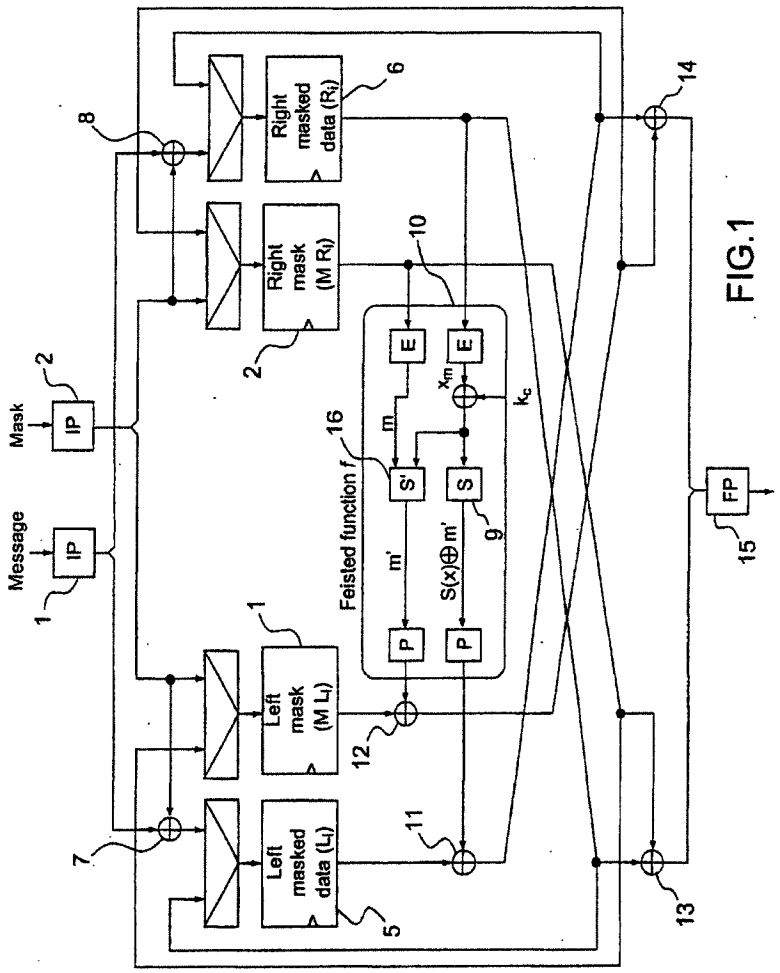
Message
Mask
IP
IP
1
2
Left masked data (L_i)
Left mask ($M L_i$)
Right mask ($M R_i$)
Right masked data (R_i)
5
1
2
6
7
8
Feisted function f
16
E
E
S'
S
P
P
m
m'
S(x)⊕ m'
x_m
k_c
g
10
11
12
13
14
FP
15

