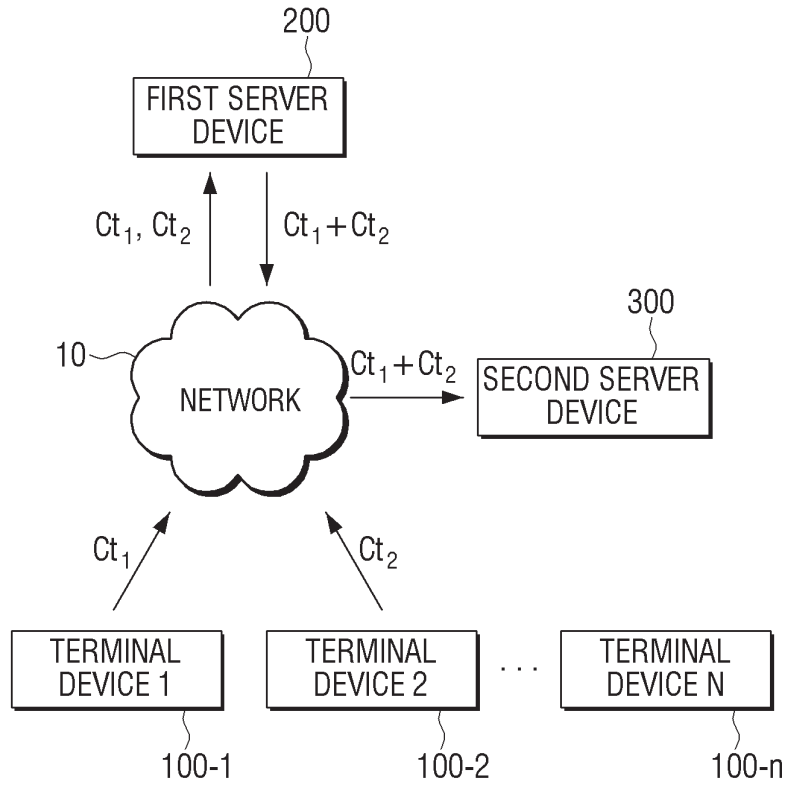
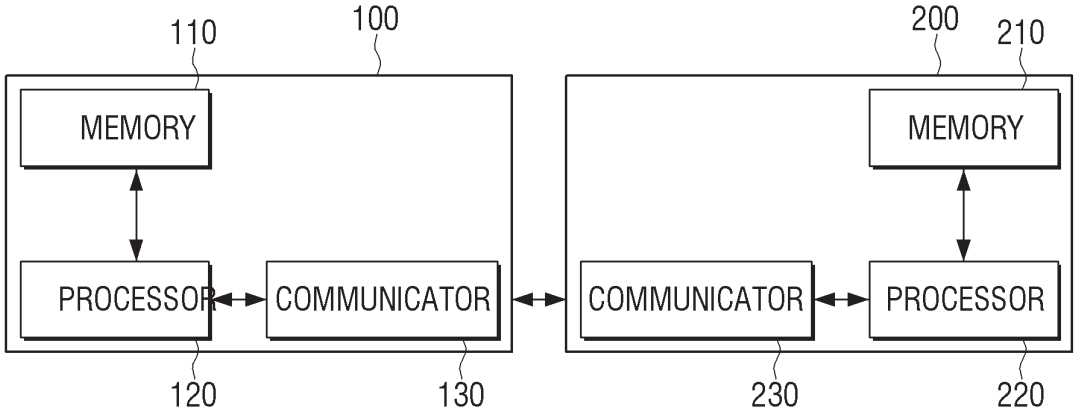
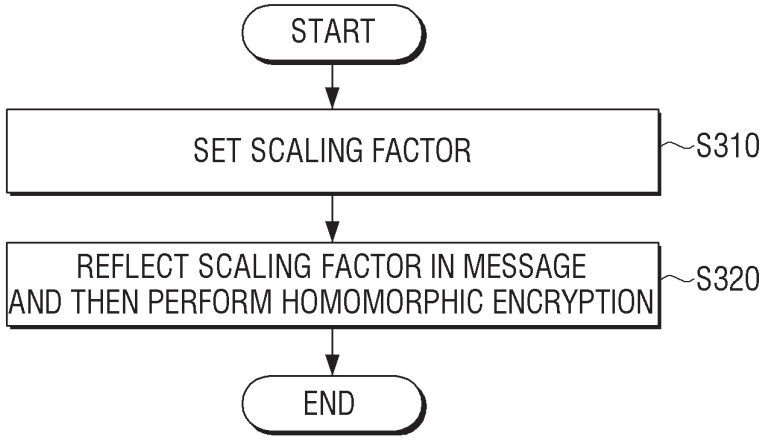
# FIG. 1


