

Fig. 1

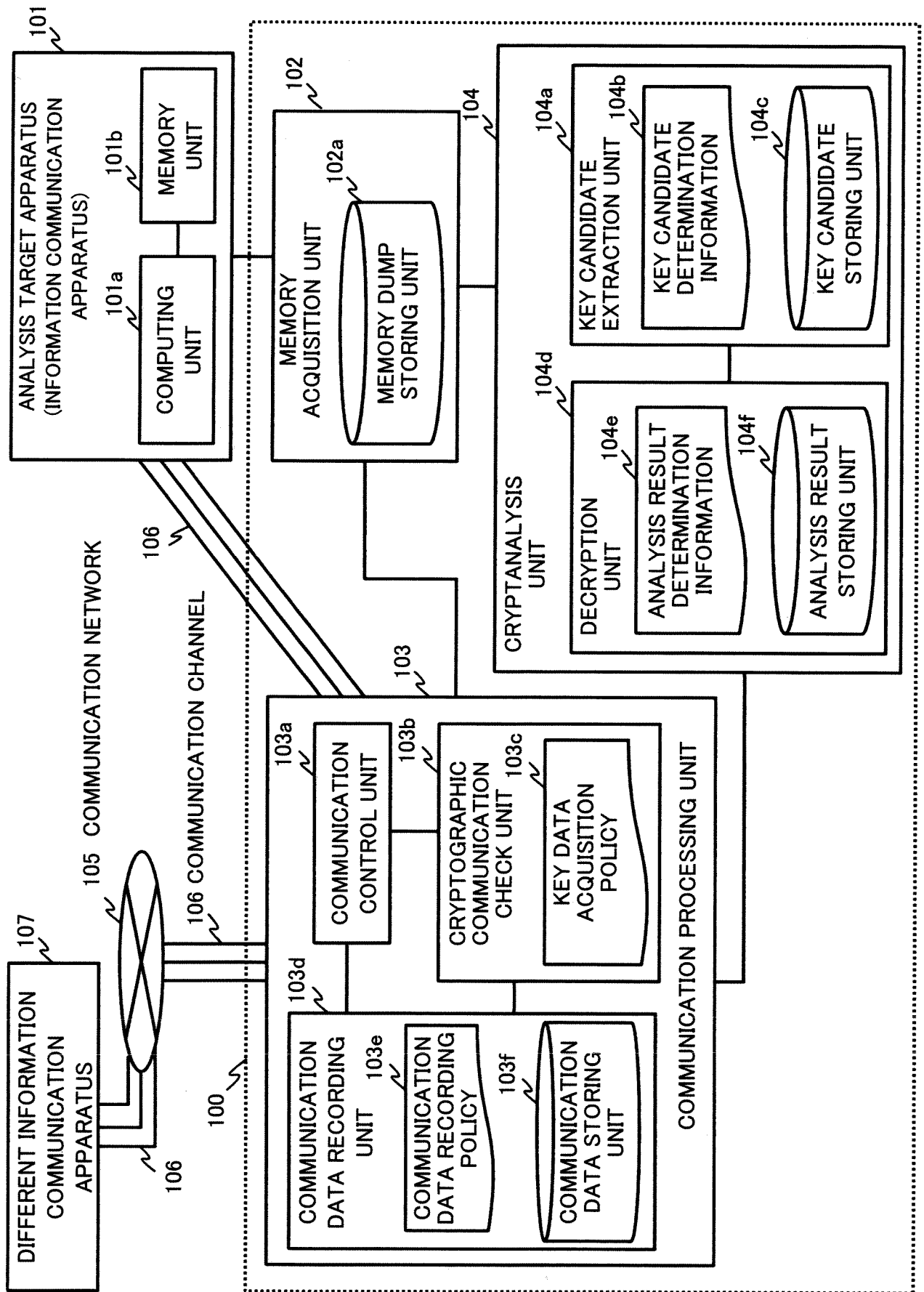


Fig. 2

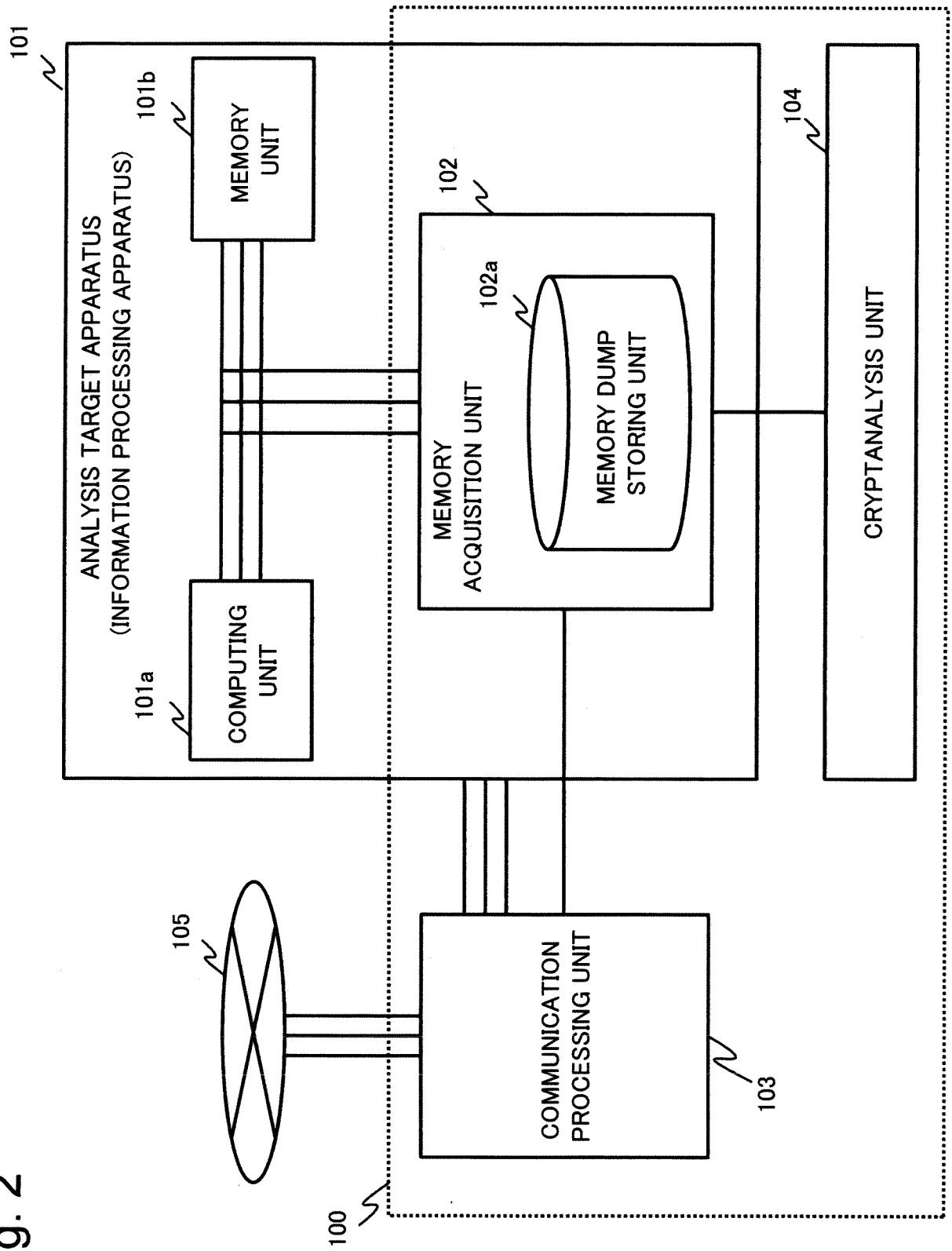


Fig. 3

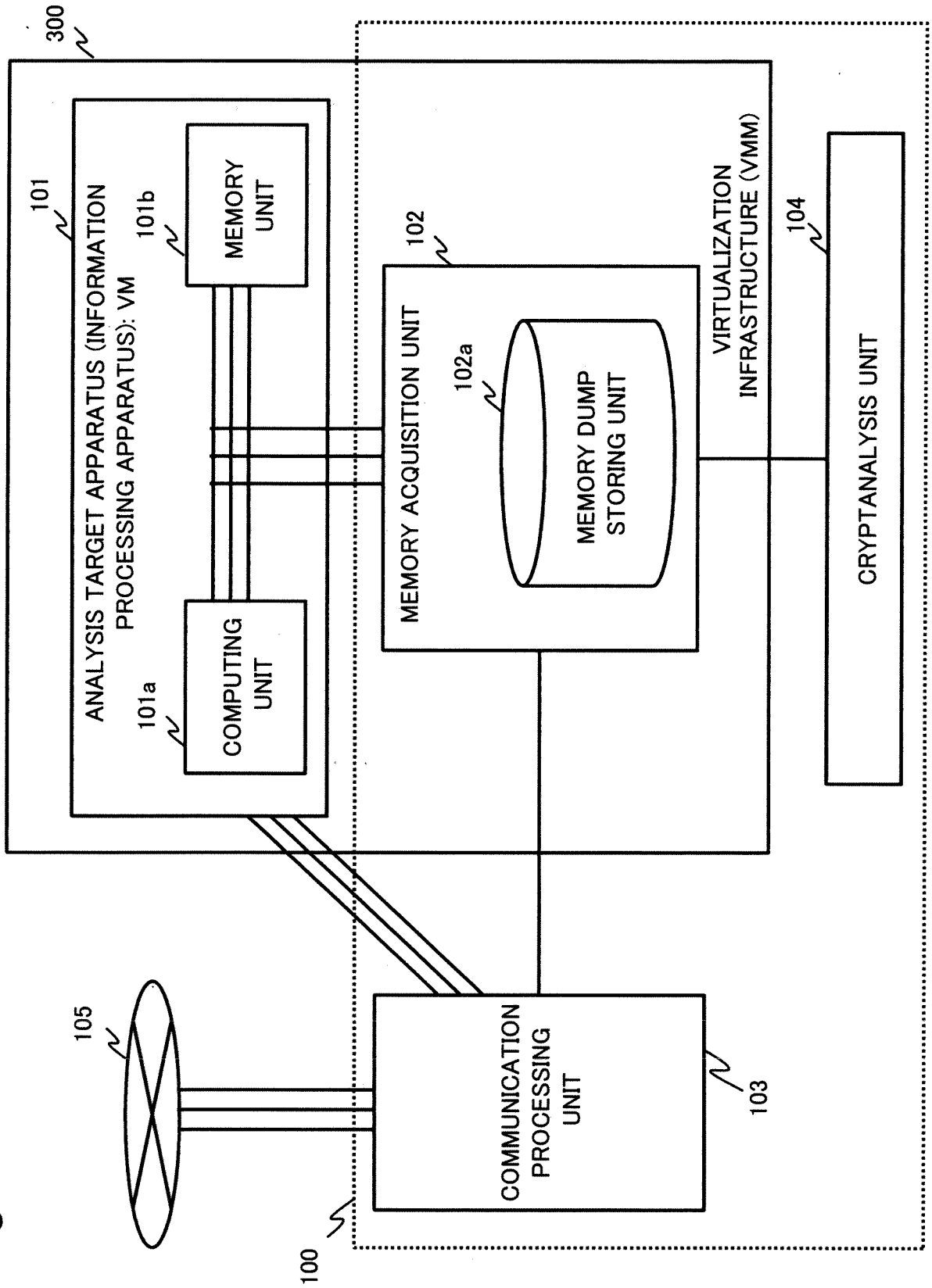


Fig. 4

103c

KEY DATA ACQUISITION POLICY		
CRYPTOGRAPHIC COMMUNICATION PROTOCOL	KEY DATA ACQUISITION CRITERION	PROCESSING CONTENT
SSL/TLS	(AFTER CHANGECIPHERSPEC IS TRANSMITTED FROM SSL/TLS SERVER) AND (BEFORE TRANSMISSION AND RECEPTION OF APPLICATION DATA START)	INSTRUCT MEMORY ACQUISITION UNIT TO ACQUIRE MEMORY. INSTRUCT COMMUNICATION PROCESSING UNIT TO SUSPEND COMMUNICATION.
SSH	(AFTER SSH2_MSG_NEWKEYS IS TRANSMITTED AND RECEIVED)	INSTRUCT MEMORY ACQUISITION UNIT TO ACQUIRE MEMORY. INSTRUCT COMMUNICATION PROCESSING UNIT TO SUSPEND COMMUNICATION.
IPSec (IKE)	...	...
...	...	...

Fig. 5

103e

COMMUNICATION DATA RECORDING POLICY		
501 CRYPTOGRAPHIC COMMUNICATION PROTOCOL	502 COMMUNICATION DATA RECORDING CRITERION	503 PROCESSING CONTENT
SSL/TLS	(AFTER TRANSMISSION AND RECEPTION OF APPLICATION DATA ARE STARTED)	RECORD COMMUNICATION DATA FOR EACH ORIGINATOR. RECORD SOURCE AND ACQUISITION TIME FOR EACH PIECE OF COMMUNICATION DATA.
SSH	...	...
IPSec (IKE)	...	...
...	...	...

