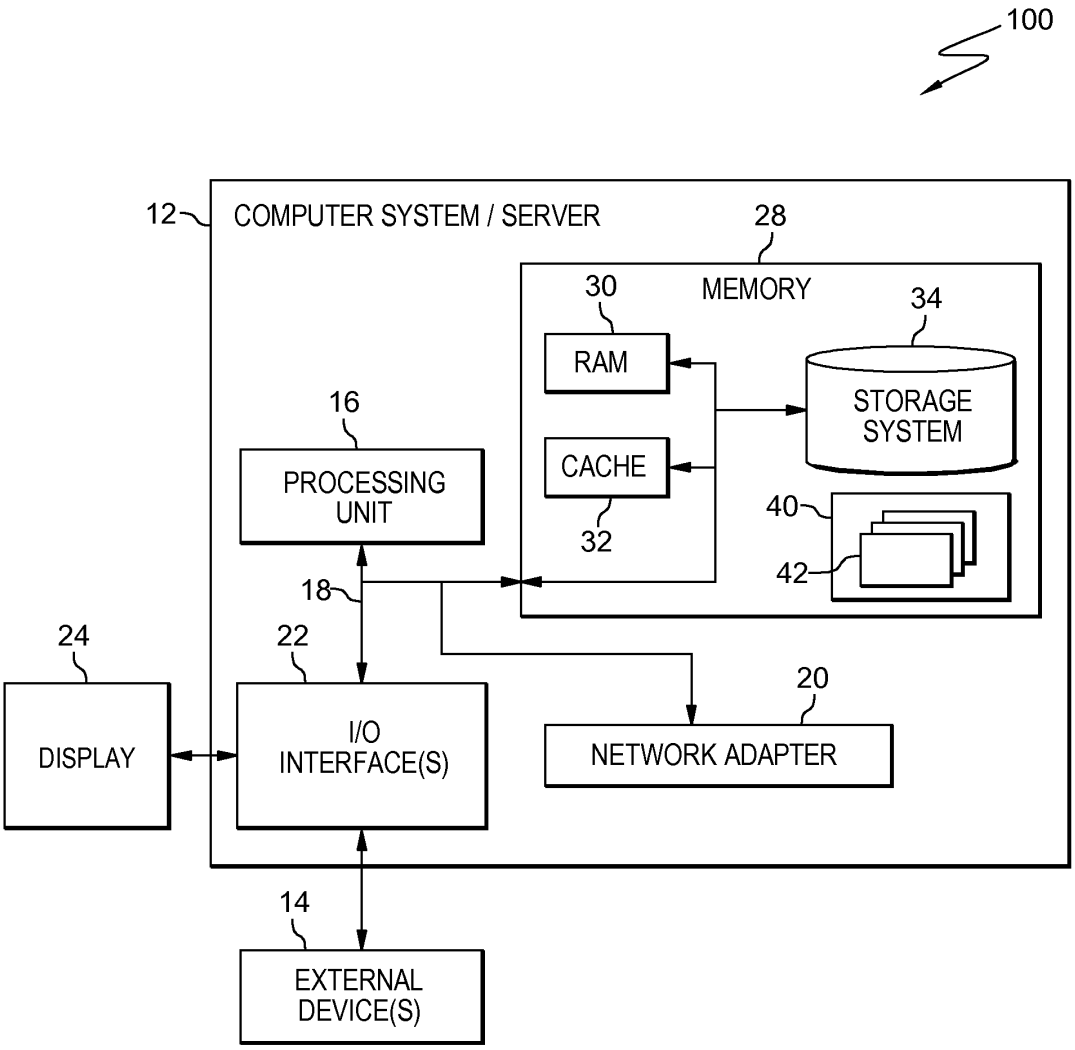

100
12
COMPUTER SYSTEM / SERVER
28
30
MEMORY
34
RAM
STORAGE SYSTEM
16
PROCESSING UNIT
CACHE
32
40
42
18
24
22
20
DISPLAY
I/O INTERFACE(S)
NETWORK ADAPTER
14
EXTERNAL DEVICE(S)

FIG. 1A

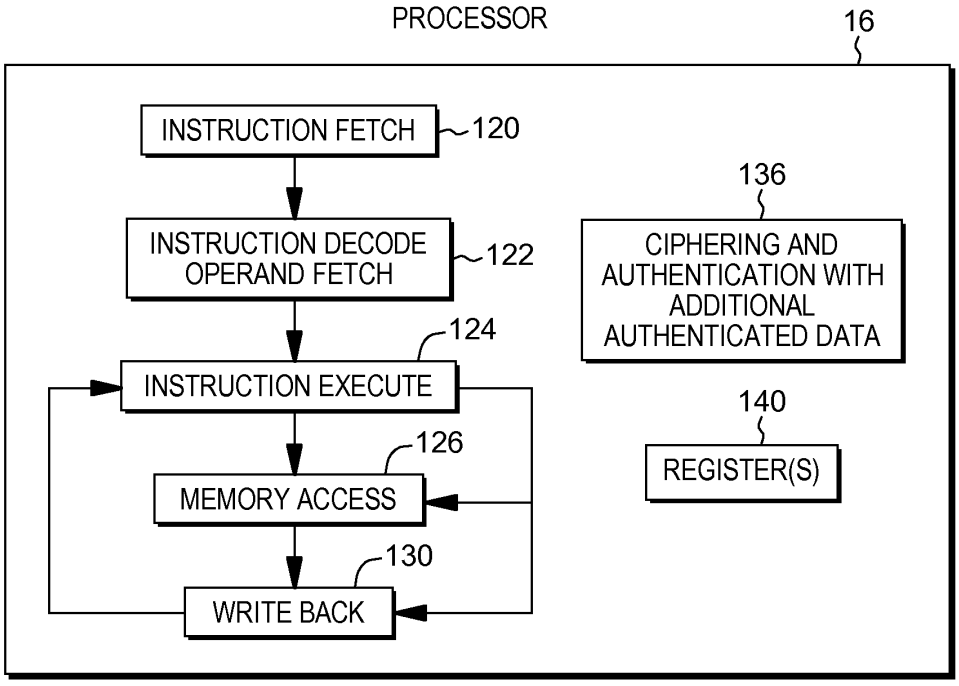

PROCESSOR
16
INSTRUCTION FETCH
120
INSTRUCTION DECODE OPERAND FETCH
122
124
INSTRUCTION EXECUTE
126
MEMORY ACCESS
130
WRITE BACK
136
CIPHERING AND AUTHENTICATION WITH ADDITIONAL AUTHENTICATED DATA
140
REGISTER(S)