200
FIRST SERVER DEVICE
Ct1, Ct2
Ct1+Ct2
300
10
NETWORK
Ct1+Ct2
SECOND SERVER DEVICE
Ct1
Ct2
TERMINAL DEVICE 1
TERMINAL DEVICE 2
. . .
TERMINAL DEVICE N
100-1
100-2
100-n

# FIG. 2


110
100
200
210
MEMORY
MEMORY
PROCESSOR
COMMUNICATOR
COMMUNICATOR
PROCESSOR
120
130
230
220

# FIG. 3


START
SET SCALING FACTOR
S310
REFLECT SCALING FACTOR IN MESSAGE AND THEN PERFORM HOMOMORPHIC ENCRYPTION
S320
END

# FIG. 4

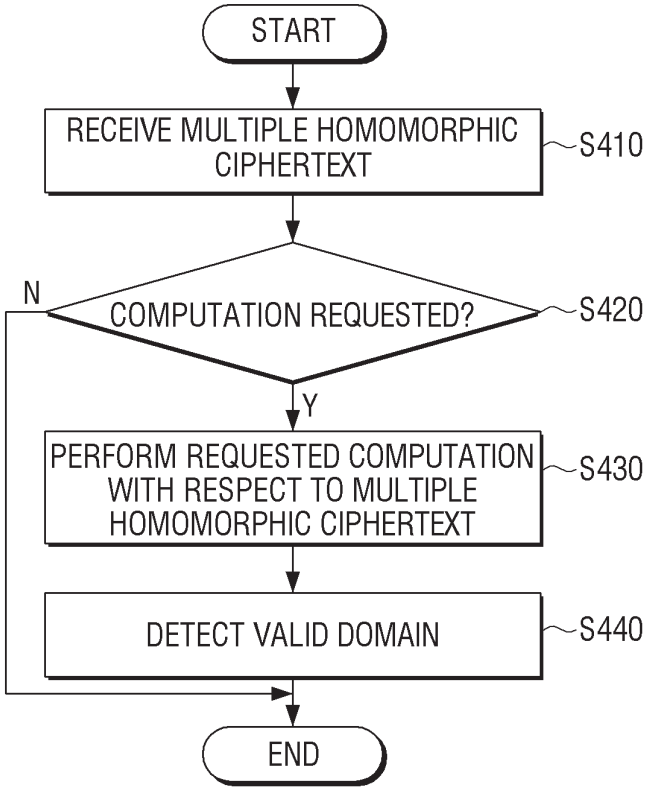
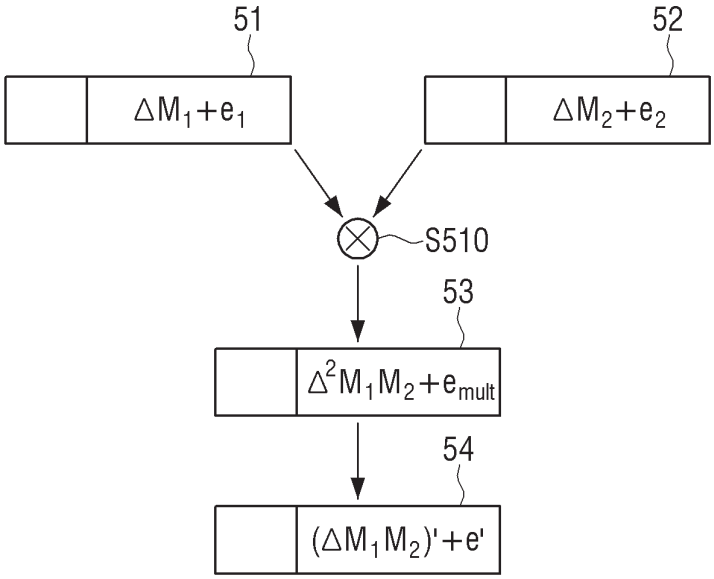
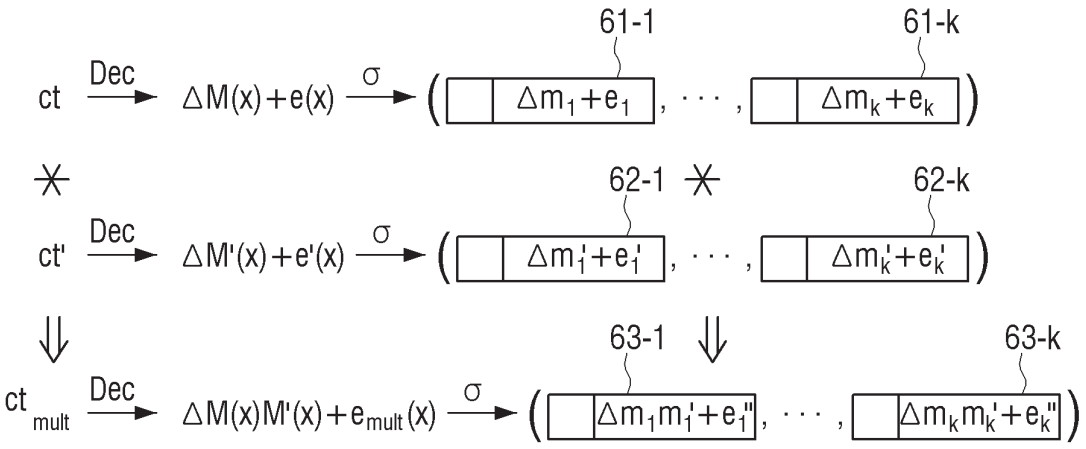

