

FIG. 1

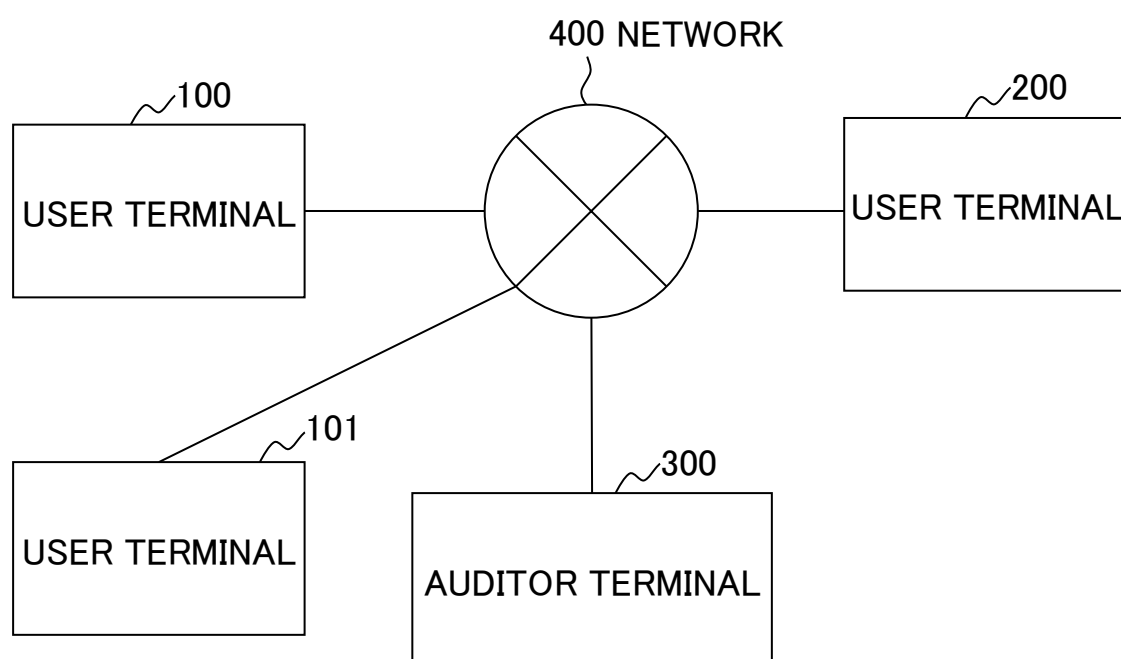