FIG. 1B

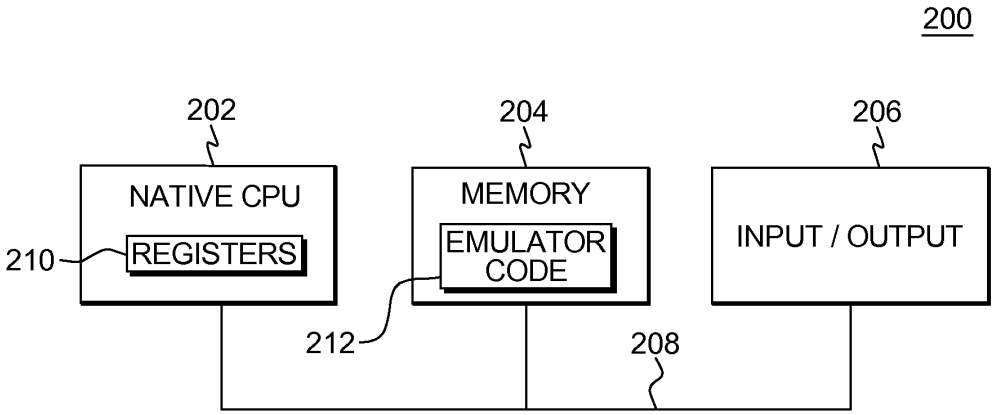

200
202
204
206
NATIVE CPU
REGISTERS
210
MEMORY
EMULATOR CODE
212
INPUT / OUTPUT
208

FIG. 2A

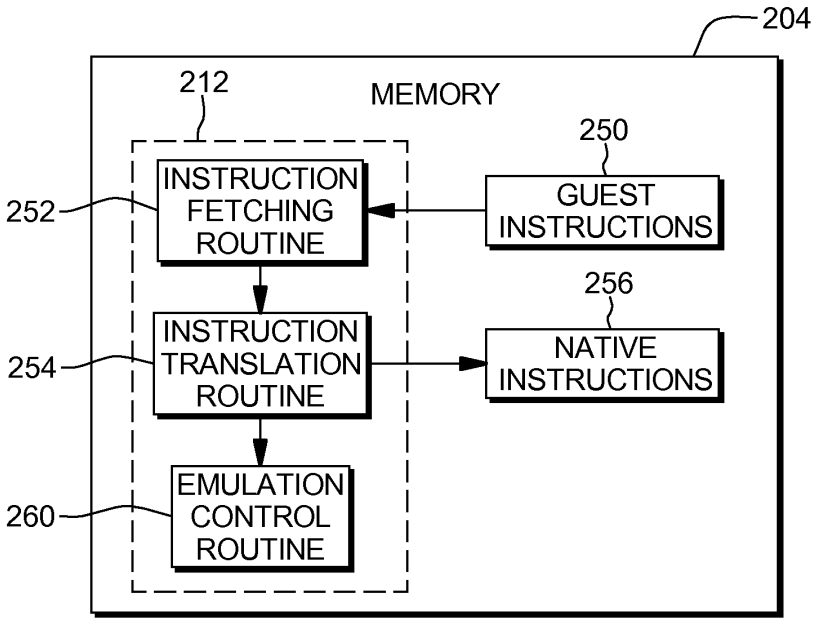

204
212
MEMORY
250
252
INSTRUCTION FETCHING ROUTINE
GUEST INSTRUCTIONS
256
254
INSTRUCTION TRANSLATION ROUTINE
NATIVE INSTRUCTIONS
260
EMULATION CONTROL ROUTINE