START
RECEIVE MULTIPLE HOMOMORPHIC CIPHERTEXT
S410
COMPUTATION REQUESTED?
S420
N
Y
PERFORM REQUESTED COMPUTATION WITH RESPECT TO MULTIPLE HOMOMORPHIC CIPHERTEXT
S430
DETECT VALID DOMAIN
S440
END

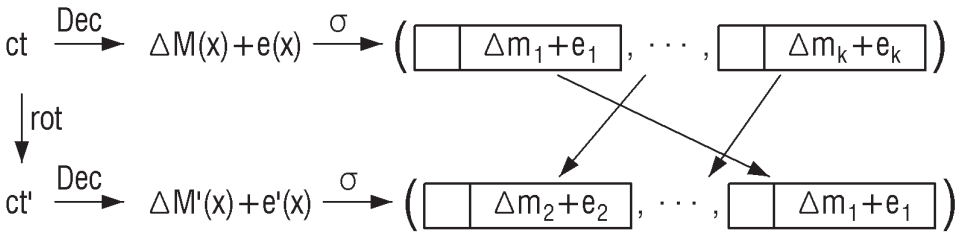
FIG. 5


51
52
$\Delta M_1+e_1$
$\Delta M_2+e_2$
S510
53
$\Delta^2 M_1 M_2+e_{mult}$
54
$(\Delta M_1 M_2)'+e'$