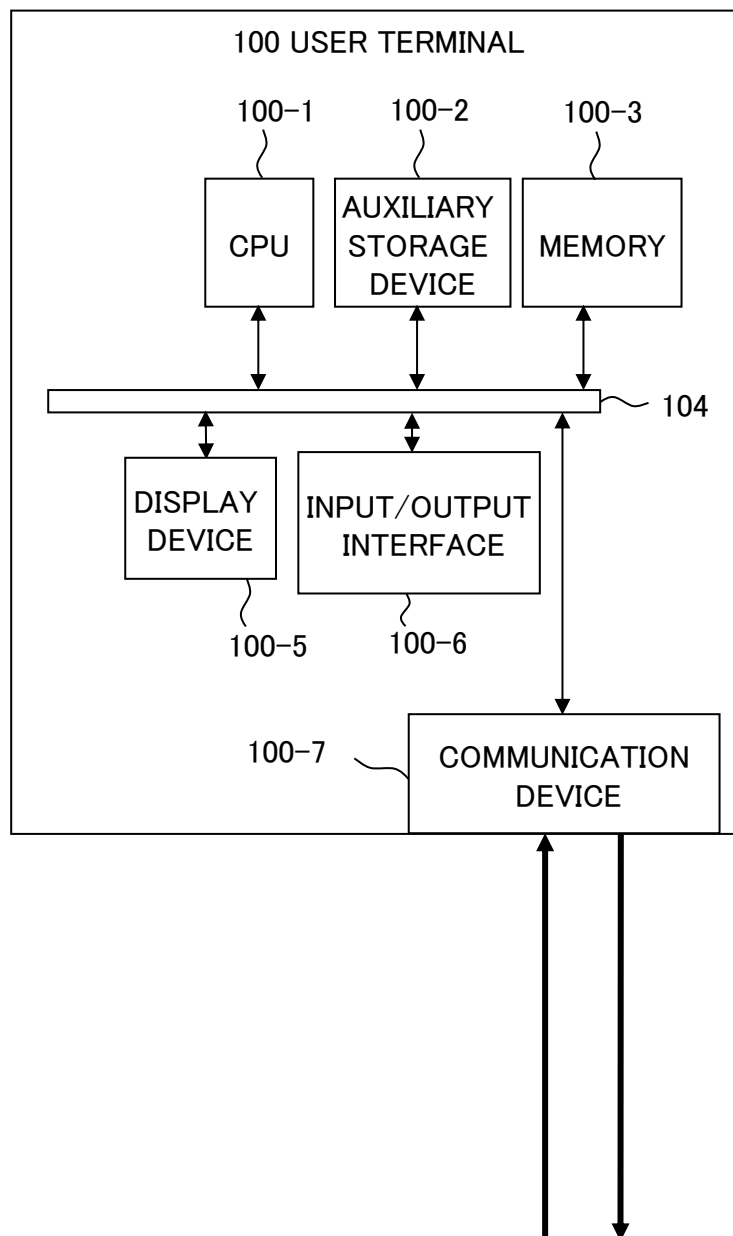
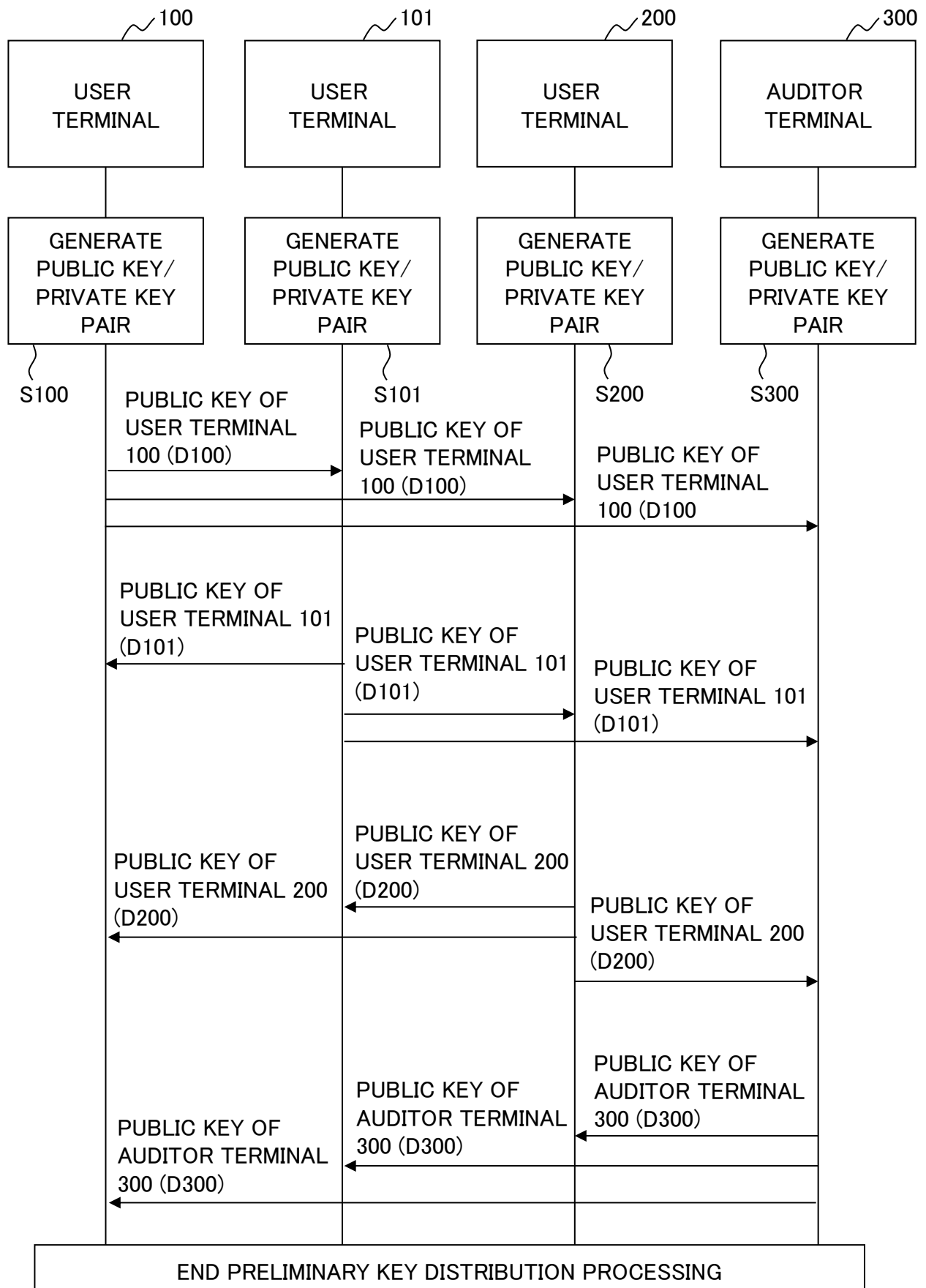