FIG. 2B

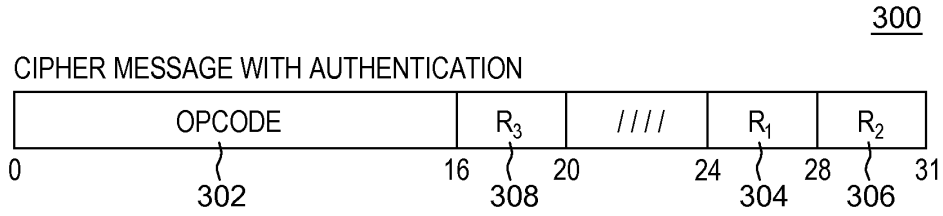


FIG. 3A

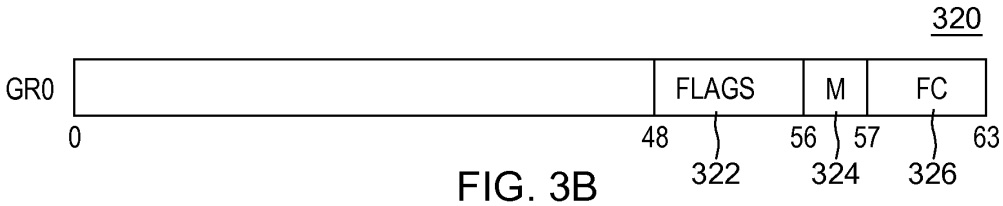


FIG. 3B

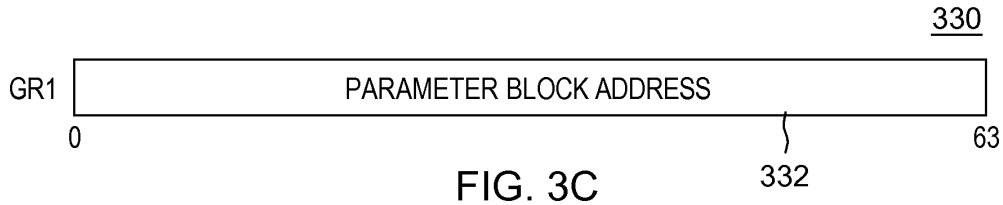


FIG. 3C

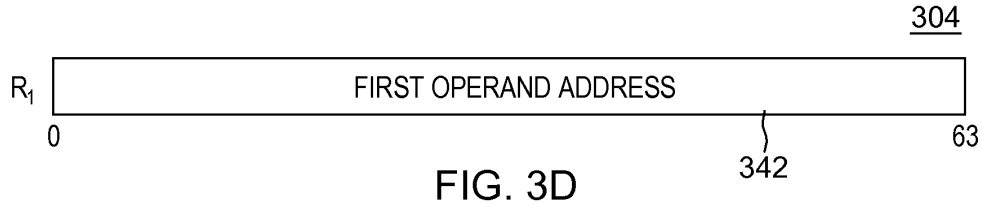


FIG. 3D

FIG. 3E

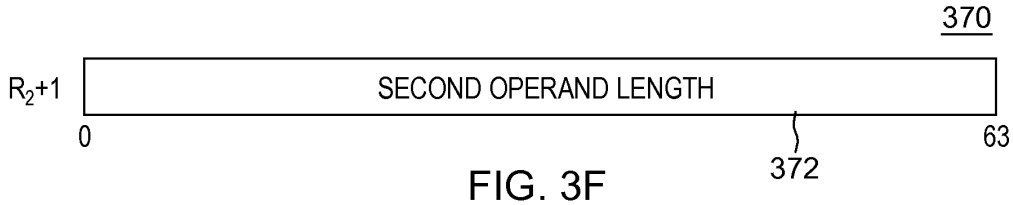


FIG. 3F

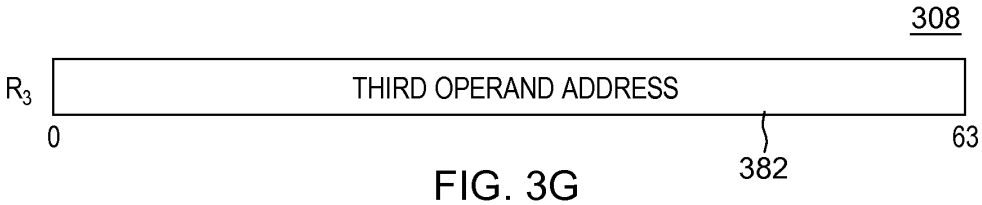

308
R3
THIRD OPERAND ADDRESS
0
63
382

FIG. 3G

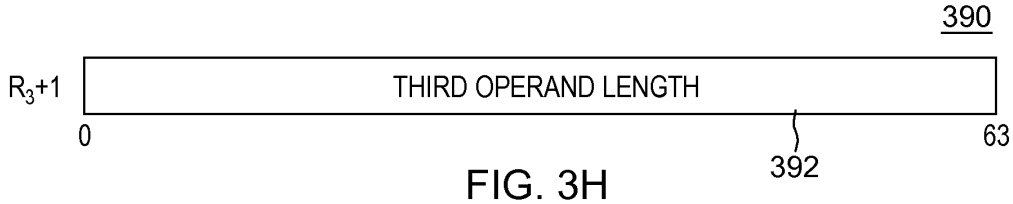

390
R3+1
THIRD OPERAND LENGTH
0
63
392

FIG. 3H

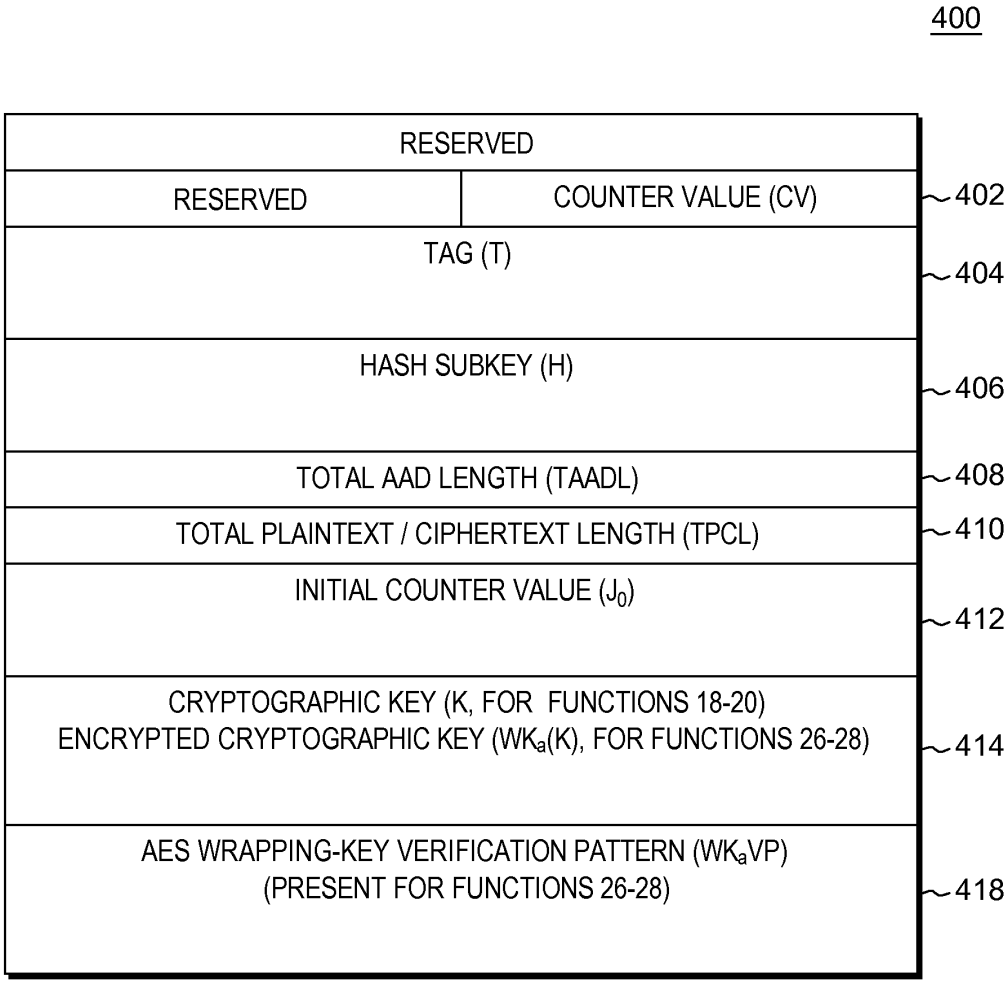
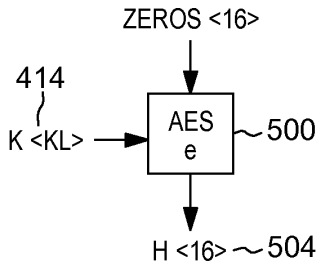
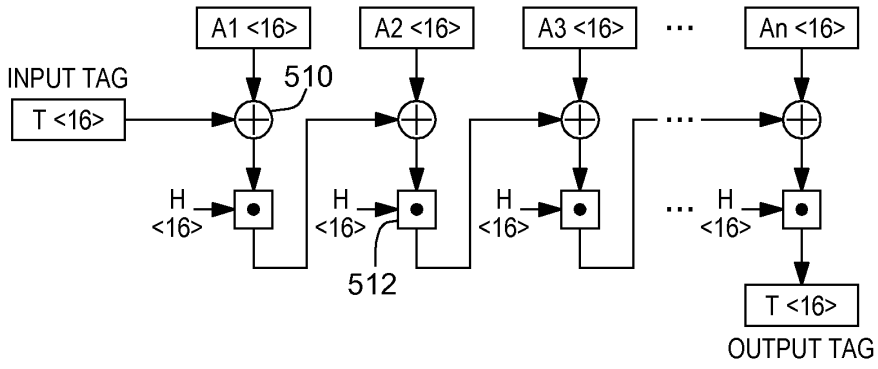

400
RESERVED
RESERVED
COUNTER VALUE (CV)
402
TAG (T)
404
HASH SUBKEY (H)
406
TOTAL AAD LENGTH (TAADL)
408
TOTAL PLAINTEXT / CIPHERTEXT LENGTH (TPCL)
410
INITIAL COUNTER VALUE (J_0)
412
CRYPTOGRAPHIC KEY (K, FOR FUNCTIONS 18-20)
ENCRYPTED CRYPTOGRAPHIC KEY (WK_a(K), FOR FUNCTIONS 26-28)
414
AES WRAPPING-KEY VERIFICATION PATTERN (WK_aVP)
(PRESENT FOR FUNCTIONS 26-28)
418

FIG. 4



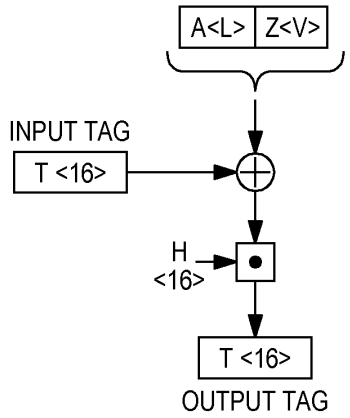
SYMBOL	EXPLANATION
<n>	LENGTH OF ITEM IN BYTES
H	HASH SUBKEY
K	KEY VALUE
KL	KEY LENGTH

FIG. 5A



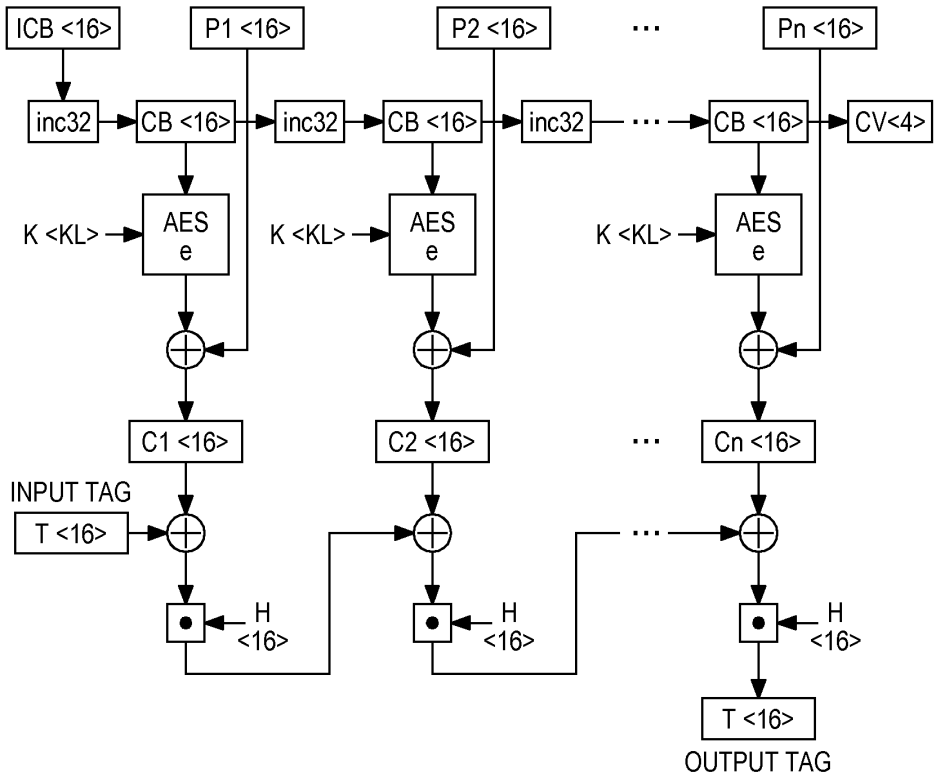
SYMBOL	EXPLANATION
<n>	LENGTH OF ITEM IN BYTES
An	BLOCK n OF ADDITIONAL AUTHENTICATED DATA (THIRD OPERAND)
H	HASH SUBKEY
T	MESSAGE AUTHENTICATION TAG (IN THE PARAMETER BLOCK)