FIG.1

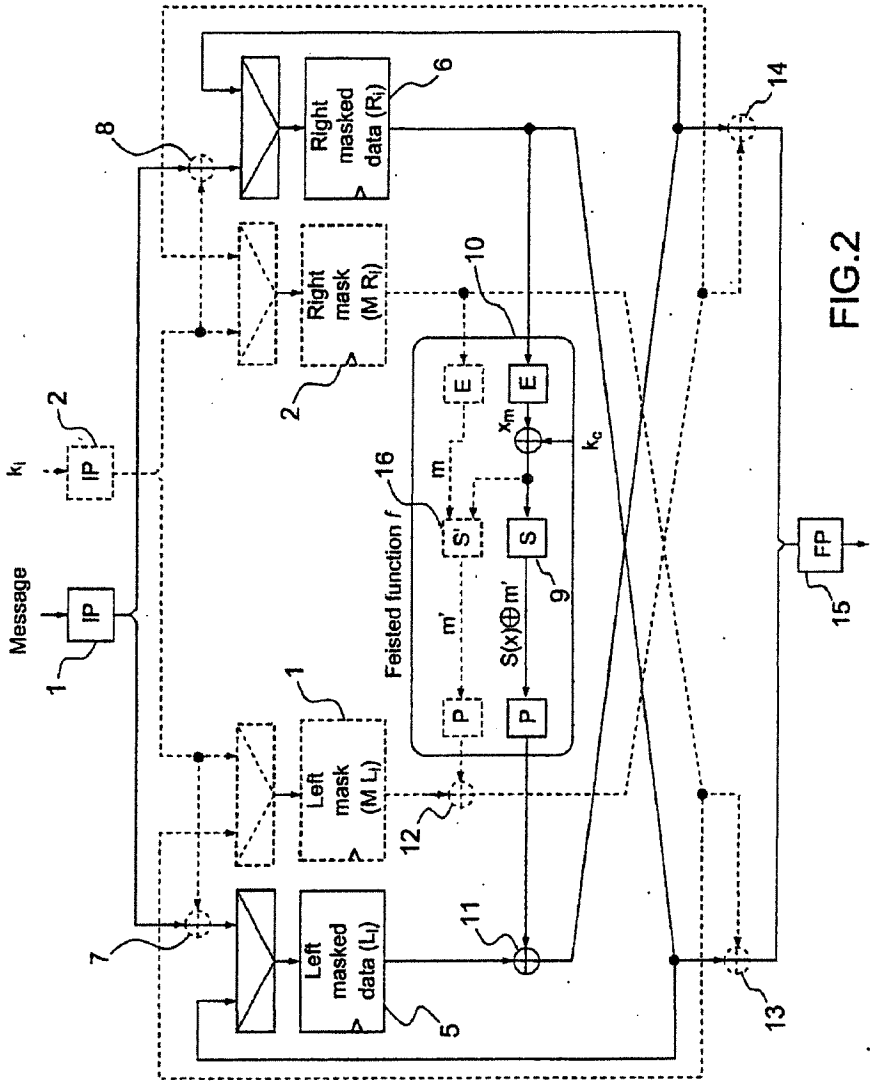
Message
IP
1
k_i
2
IP
Left mask (M L_i)
Left masked data (L_i)
5
7
Right mask (M R_i)
Right masked data (R_i)
6
8
Feisted function f
16
E
E
x_m
k_c
m
S'
S
g
m'
P
P
S(x)⊕m'
10
11
12
14
FP
15
13

FIG.2

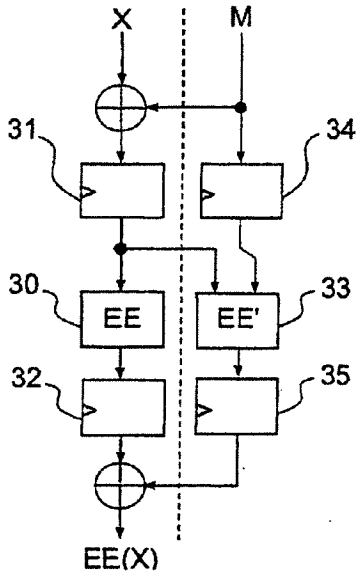

FIG.3

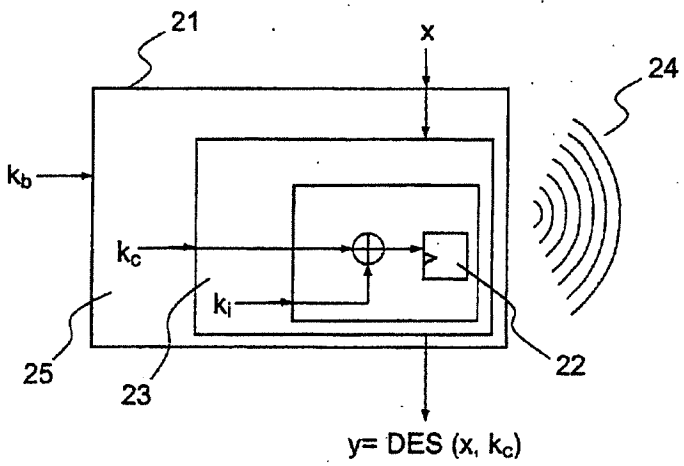

FIG.4