FIG. 2



3/10
FIG. 3



4/10
FIG. 4

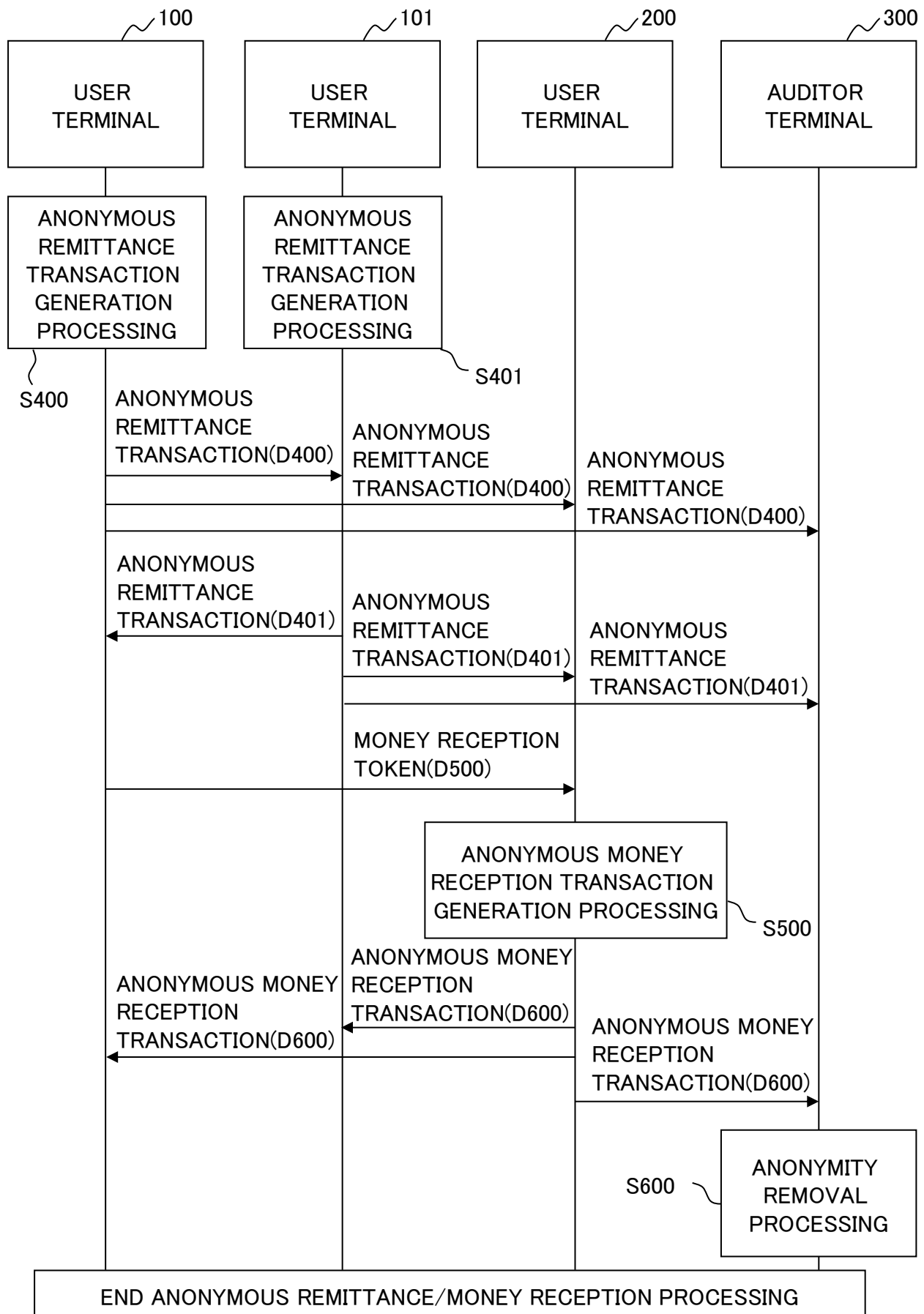


FIG. 5

↙ D400 ANONYMOUS REMITTANCE TRANSACTION DATA FORMAT

TRANSACTION ID	1234	411
REMITTANCE DESTINATION	—	412
REMITTANCE SOURCE	USER TERMINAL 100	413
AMOUNT	ONE COIN	414
EXTENDED REGION	COMMIT VALUE: C0	415-1
	ELGAMAL ENCRYPTED TEXT: $(f^{x0}, e^{x0}g^{y0})$	415-2
	ZERO-KNOWLEDGE PROOF VALUE: (r, a, b, c, S, T, U)	415-3
		415

FIG. 6

↙ D500 MONEY RECEPTION TOKEN DATA FORMAT

TRANSACTION ID	1234	511
FIRST COMMIT PRE-IMAGE	y0	512
SECOND COMMIT PRE-IMAGE	z0	513

6/10
FIG. 7

ANONYMOUS REMITTANCE TRANSACTION GENERATION PROCESSING (S400)

[GENERATE TRANSACTION ID]
GENERATE 1234 AS TRANSACTION ID
OUTPUT TRANSACTION ID: [1234] S401

[SET REMITTANCE SOURCE]
SET OWN ADDRESS OR ID AS REMITTANCE SOURCE
OUTPUT REMITTANCE SOURCE: [USER TERMINAL 100] S402

[SET AMOUNT]
SET ONE COIN TO BE REMITTED AS AMOUNT
OUTPUT AMOUNT: [ONE COIN] S403

[SET EXTENDED REGION]
GENERATE RANDOM INTEGERS x_0 , y_0 , and z_0