FIG. 5B



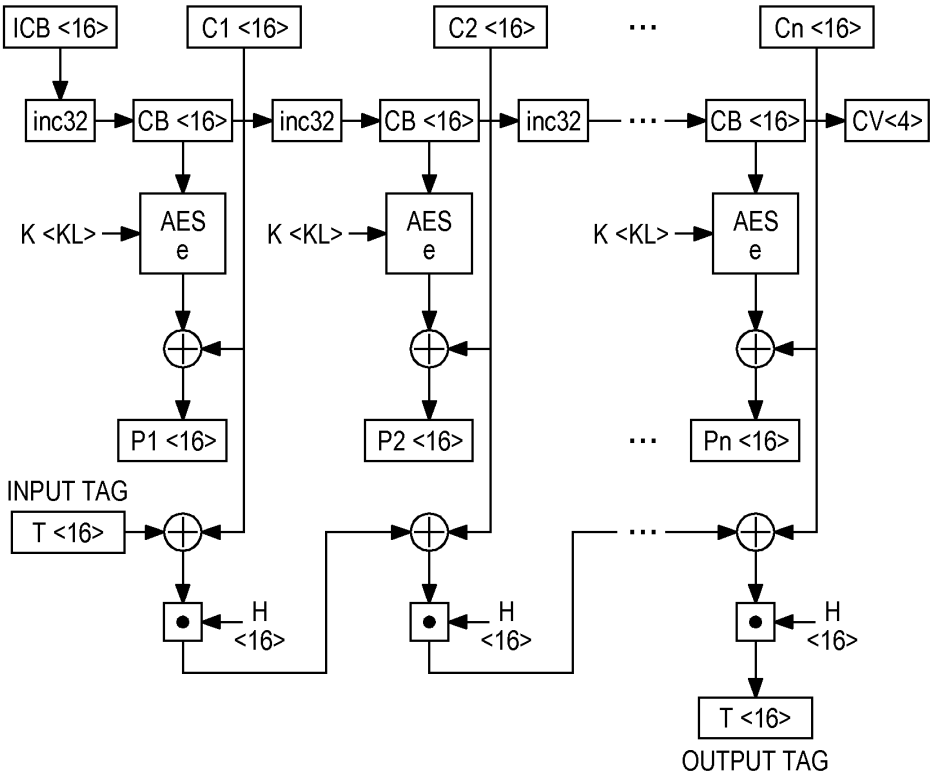
SYMBOL	EXPLANATION
<n>	LENGTH OF ITEM IN BYTES
A	LAST (SHORT) BLOCK OF ADDITIONAL AUTHENTICATED DATA (IN THE THIRD OPERAND)
H	HASH SUBKEY
L	LENGTH OF LAST THIRD OPERAND BLOCK IN BYTES (BETWEEN 1 AND 15)
T	MESSAGE AUTHENTICATION TAG (IN THE PARAMETER BLOCK)
V	NUMBER OF BYTES OF ZEROS TO PAD THE LAST BLOCK: 16 - L
Z	ZEROS

FIG. 5C



SYMBOL	EXPLANATION
<n>	LENGTH OF ITEM IN BYTES
CB	COUNTER BLOCK FORMED FROM THE CONCATENATION OF THE LEFTMOST 12 BYTES OF J_0 WITH THE INCREMENTED COUNTER VALUE (CV)
Cn	BLOCK n OF THE CIPHERTEXT (FIRST OPERAND)
CV	COUNTER VALUE STORED INTO THE PARAMETER BLOCK
H	HASH SUBKEY
ICB	INITIAL COUNTER BLOCK COMPRISING THE LEFTMOST 12 BYTES OF THE INITIAL-COUNTER VALUE (J_0) CONCATENATED WITH THE 4-BYTE COUNTER VALUE (CV)
inc32	INCREMENTING OF THE 32-BIT COUNTER VALUE (CV); A CARRY OUT OF THE LEFTMOST BIT POSITION IS IGNORED
K	KEY VALUE
KL	KEY LENGTH
Pn	BLOCK n OF THE PLAINTEXT (SECOND OPERAND)
T	MESSAGE AUTHENTICATION TAG (IN THE PARAMETER BLOCK)

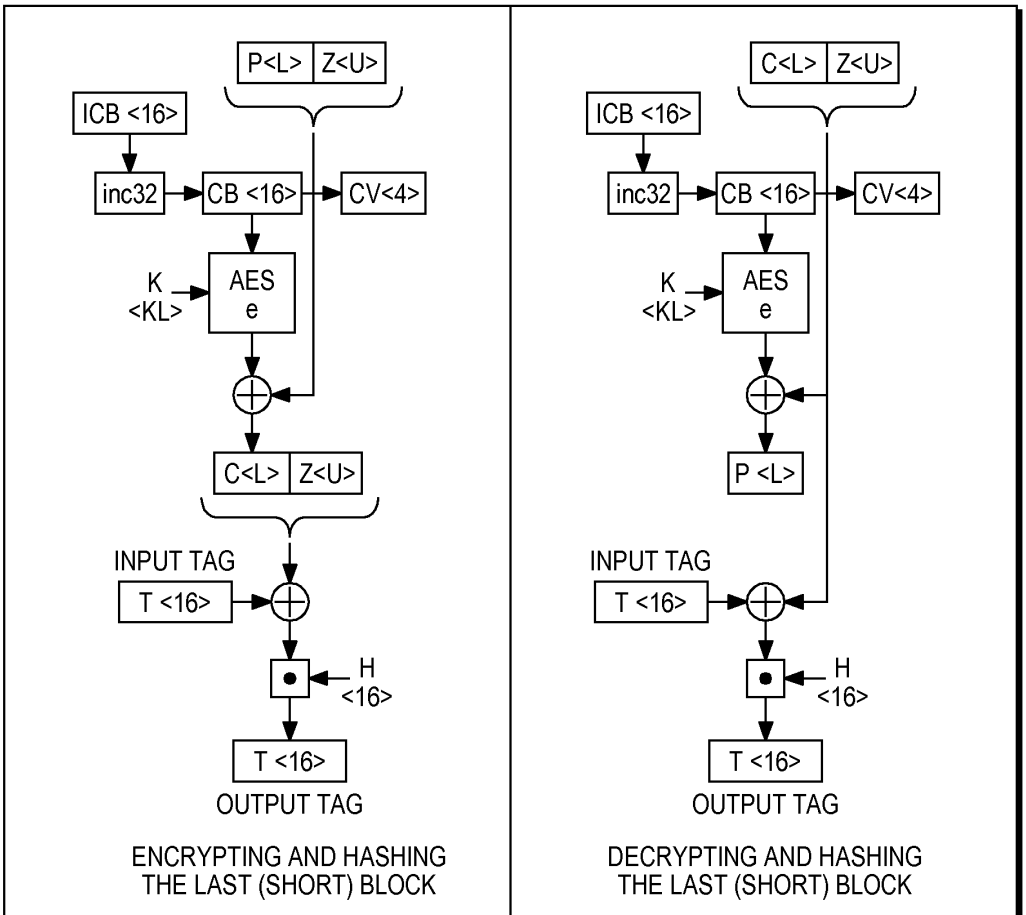
FIG. 5D



SYMBOL	EXPLANATION
Cn	BLOCK n OF THE CIPHERTEXT (SECOND OPERAND)
Pn	BLOCK n OF THE PLAINTEXT (FIRST OPERAND)

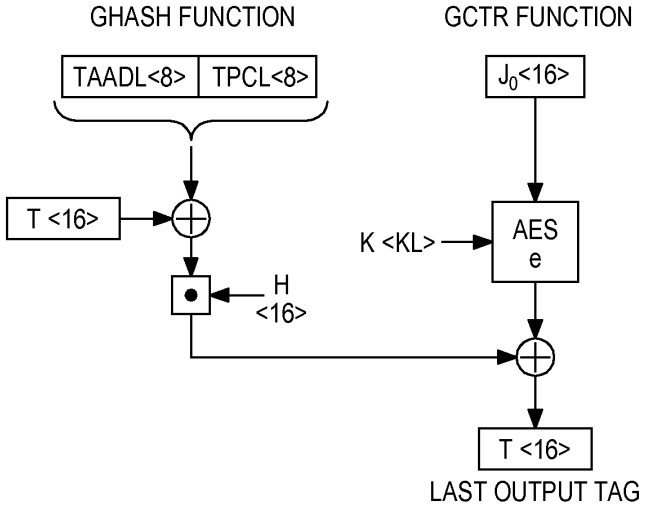
OTHER SYMBOLS THE SAME AS FIG. 5D

FIG. 5E



SYMBOL	EXPLANATION
<n>	LENGTH OF ITEM IN BYTES
CB	COUNTER BLOCK FORMED FROM THE CONCATENATION OF THE LEFTMOST 12 BYTES OF J_0 WITH THE INCREMENTED COUNTER VALUE (CV)
C	LAST (SHORT) BLOCK OF THE CIPHERTEXT (FIRST OPERAND WHEN M=0, SECOND OPERAND WHEN M=1)
CV	COUNTER VALUE (IN THE PARAMETER BLOCK)
H	HASH SUBKEY
ICB	INITIAL COUNTER BLOCK COMPRISING THE LEFTMOST 12 BYTES OF THE INITIAL-COUNTER VALUE (J_0) CONCATENATED WITH THE 4-BYTE COUNTER VALUE (CV)
inc32	INCREMENTING OF THE 32-BIT COUNTER VALUE (CV); A CARRY OUT OF THE LEFTMOST BIT POSITION IS IGNORED
K	KEY VALUE
KL	KEY LENGTH
L	LENGTH OF LAST SECOND OPERAND BLOCK IN BYTES (BETWEEN 1 AND 15)
P	LAST (SHORT) BLOCK n OF THE PLAINTEXT (SECOND OPERAND WHEN M=0, FIRST OPERAND WHEN M=1)
T	MESSAGE AUTHENTICATION TAG (IN THE PARAMETER BLOCK)
U	NUMBER OF BYTES OF ZEROS TO PAD THE LAST BLOCK: 16 - L
Z	ZEROS