Fig. 6

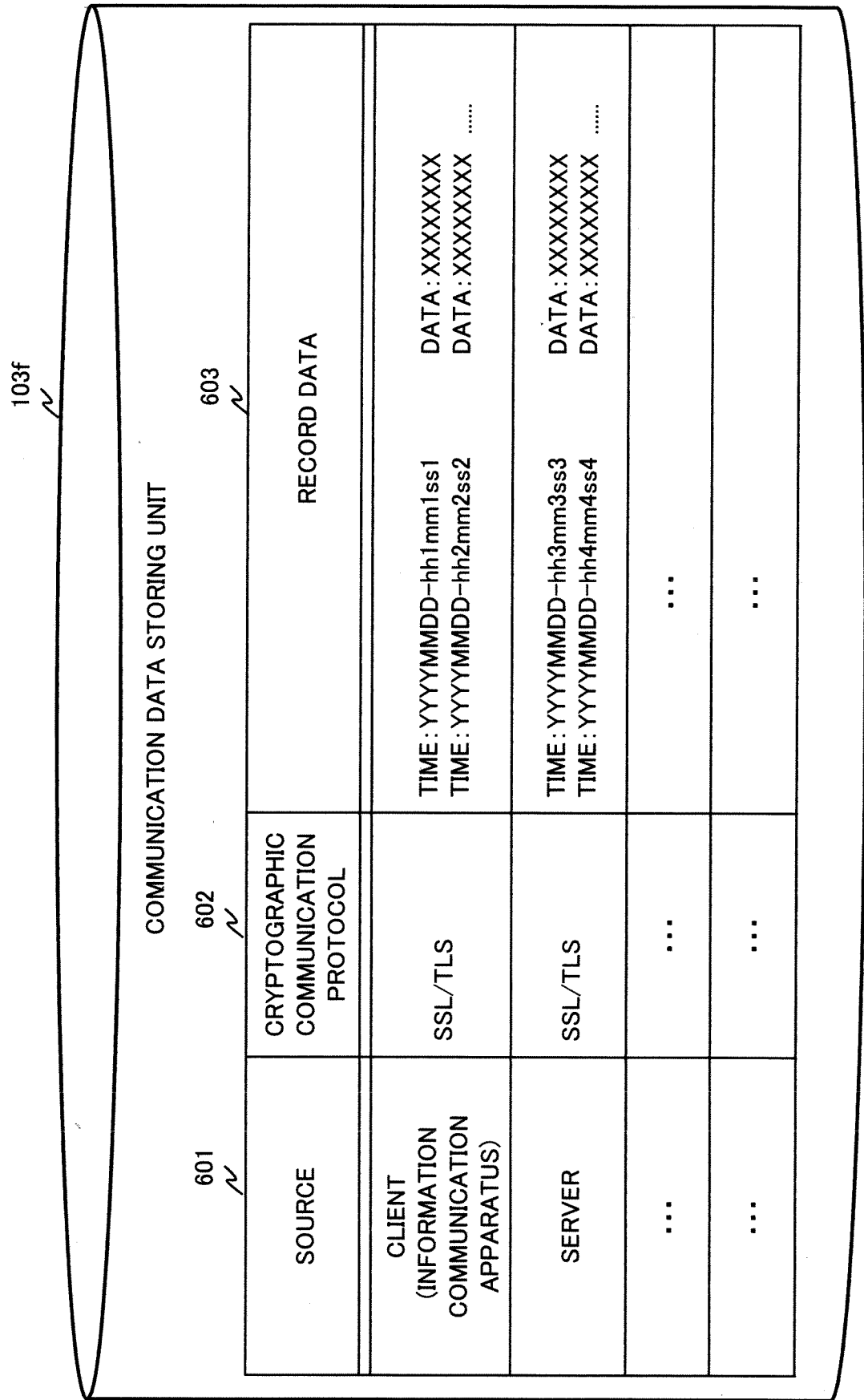


Fig. 7

104b

KEY CANDIDATE DETERMINATION INFORMATION				
701 ENCIPHERMENT ALGORITHM	702 ENCIPHERMENT PARAMETER		703 EXECUTION ENVIRONMENT INFORMATION	704 KEY CANDIDATE DETERMINATION CRITERION
	KEY LENGTH (UNIT: BIT)	CIPHER MODE OF OPERATION		
AES	128	CBC	A	16 CONSECUTIVE BYTES OF DATA AREA WITH ENTROPY VALUE GREATER THAN OR EQUAL TO SPECIFIC REFERENCE VALUE
AES	256	CBC	B	32 CONSECUTIVE BYTES OF DATA AREA WITH ENTROPY VALUE GREATER THAN OR EQUAL TO SPECIFIC REFERENCE VALUE
AES	128	GCM	C	560 CONSECUTIVE BYTES OF DATA STARTING FROM 0x30, 0x02, 0x00, 0x00, 0x4b, 0x53, 0x4D
...	...	...	...	...