CALCULATE COMMIT VALUE: $CO = g^{y_0} h^{z_0}$ FOR PUBLIC
SYSTEM PARAMETERS g AND h , AND OUTPUT COMMIT VALUE: $[CO]$
USE PUBLIC KEY $e = f^k$ OF AUDITOR TERMINAL 300 AND
INTEGER x_0 TO CALCULATE ELGAMAL ENCRYPTED TEXT $M = (f^{x_0}, e^{x_0} g^{y_0})$
FOR PLAIN TEXT g^{y_0} , AND OUTPUT ENCRYPTED TEXT $[(f^{x_0}, e^{x_0} g^{y_0})]$ S404
GENERATE RANDOM INTEGERS α , β , AND γ
CALCULATE $S = f^\alpha$, $T = e^\alpha g^\beta$, AND $U = g^\beta h^\gamma$ FOR PUBLIC
SYSTEM PARAMETERS f , g , AND h , FURTHER CALCULATE $r = H(S, T, U)$
FOR HASH FUNCTION H , CALCULATE $a = rx_0 + \alpha$, $b = ry_0 + \beta$, AND $c = rz_0 + \gamma$,
AND OUTPUT ZERO-KNOWLEDGE PROOF VALUE: $[r, a, b, c, S, T, U]$

OUTPUT, AS ANONYMOUS REMITTANCE TRANSACTION (D400),
TRANSACTION ID=[1234],
REMITTANCE SOURCE: [USER TERMINAL 100],
AMOUNT: [ONE COIN],
EXTENDED REGION=COMMIT VALUE: $[CO]$,
ELGAMAL ENCRYPTED TEXT: $[(f^{x_0}, e^{x_0} g^{y_0})]$,
AND ZERO-KNOWLEDGE PROOF VALUE: $[(r, a, b, c, S, T, U)]$,
AND END PROCESSING S405