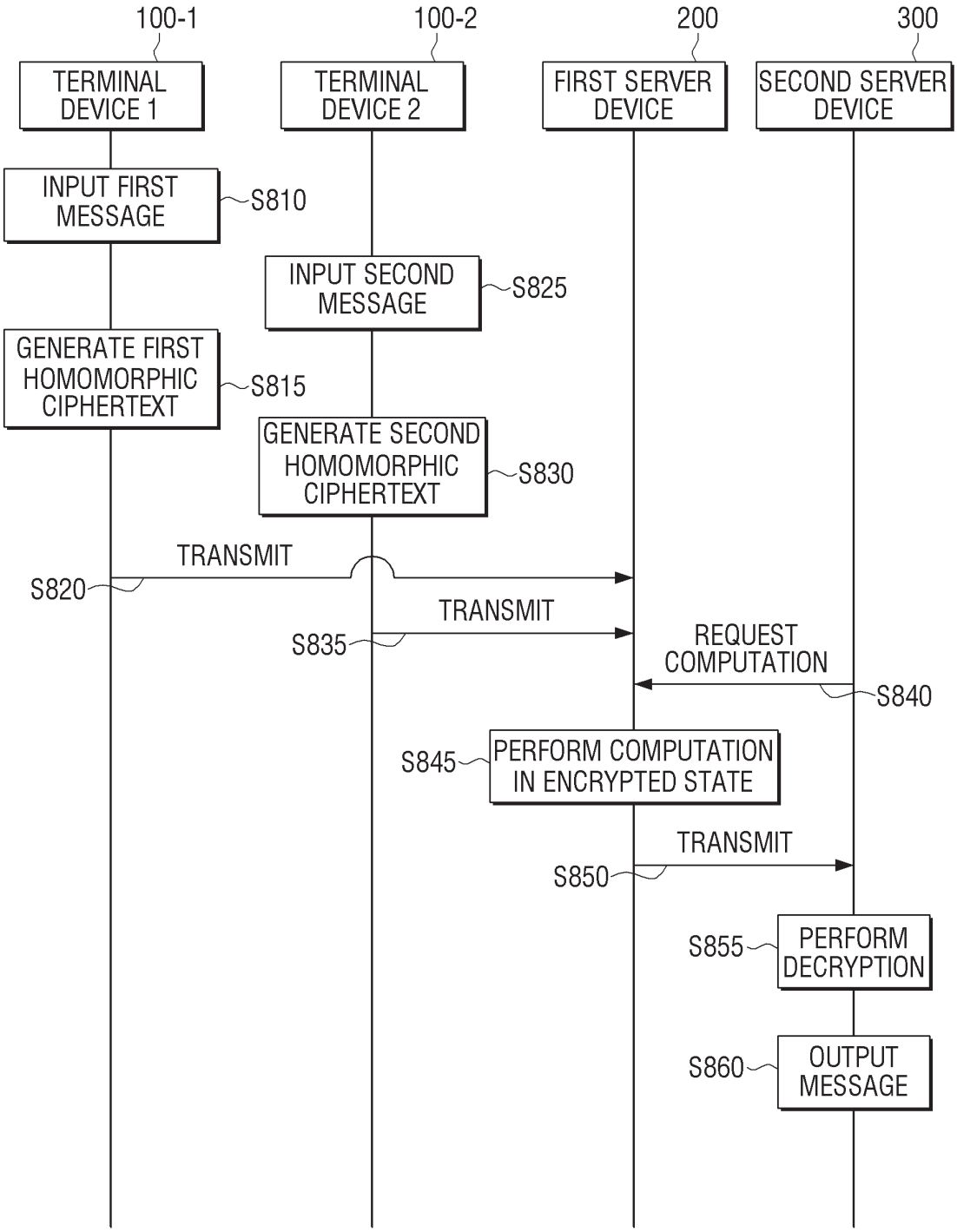
# FIG. 6


61-1
61-k
ct
Dec
ΔM(x)+e(x)
σ
Δm1+e1
Δmk+ek
62-1
62-k
ct'
ΔM'(x)+e'(x)
Δm1'+e1'
Δmk'+ek'
63-1
63-k
ctmult
ΔM(x)M'(x)+emult(x)
Δm1m1'+e1''
Δmkmk'+ek''