FIG. 5F



SYMBOL	EXPLANATION
<n>	LENGTH OF ITEM IN BYTES
H	HASH SUBKEY
J_0	INITIAL COUNTER VALUE (FROM THE PARAMETER BLOCK)
K	KEY VALUE
KL	KEY LENGTH
T	MESSAGE AUTHENTICATION TAG (IN THE PARAMETER BLOCK)
TAADL	TOTAL LENGTH OF THE MESSAGE'S ADDITIONAL AUTHENTICATED DATA (AAD) IN BITS (FROM THE PARAMETER BLOCK)
TPCL	TOTAL LENGTH OF THE MESSAGE'S PLAINTEXT OR CIPHERTEXT IN BITS (FROM THE PARAMETER BLOCK)

FIG. 5G

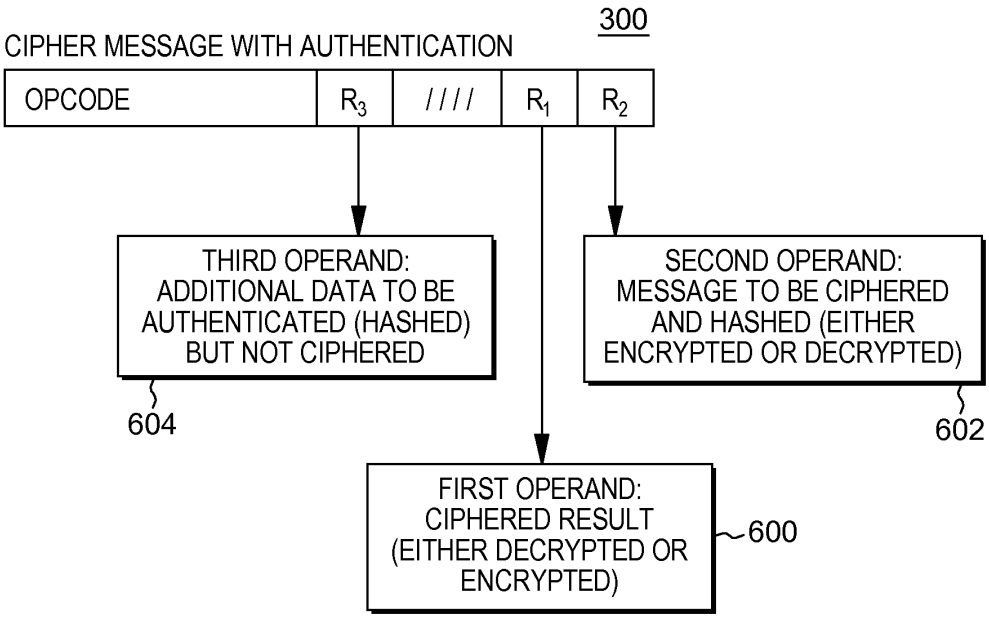

300
CIPHER MESSAGE WITH AUTHENTICATION
OPCODE
R3
////
R1
R2
THIRD OPERAND: ADDITIONAL DATA TO BE AUTHENTICATED (HASHED) BUT NOT CIPHERED
604
SECOND OPERAND: MESSAGE TO BE CIPHERED AND HASHED (EITHER ENCRYPTED OR DECRYPTED)
602
FIRST OPERAND: CIPHERED RESULT (EITHER DECRYPTED OR ENCRYPTED)
600

FIG. 6

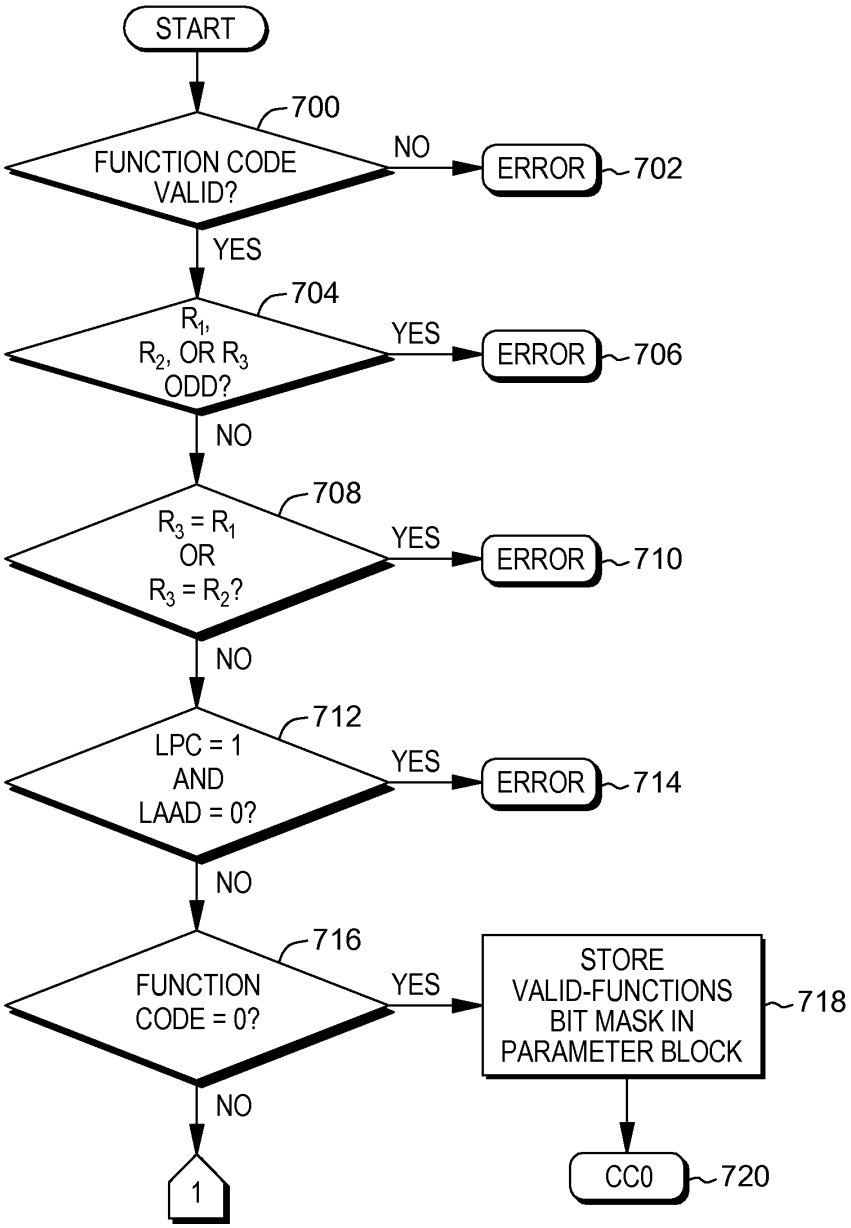

START
700
FUNCTION CODE VALID?
NO
ERROR
702
YES
704
R1, R2, OR R3 ODD?
YES
ERROR
706
NO
708
R3 = R1 OR R3 = R2?
YES
ERROR
710
NO
712
LPC = 1 AND LAAD = 0?
YES
ERROR
714
NO
716
FUNCTION CODE = 0?
YES
STORE VALID-FUNCTIONS BIT MASK IN PARAMETER BLOCK
718
NO
1
CC0
720

