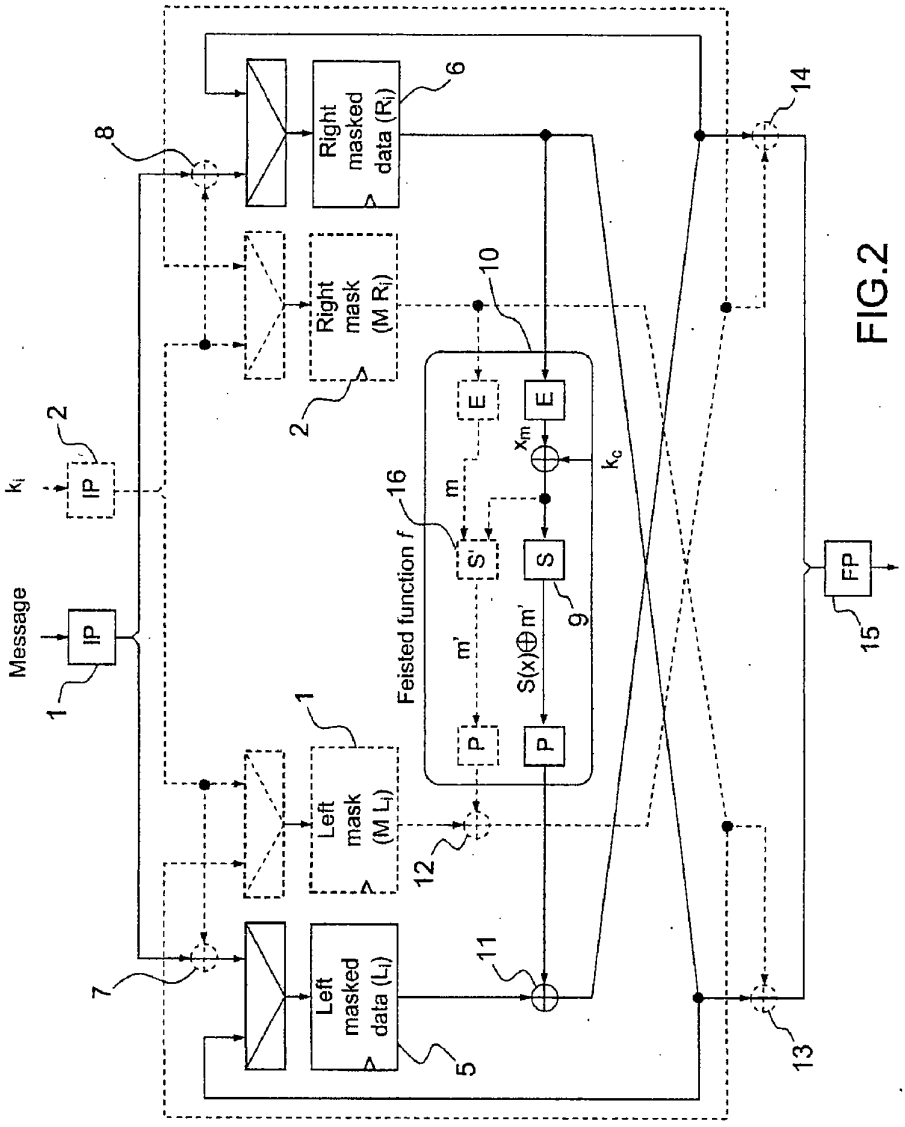
Message
IP
1
k_i
IP
2
Left masked data (L_i)
5
Right masked data (R_i)
6
7
8
Left mask (M L_i)
1
Right mask (M R_i)
2
Feisted function f
16
E
m
S'
m'
P
E
x_m
k_c
S
g
S(x)⊕m'
P
10
11
12
FP
15
13
14

FIG.2

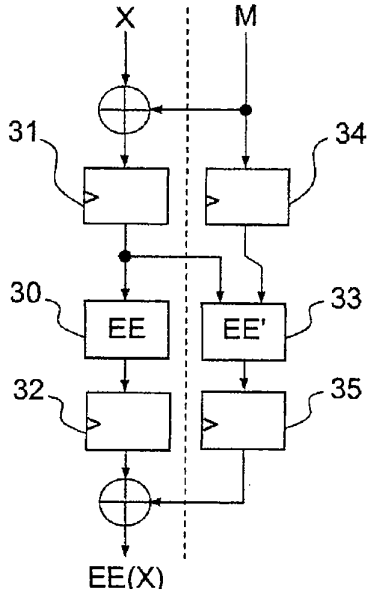

FIG.3

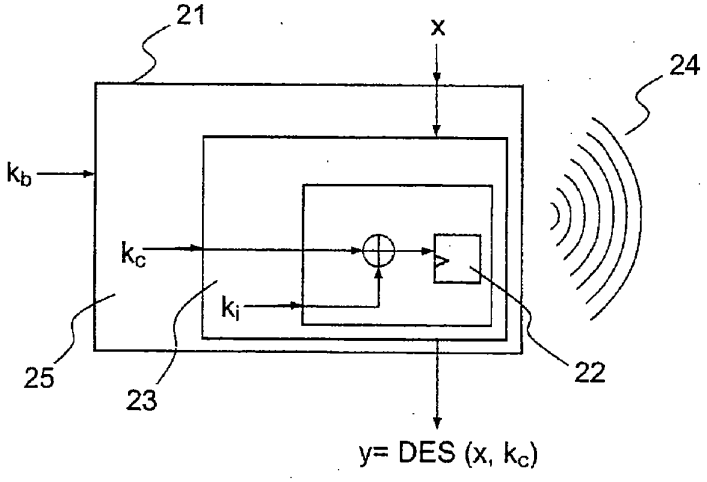

FIG.4