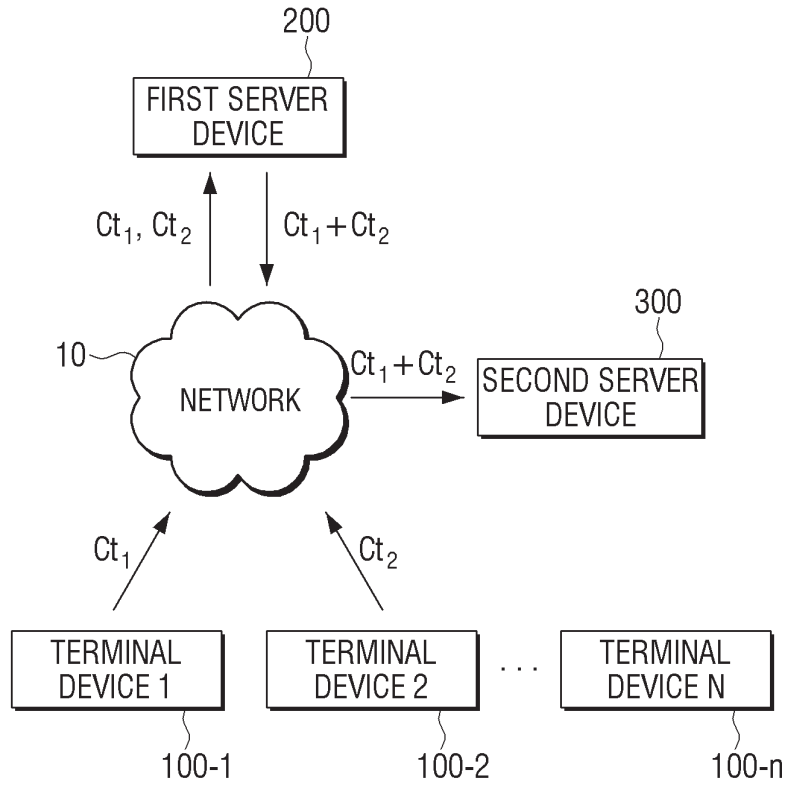
# FIG. 7



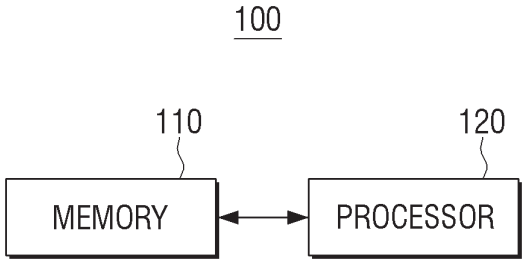
# FIG. 8


100-1
100-2
200
300
TERMINAL DEVICE 1
TERMINAL DEVICE 2
FIRST SERVER DEVICE
SECOND SERVER DEVICE
INPUT FIRST MESSAGE
S810
INPUT SECOND MESSAGE
S825
GENERATE FIRST HOMOMORPHIC CIPHERTEXT
S815
GENERATE SECOND HOMOMORPHIC CIPHERTEXT
S830
TRANSMIT
S820
TRANSMIT
S835
REQUEST COMPUTATION
S840
S845
PERFORM COMPUTATION IN ENCRYPTED STATE
TRANSMIT
S850
S855
PERFORM DECRYPTION
S860
OUTPUT MESSAGE

# FIG. 9


200
FIRST SERVER DEVICE
Ct1, Ct2
Ct1+Ct2
300
10
NETWORK
Ct1+Ct2
SECOND SERVER DEVICE
Ct1
Ct2
TERMINAL DEVICE 1
TERMINAL DEVICE 2
. . .
TERMINAL DEVICE N
100-1
100-2
100-n