FIG. 7A

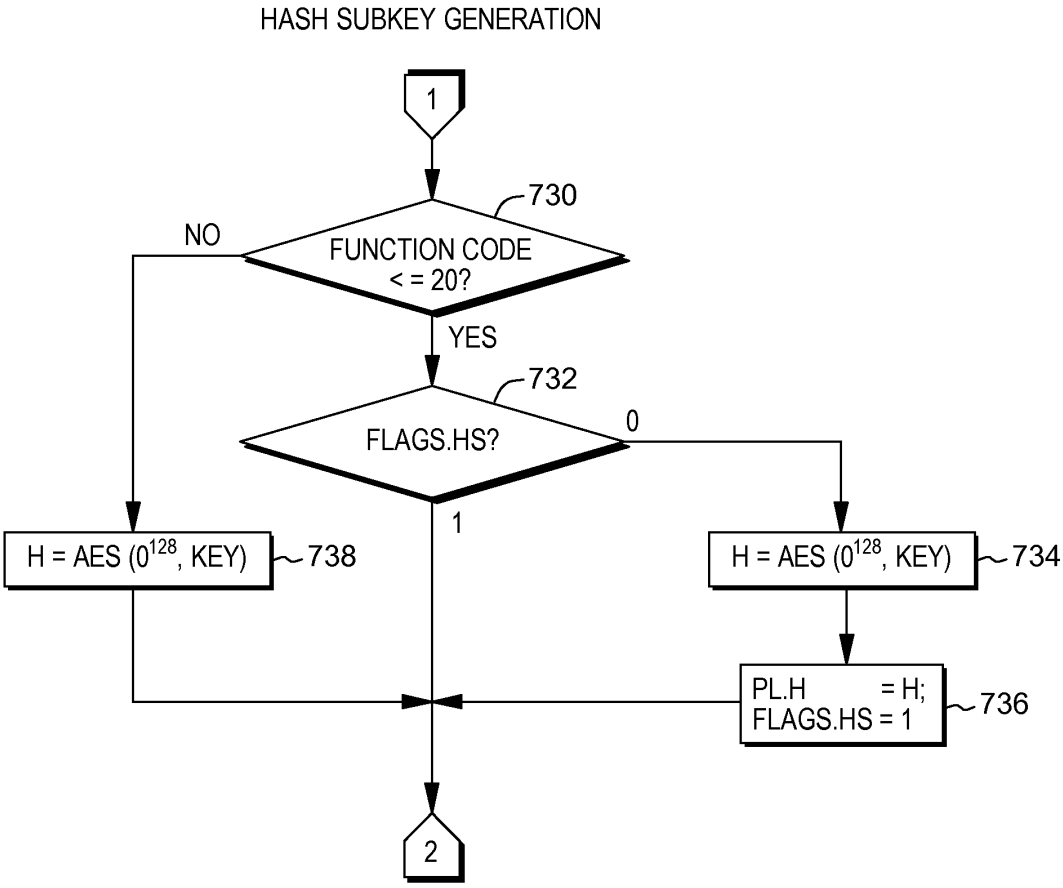

HASH SUBKEY GENERATION
1
730
NO
FUNCTION CODE
< = 20?
YES
732
FLAGS.HS?
0
1
H = AES (0^128, KEY)
738
H = AES (0^128, KEY)
734
PL.H = H;
FLAGS.HS = 1
736
2

FIG. 7B

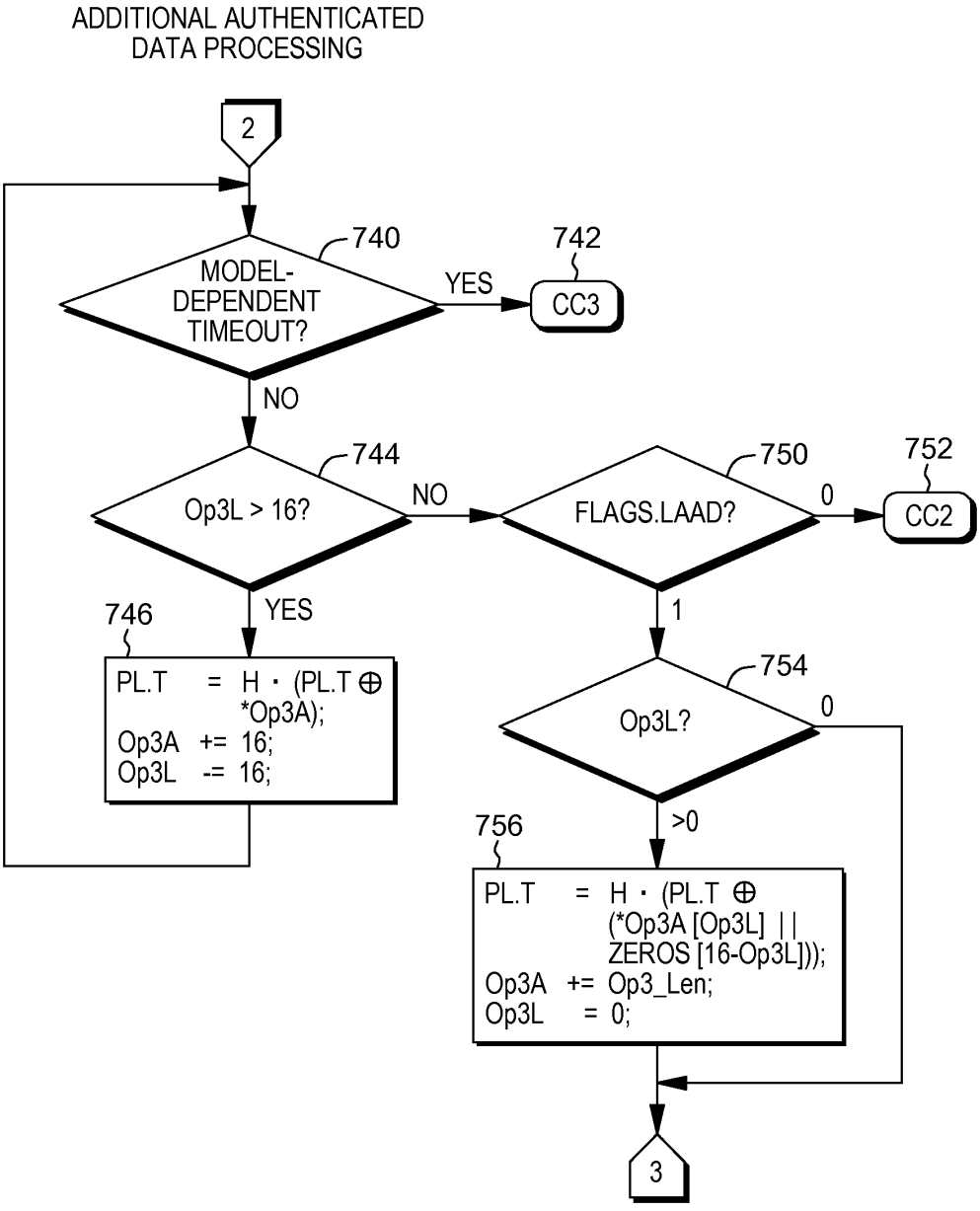

ADDITIONAL AUTHENTICATED DATA PROCESSING
2
740
MODEL-DEPENDENT TIMEOUT?
YES
742
CC3
NO
744
Op3L > 16?
NO
750
FLAGS.LAAD?
0
752
CC2
YES
1
746
PL.T = H · (PL.T ⊕ *Op3A);
Op3A += 16;
Op3L -= 16;
754
Op3L?
0
>0
756
PL.T = H · (PL.T ⊕ (*Op3A [Op3L] || ZEROS [16-Op3L]));
Op3A += Op3_Len;
Op3L = 0;
3