FIG. 8

↙ D600 ANONYMOUS MONEY RECEPTION TRANSACTION DATA FORMAT

TRANSACTION ID	5678	601
REMITTANCE DESTINATION	USER TERMINAL 200	602
REMITTANCE SOURCE		603
AMOUNT	ONE COIN	604
EXTENDED REGION	FIRST COMMIT PRE-IMAGE: y_0 ----- ZERO-KNOWLEDGE PROOF VALUE: π (ZERO-KNOWLEDGE PROOF VALUE INDICATING THAT DISCRETE LOGARITHM VALUE HAVING h OF $C0g^{-y_0}$ OR $C1g^{-y_0}$ AS ITS BASE IS KNOWN	605-1 605-2 605

8/10
FIG. 9

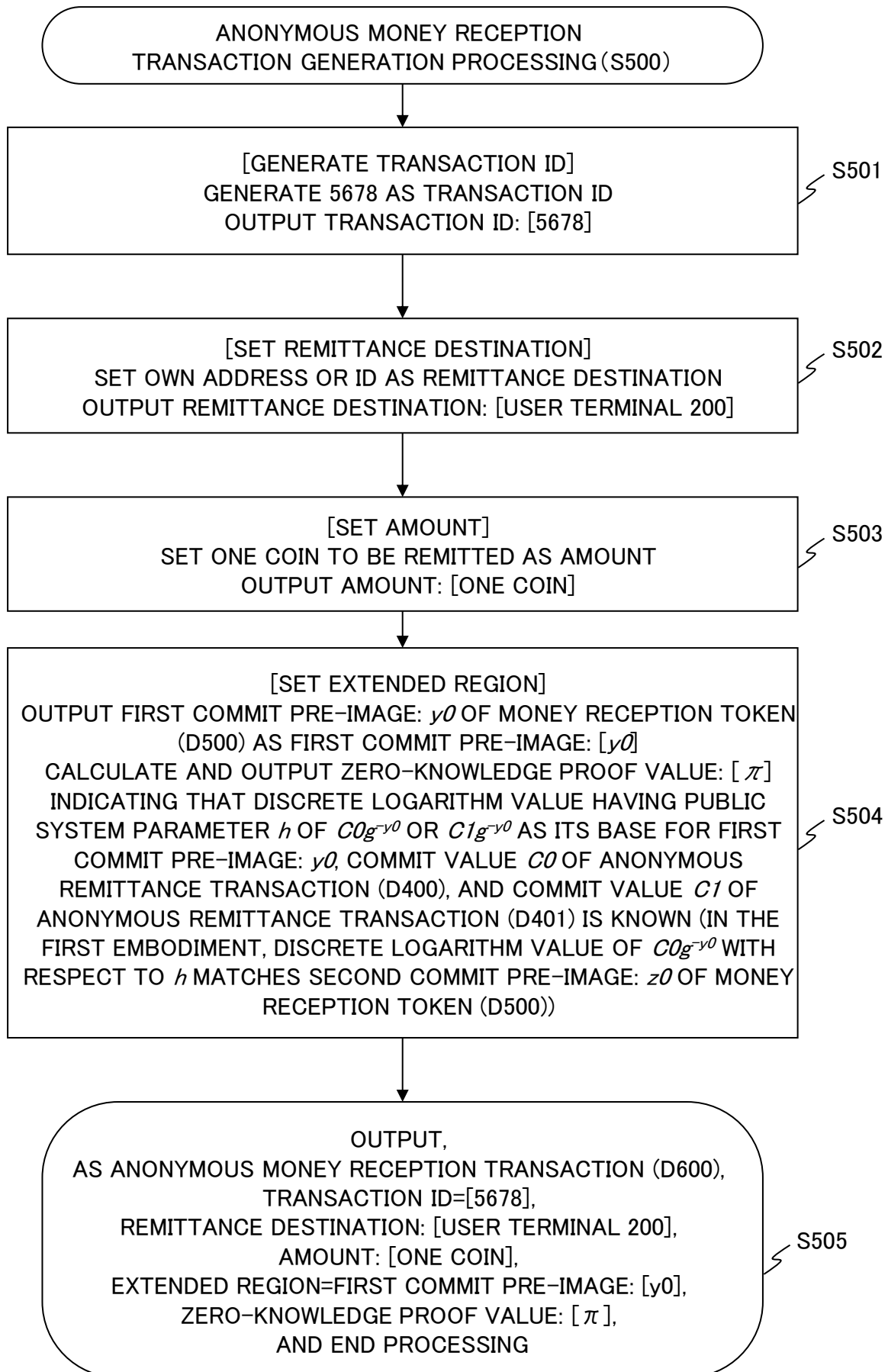


FIG. 10

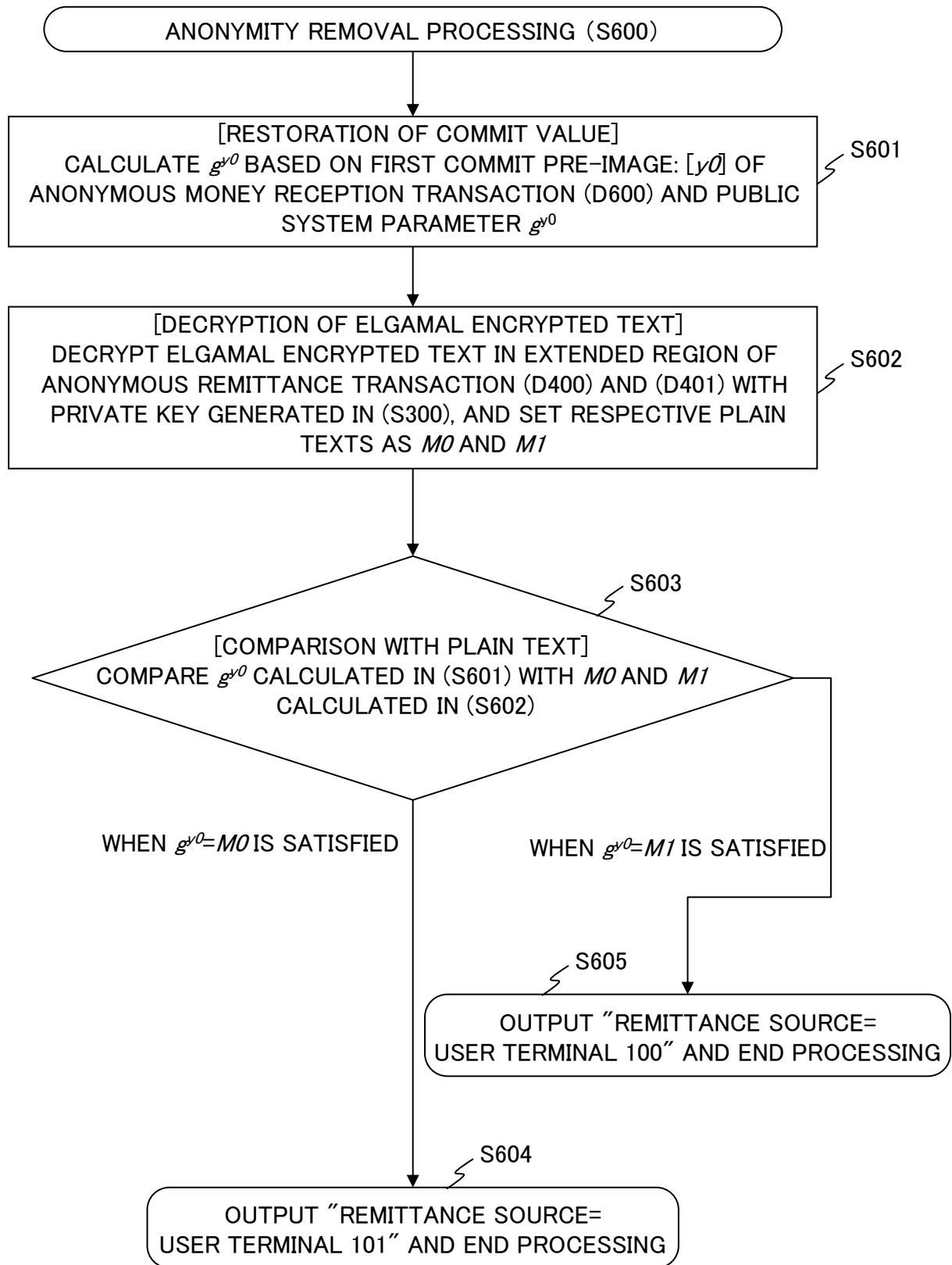


FIG. 11