# FIG. 10



# FIG. 11

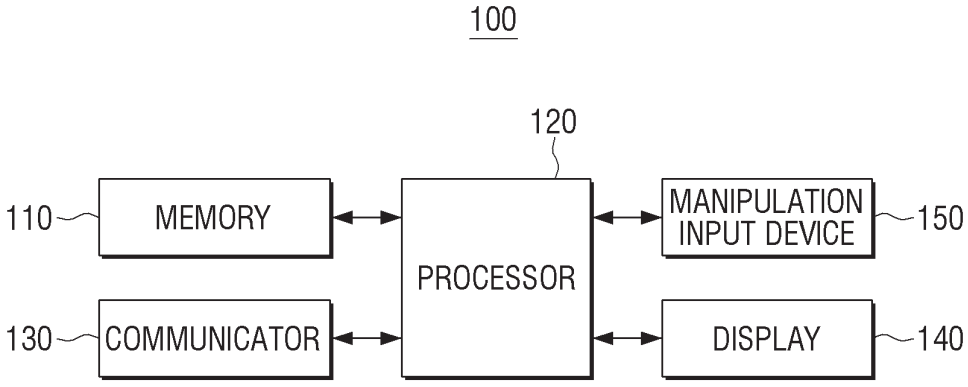

100
120
110
MEMORY
PROCESSOR
MANIPULATION INPUT DEVICE
150
130
COMMUNICATOR
DISPLAY
140

FIG. 12

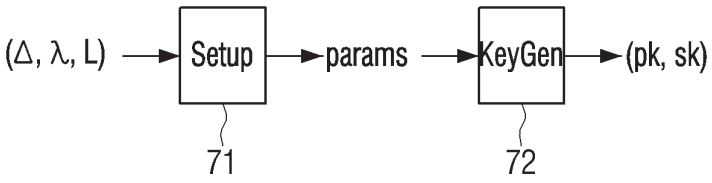
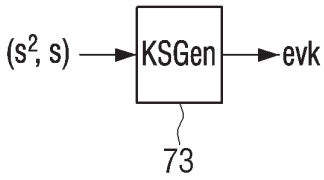
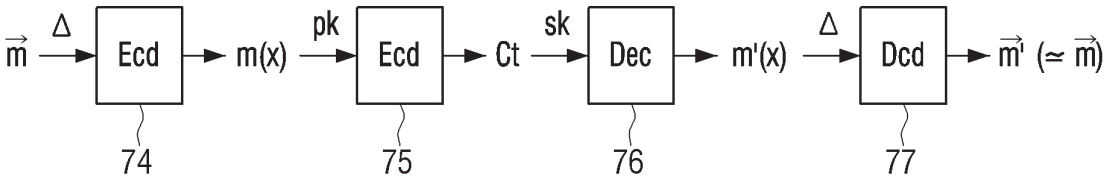


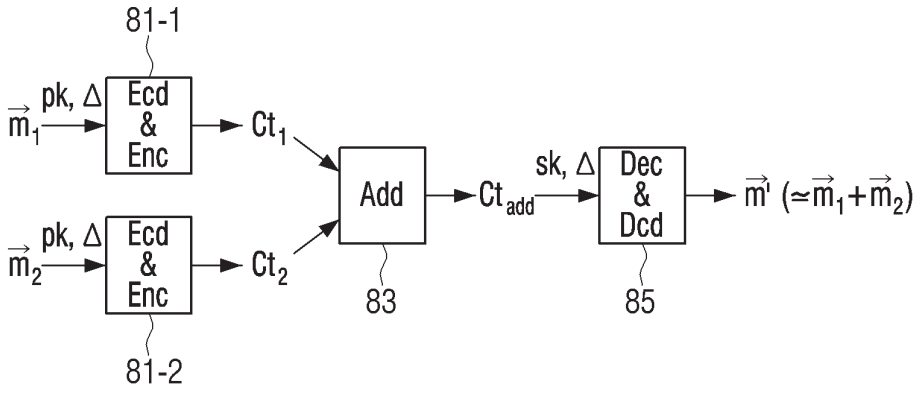
FIG. 13



# FIG. 14



# FIG. 15


81-1
pk, Δ
Ecd & Enc
Ct1
m1
pk, Δ
Ecd & Enc
Ct2
m2
81-2
Add
83
Ctadd
sk, Δ
Dec & Dcd
85
m' (≃m1+m2)