Fig. 8

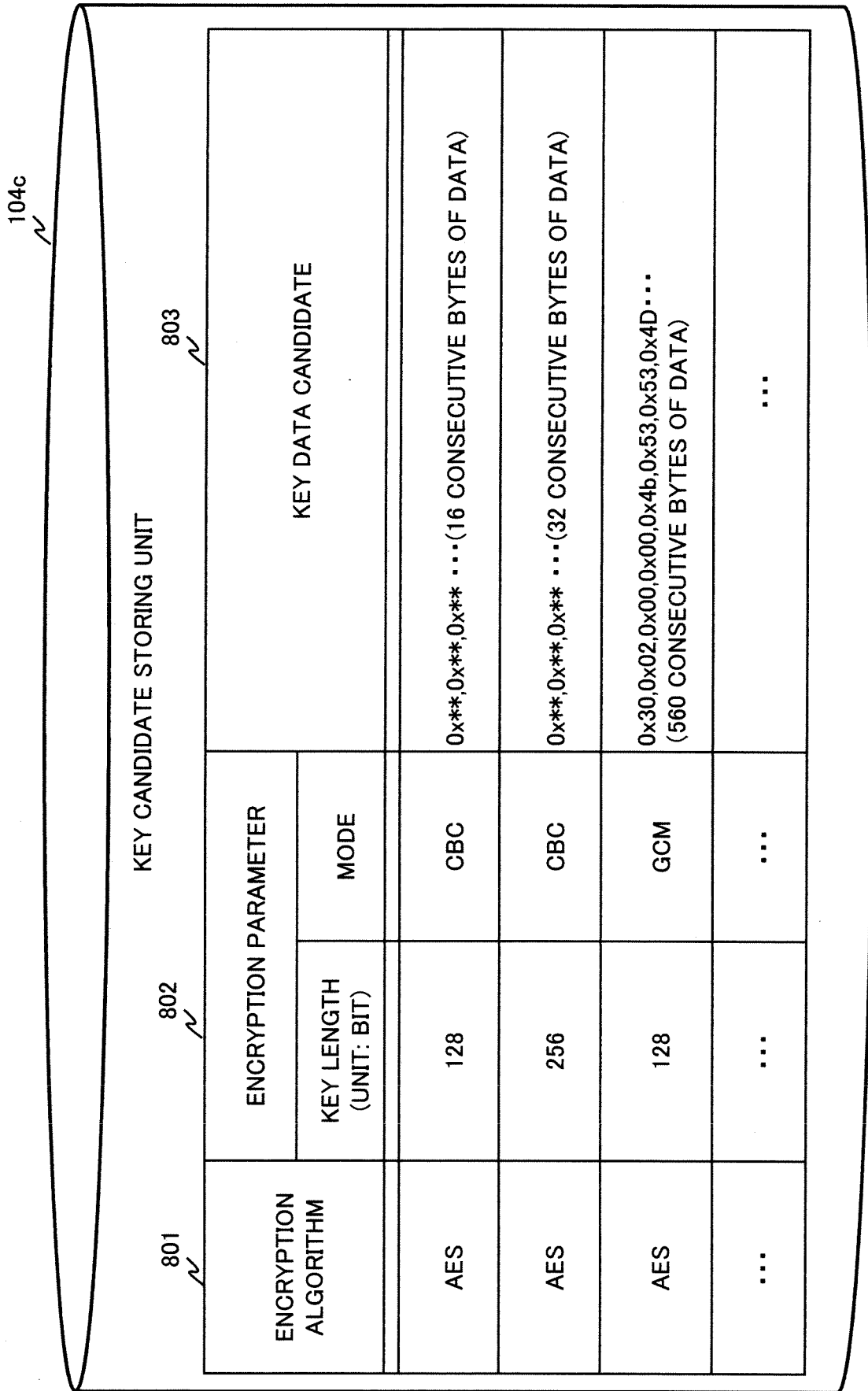


Fig. 9

ANALYSIS RESULT DETERMINATION INFORMATION	
901	902
ANALYSIS RESULT DETERMINATION CRITERION	DETERMINATION RESULT
(ENTROPY OF DECODING PROCESSING RESULT) $\leq$ (SPECIFIC REFERENCE VALUE)	DECRYPTION SUCCEEDED
(ENTROPY OF DECODING PROCESSING RESULT) $>$ (SPECIFIC REFERENCE VALUE)	DECRYPTION FAILED
(FIRST 4 BYTES OF PAYLOAD INCLUDED IN DECODING PROCESSING RESULT ARE "GET")	DECRYPTION SUCCEEDED
...	...

Fig. 10

104f
~

ANALYSIS RESULT STORING UNIT		
1001 ~	1002 ~	1003 ~
ENCRYPTION ALGORITHM	KEY DATA (CORRECT KEY DATA)	DECRYPTION RESULT (DECRYPTED COMMUNICATION DATA)
AES	0x**,0x**,0x** ... (16 CONSECUTIVE BYTES OF DATA)	username=XXXXXX&password=YYYYY&is:... ..
AES	0x**,0x**,0x** ... (32 CONSECUTIVE BYTES OF DATA)	...
...	...	...