FIG. 7C

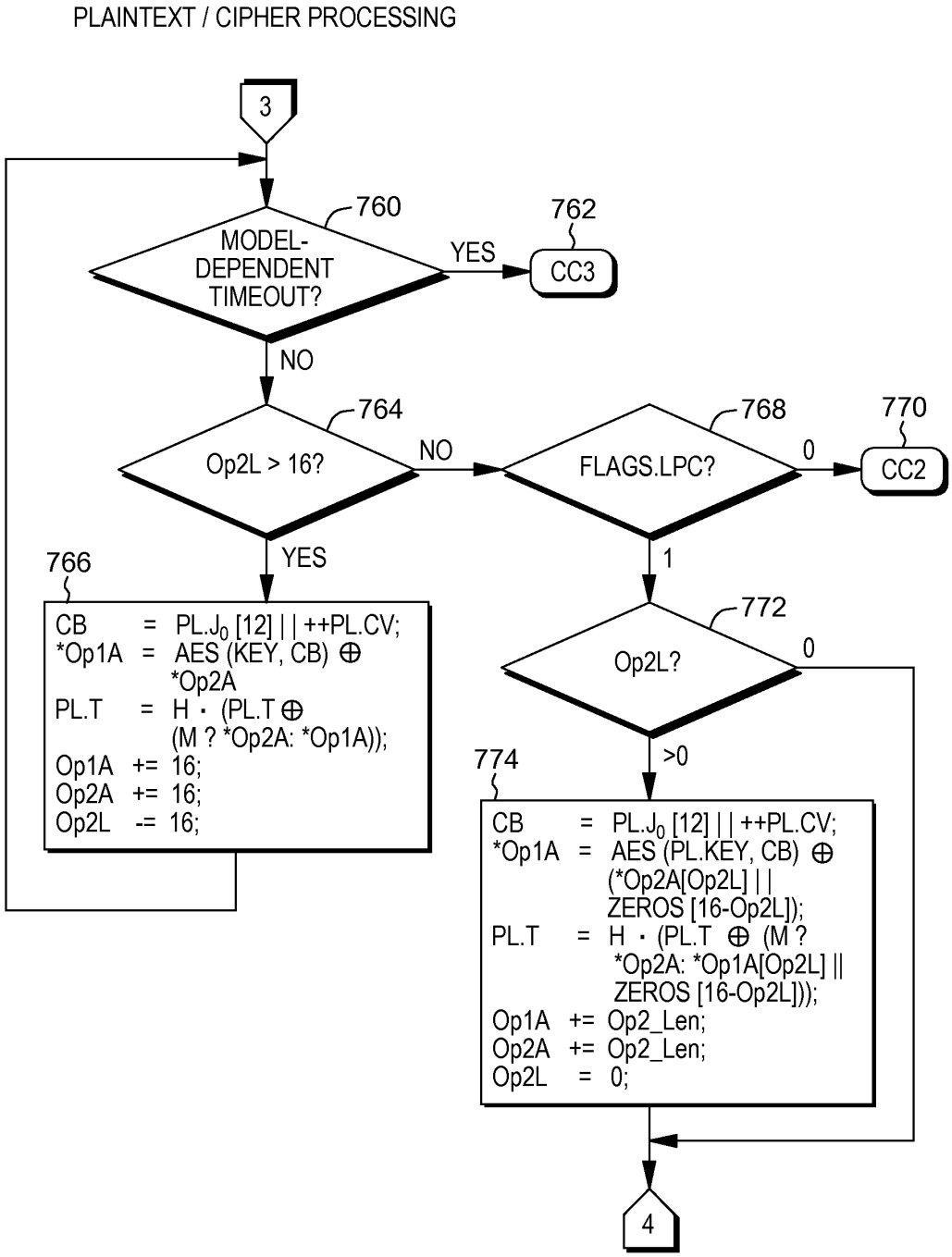

PLAINTEXT / CIPHER PROCESSING
3
760
MODEL-DEPENDENT TIMEOUT?
YES
762
CC3
NO
764
Op2L > 16?
NO
768
FLAGS.LPC?
0
770
CC2
YES
1
766
CB = PL.J0 [12] | | ++PL.CV;
*Op1A = AES (KEY, CB) ⊕ *Op2A
PL.T = H · (PL.T ⊕ (M ? *Op2A: *Op1A));
Op1A += 16;
Op2A += 16;
Op2L -= 16;
772
Op2L?
0
>0
774
CB = PL.J0 [12] | | ++PL.CV;
*Op1A = AES (PL.KEY, CB) ⊕ (*Op2A[Op2L] | | ZEROS [16-Op2L]);
PL.T = H · (PL.T ⊕ (M ? *Op2A: *Op1A[Op2L] || ZEROS [16-Op2L]));
Op1A += Op2_Len;
Op2A += Op2_Len;
Op2L = 0;
4