# FIG. 16

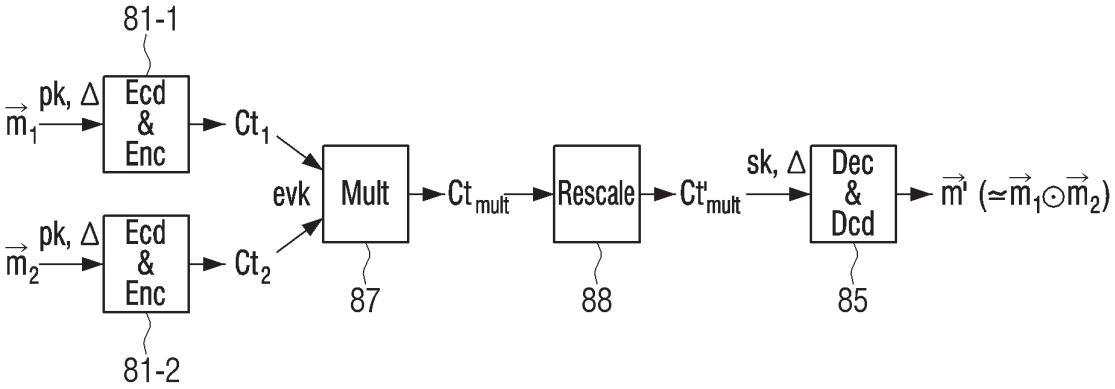
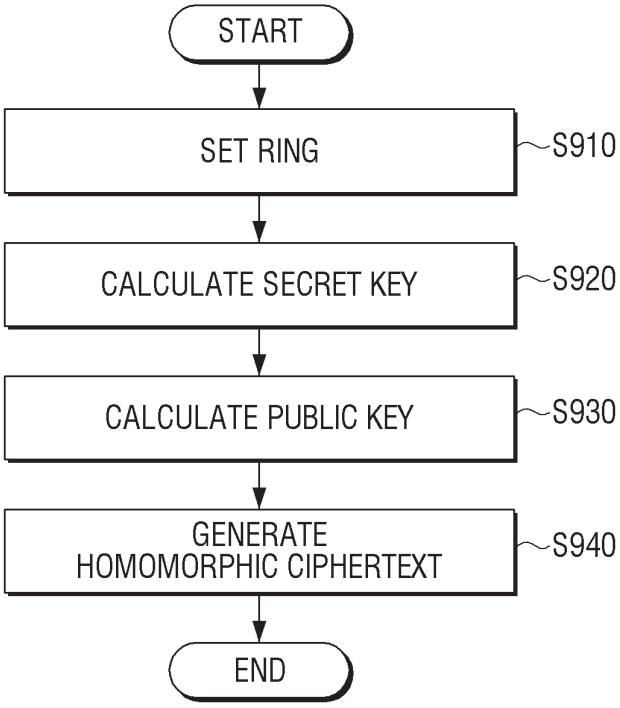
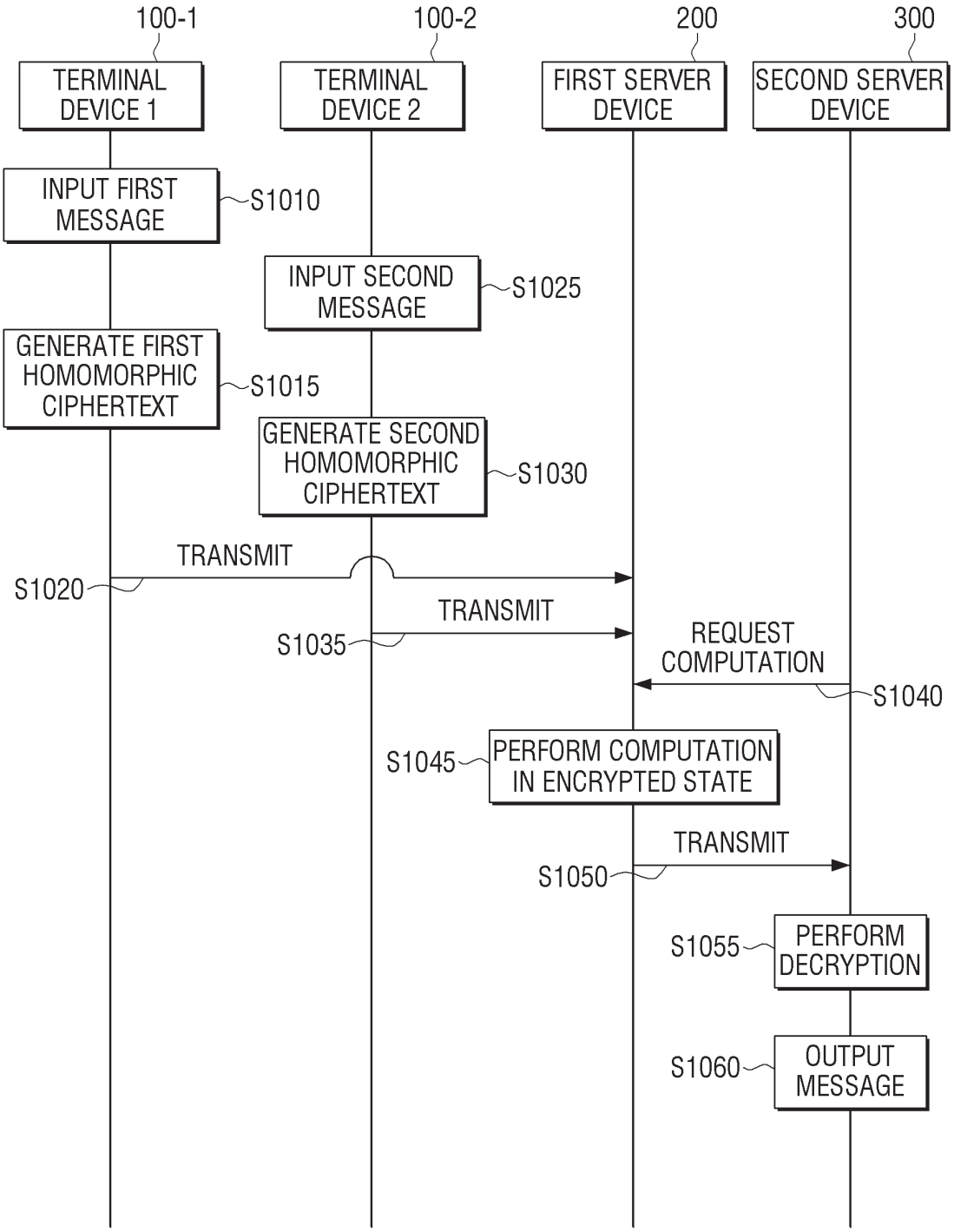