Fig. 11

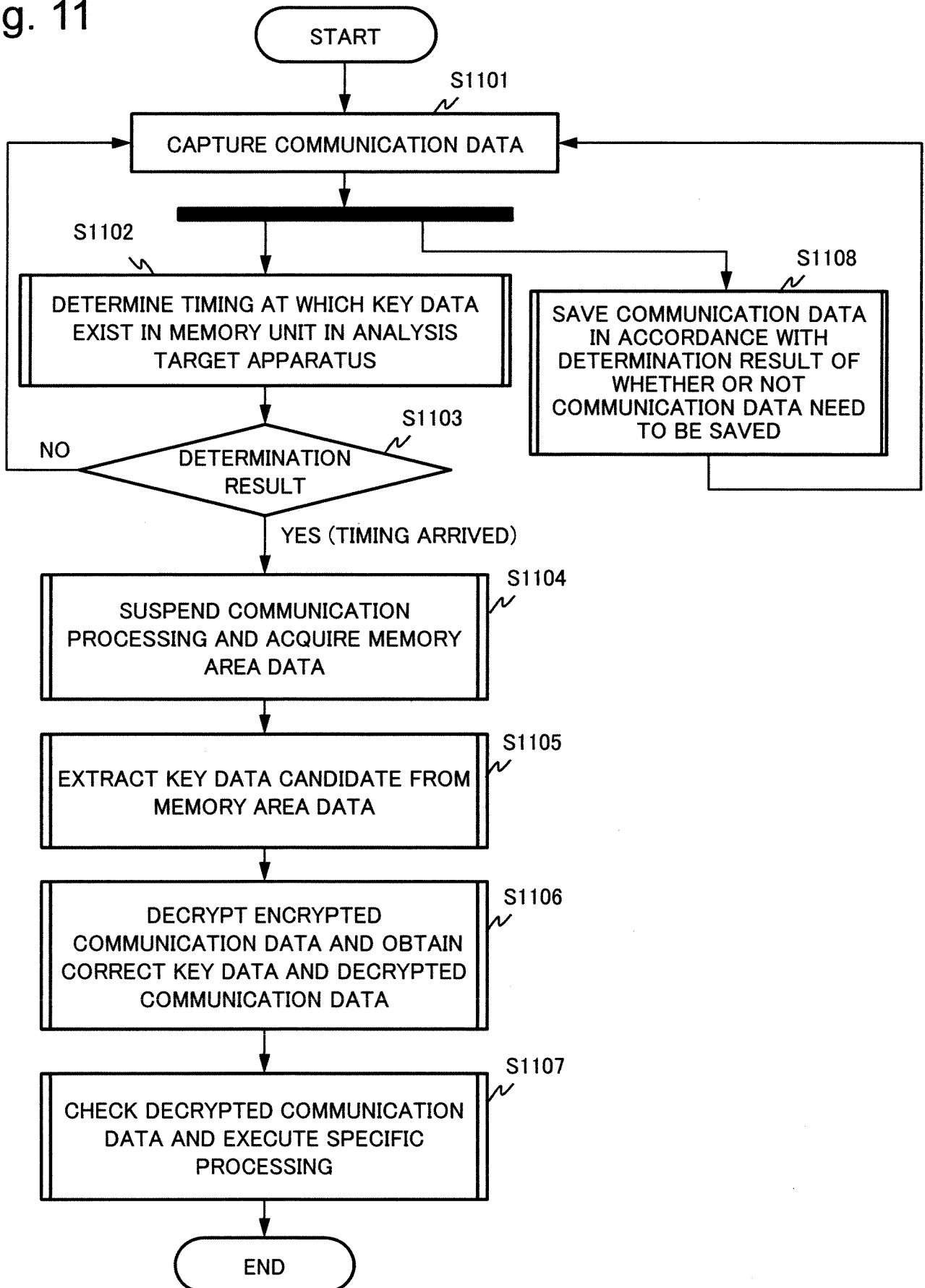


Fig. 12A

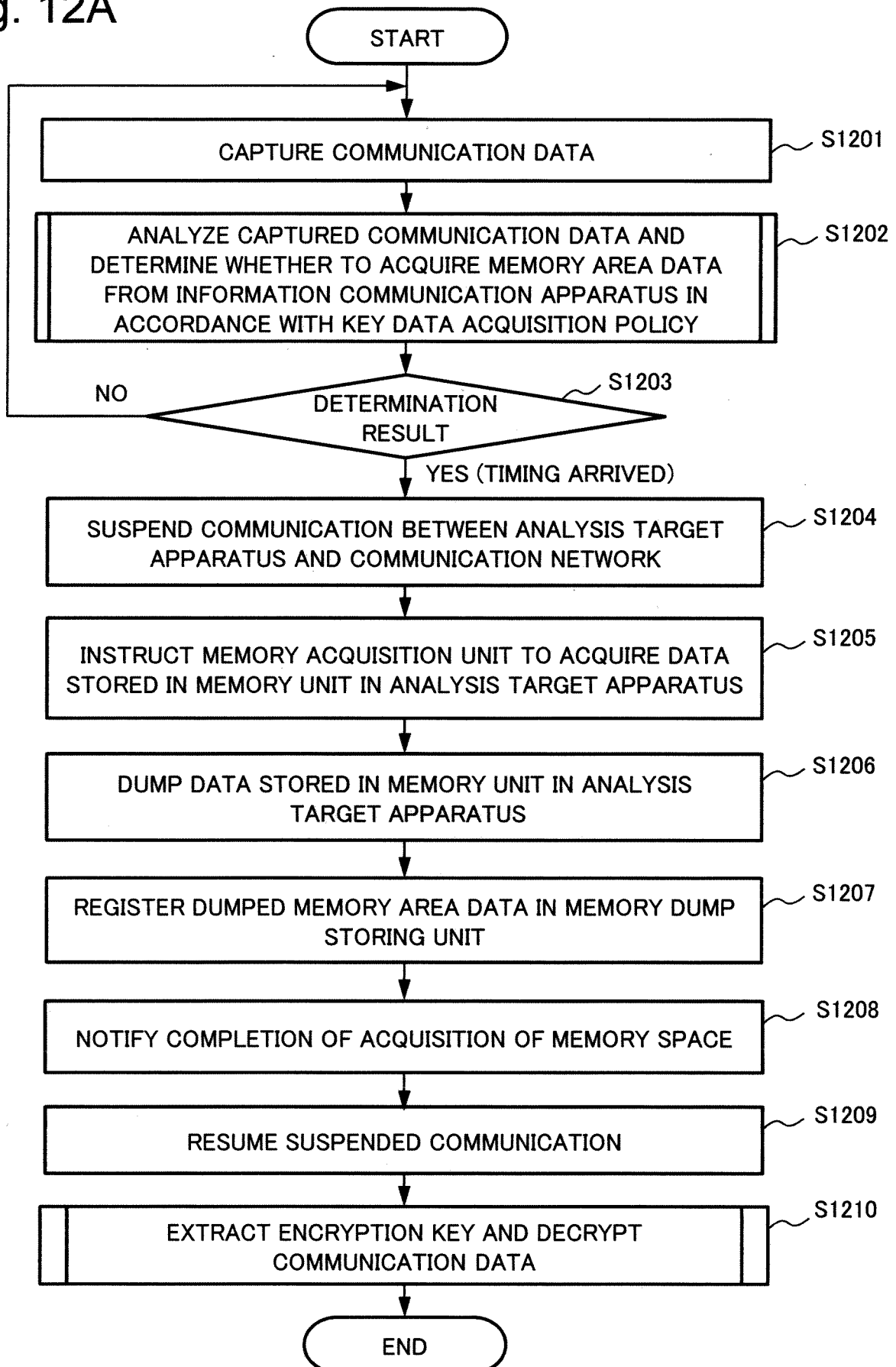