FIG. 7D

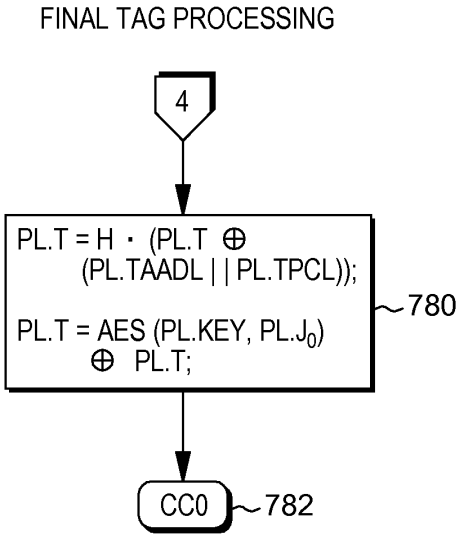

FINAL TAG PROCESSING
4
PL.T = H · (PL.T ⊕
(PL.TAADL | | PL.TPCL));
PL.T = AES (PL.KEY, PL.J0)
⊕ PL.T;
780
CC0
782

FIG. 7E

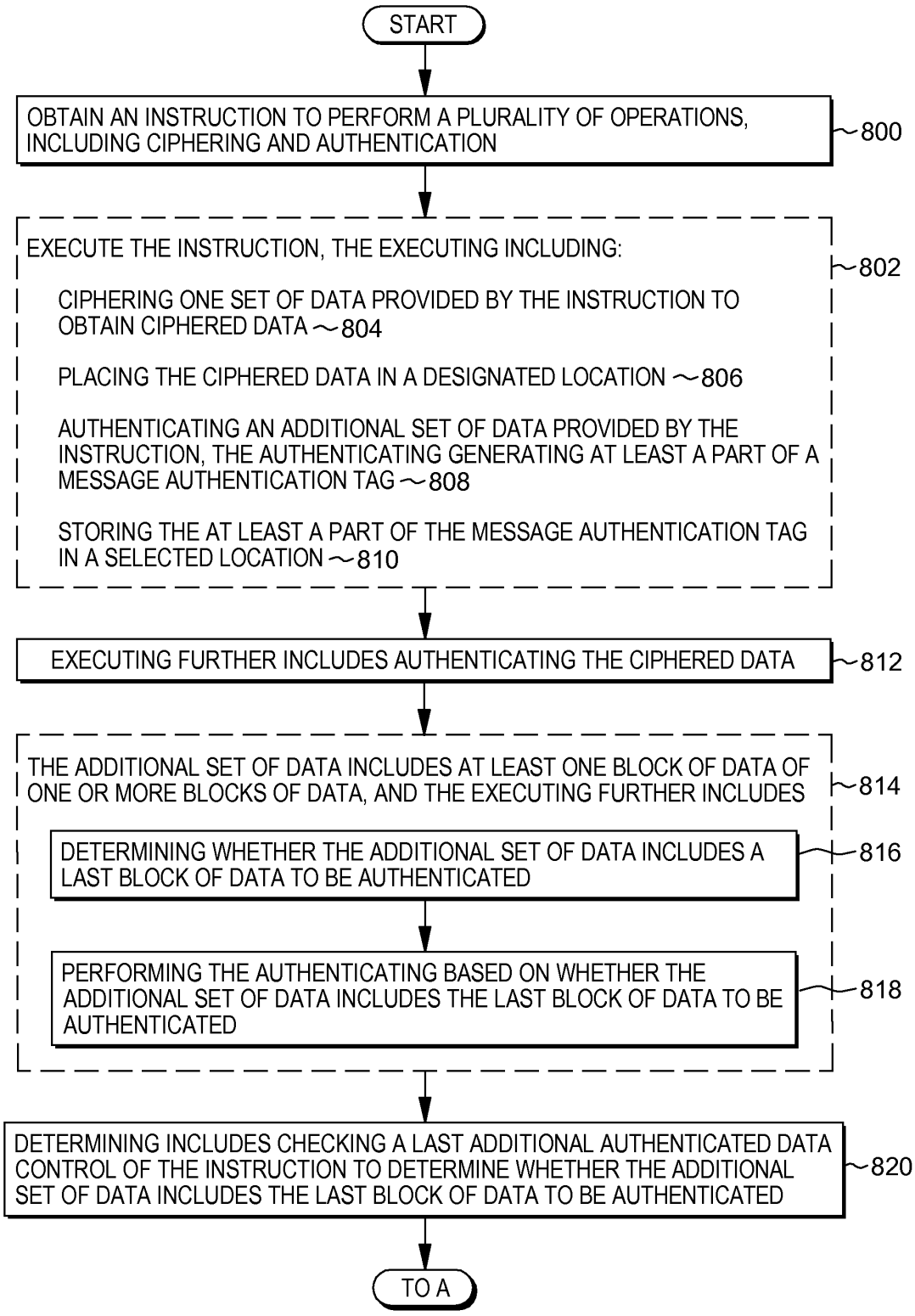

START
OBTAIN AN INSTRUCTION TO PERFORM A PLURALITY OF OPERATIONS, INCLUDING CIPHERING AND AUTHENTICATION
800
EXECUTE THE INSTRUCTION, THE EXECUTING INCLUDING:
802
CIPHERING ONE SET OF DATA PROVIDED BY THE INSTRUCTION TO OBTAIN CIPHERED DATA
804
PLACING THE CIPHERED DATA IN A DESIGNATED LOCATION
806
AUTHENTICATING AN ADDITIONAL SET OF DATA PROVIDED BY THE INSTRUCTION, THE AUTHENTICATING GENERATING AT LEAST A PART OF A MESSAGE AUTHENTICATION TAG
808
STORING THE AT LEAST A PART OF THE MESSAGE AUTHENTICATION TAG IN A SELECTED LOCATION
810
EXECUTING FURTHER INCLUDES AUTHENTICATING THE CIPHERED DATA
812
THE ADDITIONAL SET OF DATA INCLUDES AT LEAST ONE BLOCK OF DATA OF ONE OR MORE BLOCKS OF DATA, AND THE EXECUTING FURTHER INCLUDES
814
DETERMINING WHETHER THE ADDITIONAL SET OF DATA INCLUDES A LAST BLOCK OF DATA TO BE AUTHENTICATED
816
PERFORMING THE AUTHENTICATING BASED ON WHETHER THE ADDITIONAL SET OF DATA INCLUDES THE LAST BLOCK OF DATA TO BE AUTHENTICATED
818
DETERMINING INCLUDES CHECKING A LAST ADDITIONAL AUTHENTICATED DATA CONTROL OF THE INSTRUCTION TO DETERMINE WHETHER THE ADDITIONAL SET OF DATA INCLUDES THE LAST BLOCK OF DATA TO BE AUTHENTICATED
820
TO A

FIG. 8A

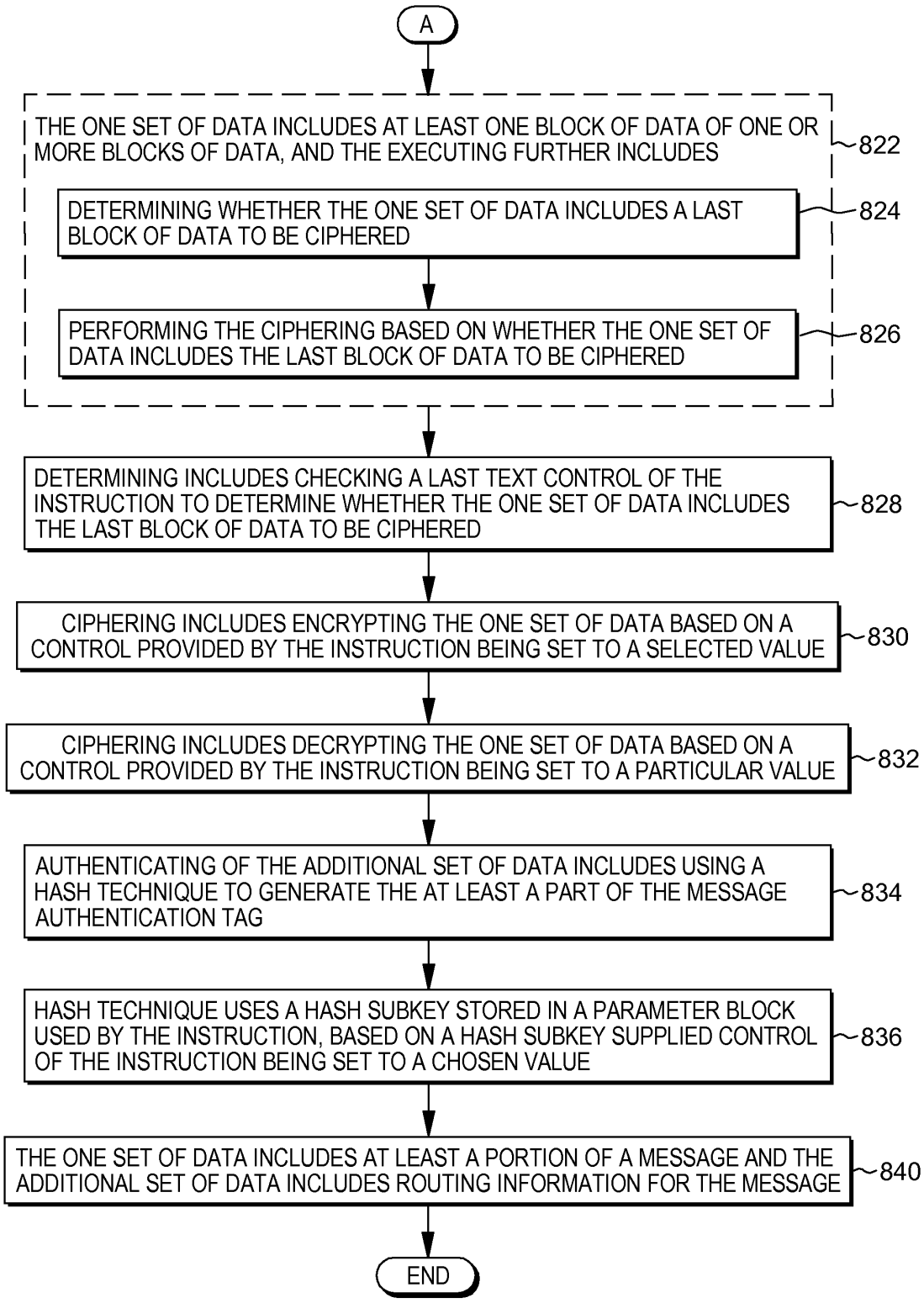

A
THE ONE SET OF DATA INCLUDES AT LEAST ONE BLOCK OF DATA OF ONE OR MORE BLOCKS OF DATA, AND THE EXECUTING FURTHER INCLUDES
822
DETERMINING WHETHER THE ONE SET OF DATA INCLUDES A LAST BLOCK OF DATA TO BE CIPHERED
824
PERFORMING THE CIPHERING BASED ON WHETHER THE ONE SET OF DATA INCLUDES THE LAST BLOCK OF DATA TO BE CIPHERED
826
DETERMINING INCLUDES CHECKING A LAST TEXT CONTROL OF THE INSTRUCTION TO DETERMINE WHETHER THE ONE SET OF DATA INCLUDES THE LAST BLOCK OF DATA TO BE CIPHERED
828
CIPHERING INCLUDES ENCRYPTING THE ONE SET OF DATA BASED ON A CONTROL PROVIDED BY THE INSTRUCTION BEING SET TO A SELECTED VALUE
830
CIPHERING INCLUDES DECRYPTING THE ONE SET OF DATA BASED ON A CONTROL PROVIDED BY THE INSTRUCTION BEING SET TO A PARTICULAR VALUE
832
AUTHENTICATING OF THE ADDITIONAL SET OF DATA INCLUDES USING A HASH TECHNIQUE TO GENERATE THE AT LEAST A PART OF THE MESSAGE AUTHENTICATION TAG
834
HASH TECHNIQUE USES A HASH SUBKEY STORED IN A PARAMETER BLOCK USED BY THE INSTRUCTION, BASED ON A HASH SUBKEY SUPPLIED CONTROL OF THE INSTRUCTION BEING SET TO A CHOSEN VALUE
836
THE ONE SET OF DATA INCLUDES AT LEAST A PORTION OF A MESSAGE AND THE ADDITIONAL SET OF DATA INCLUDES ROUTING INFORMATION FOR THE MESSAGE
840
END

FIG. 8B