81-1
$\vec{m}_1$
pk, Δ
Ecd & Enc
$Ct_1$
$\vec{m}_2$
pk, Δ
Ecd & Enc
$Ct_2$
81-2
evk
Mult
87
$Ct_{mult}$
Rescale
88
$Ct'_{mult}$
sk, Δ
Dec & Dcd
85
$\vec{m}'$ $(\simeq \vec{m}_1 \odot \vec{m}_2)$

FIG. 17


START
SET RING
S910
CALCULATE SECRET KEY
S920
CALCULATE PUBLIC KEY
S930
GENERATE HOMOMORPHIC CIPHERTEXT
S940
END

# FIG. 18


100-1
100-2
200
300
TERMINAL DEVICE 1
TERMINAL DEVICE 2
FIRST SERVER DEVICE
SECOND SERVER DEVICE
INPUT FIRST MESSAGE
S1010
INPUT SECOND MESSAGE
S1025
GENERATE FIRST HOMOMORPHIC CIPHERTEXT
S1015
GENERATE SECOND HOMOMORPHIC CIPHERTEXT
S1030
TRANSMIT
S1020
TRANSMIT
S1035
REQUEST COMPUTATION
S1040
S1045
PERFORM COMPUTATION IN ENCRYPTED STATE
TRANSMIT
S1050
S1055
PERFORM DECRYPTION
S1060
OUTPUT MESSAGE