Fig. 12B

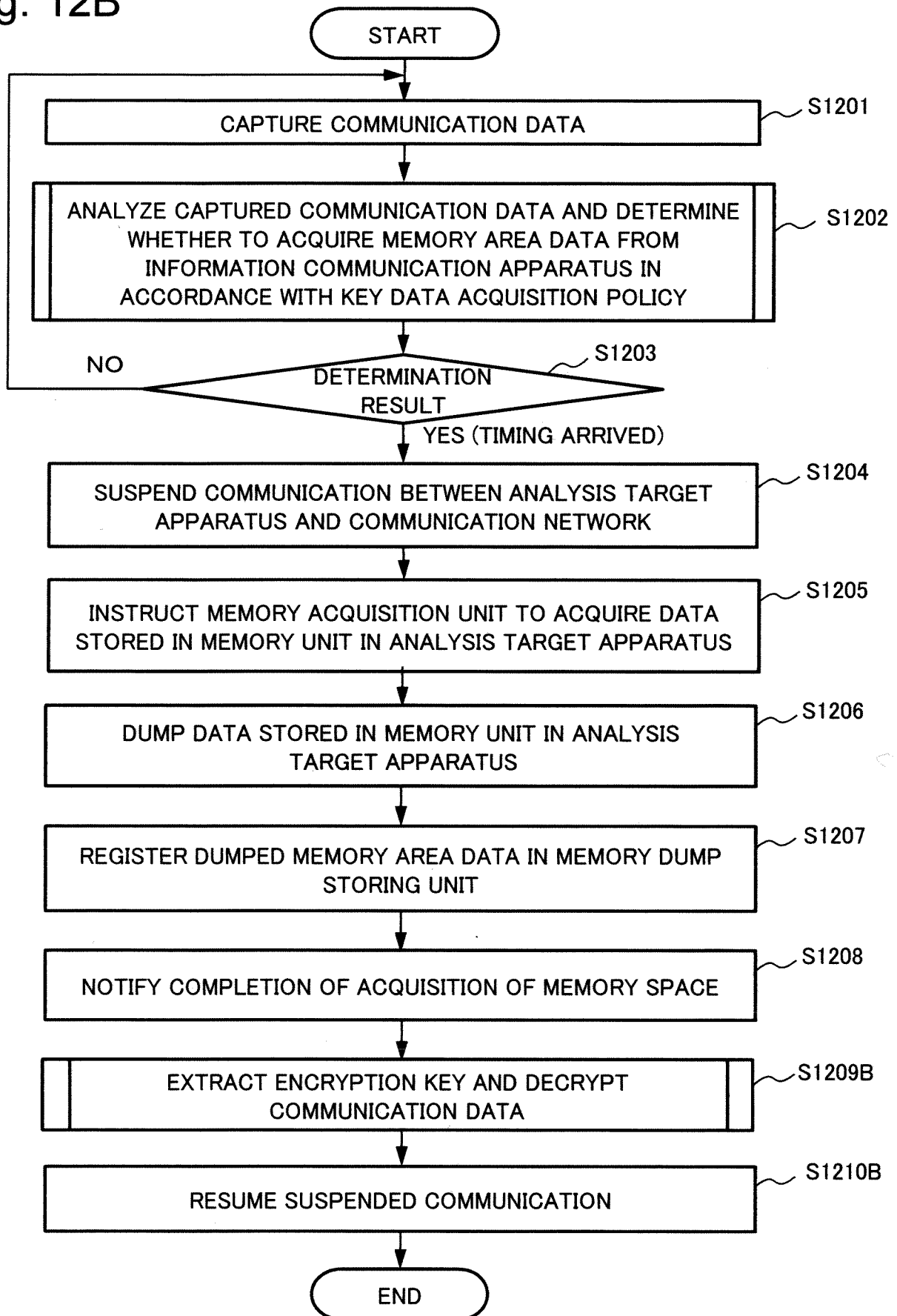


Fig. 13

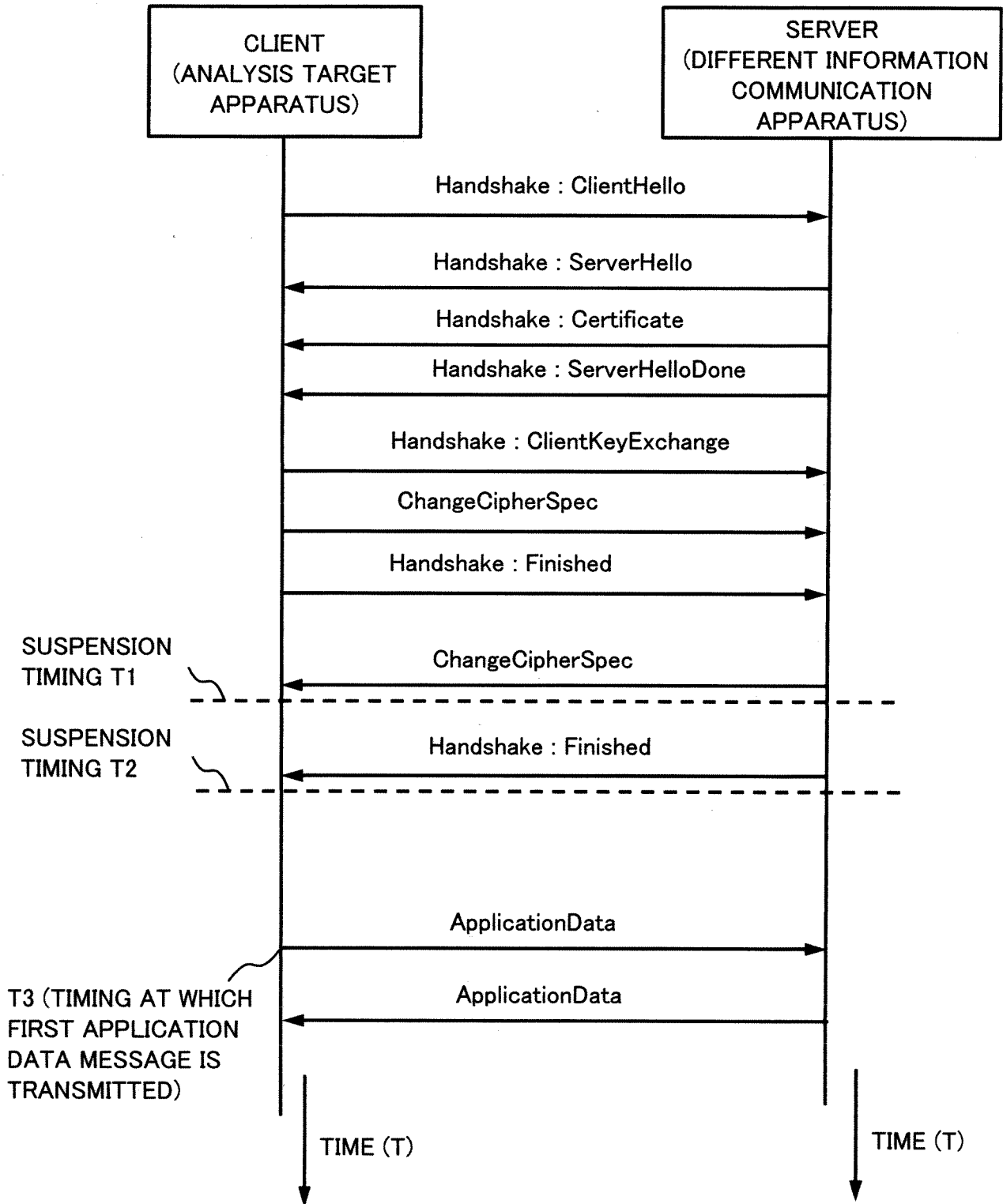


Fig. 14

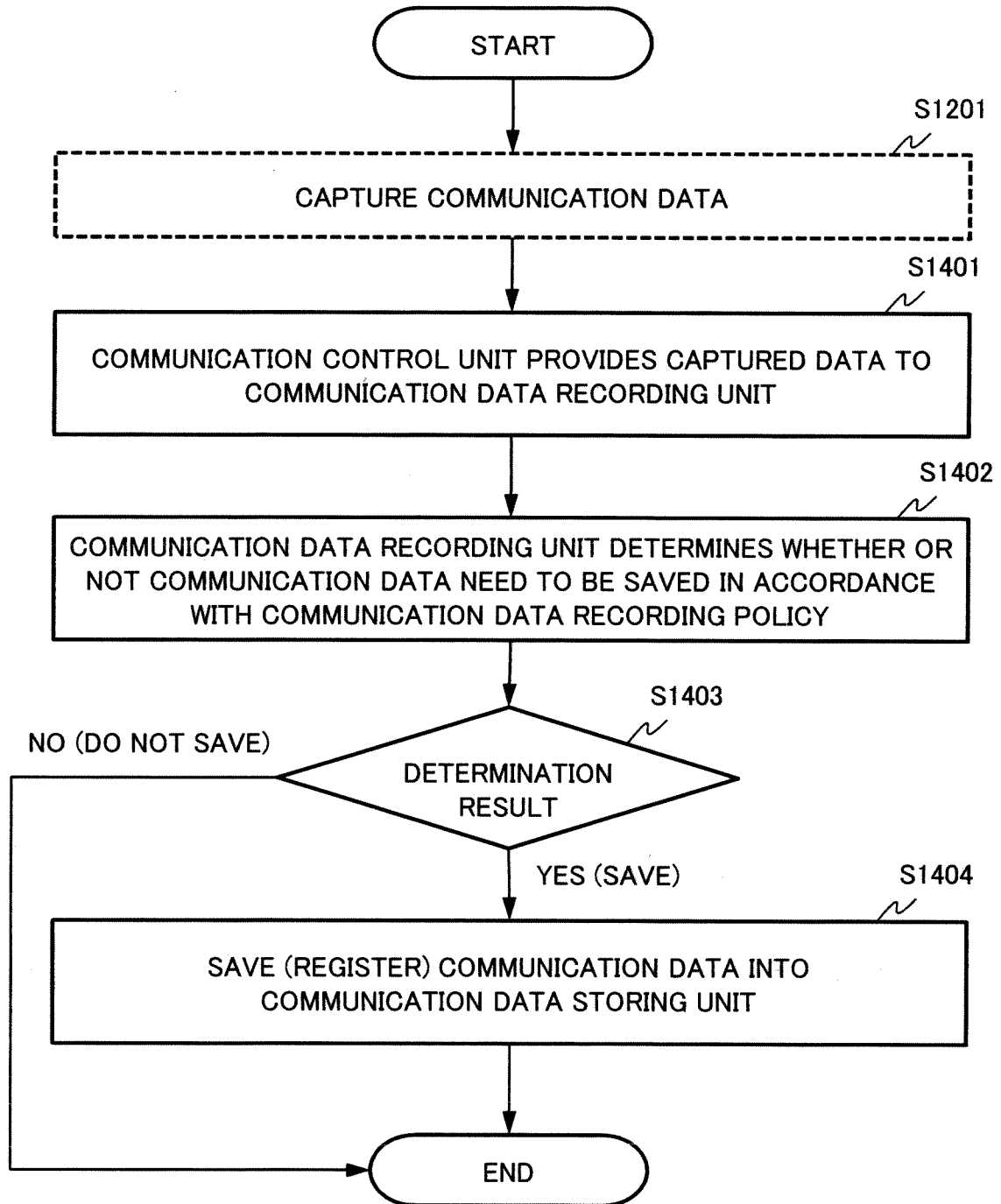


Fig. 15

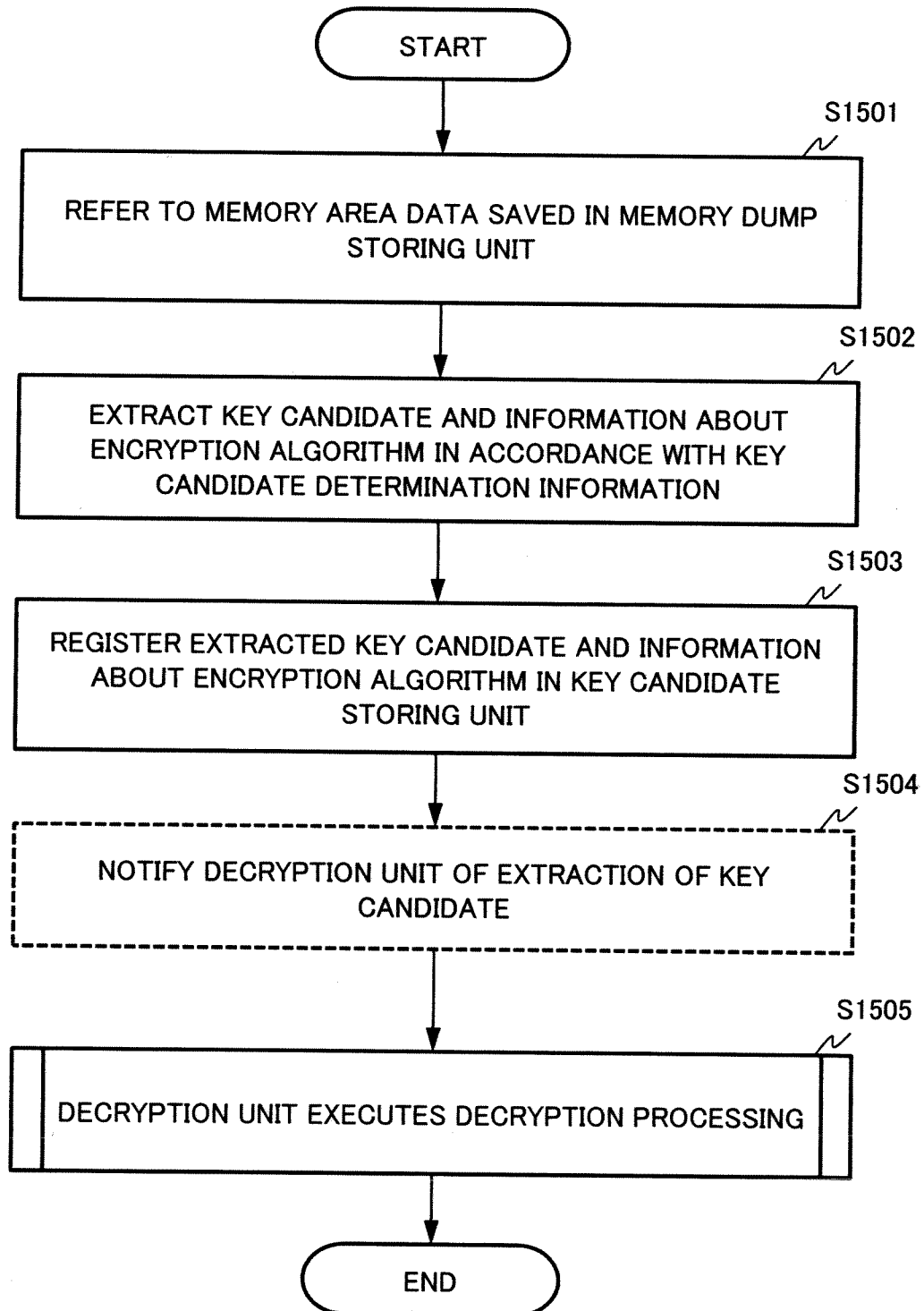


Fig. 16

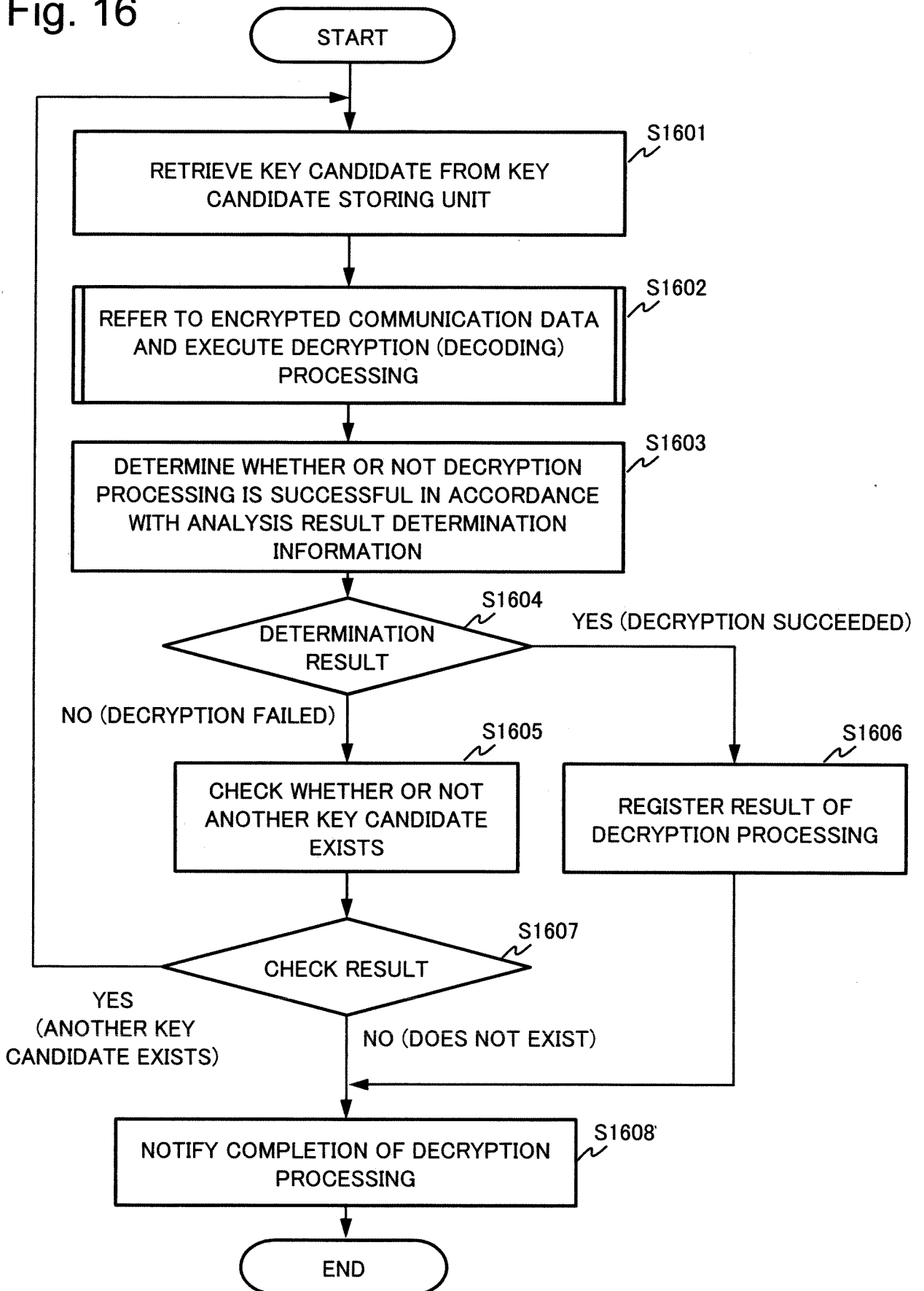


Fig. 17

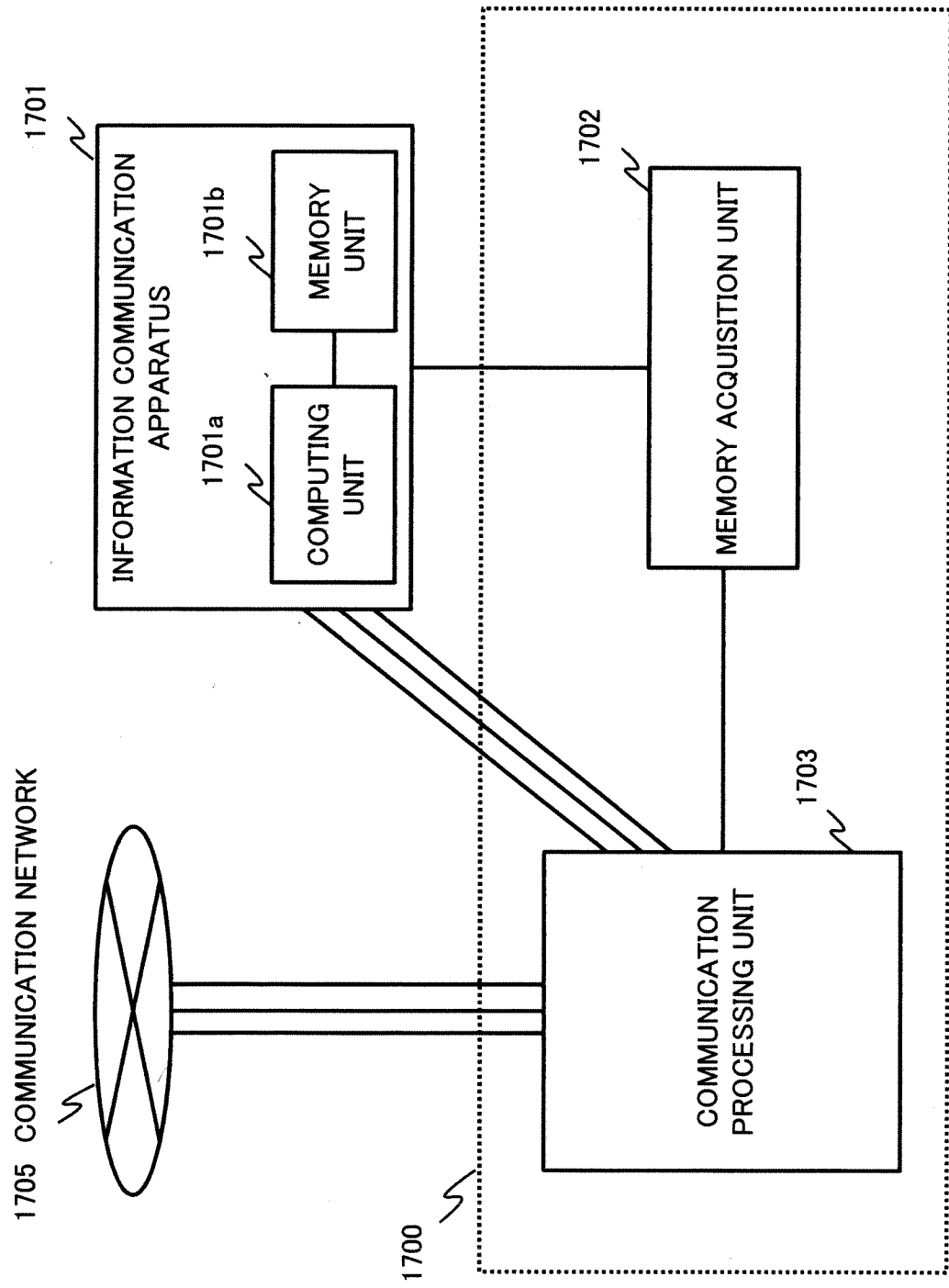


Fig. 18

