

Fig. 1

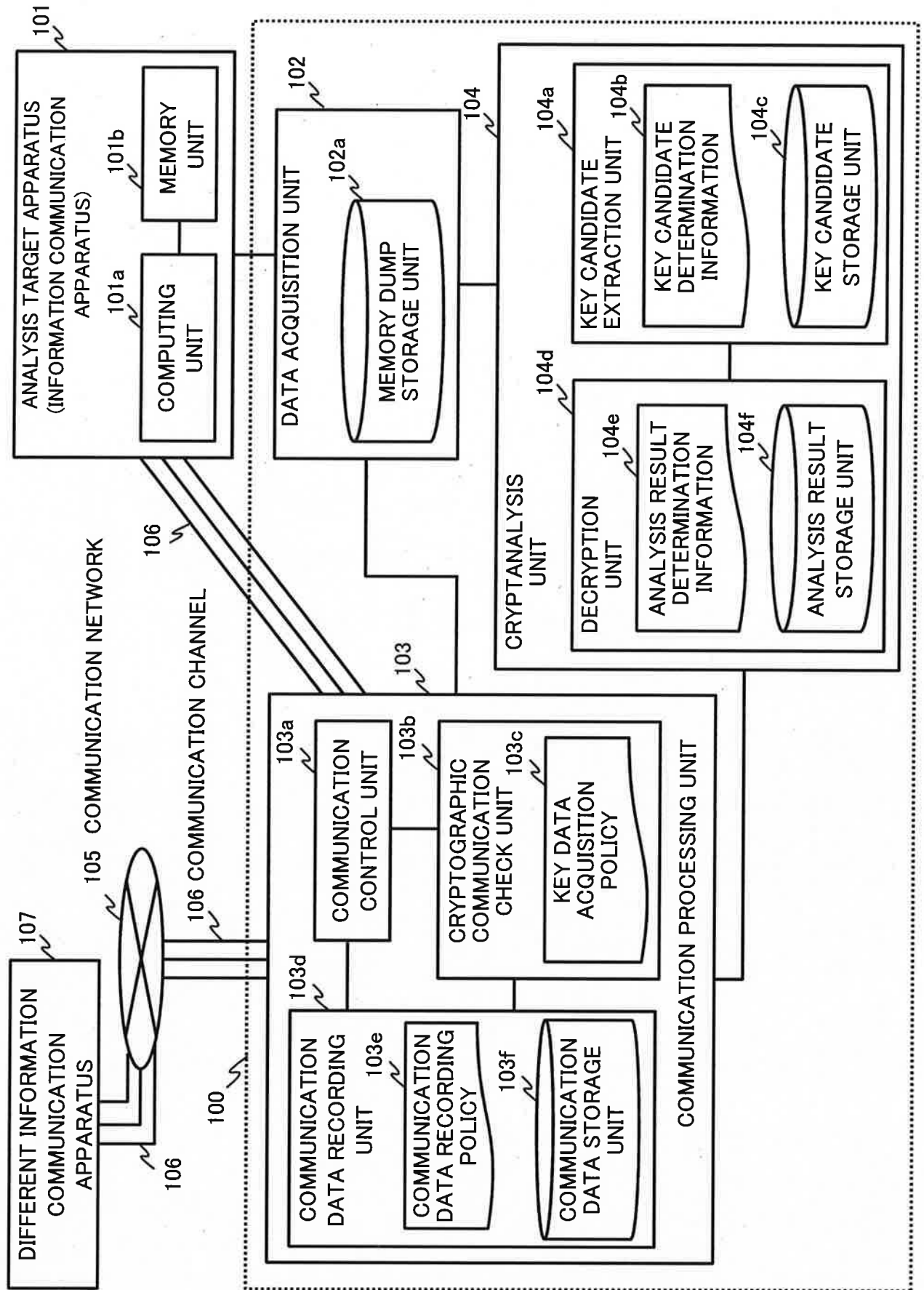


Fig. 2

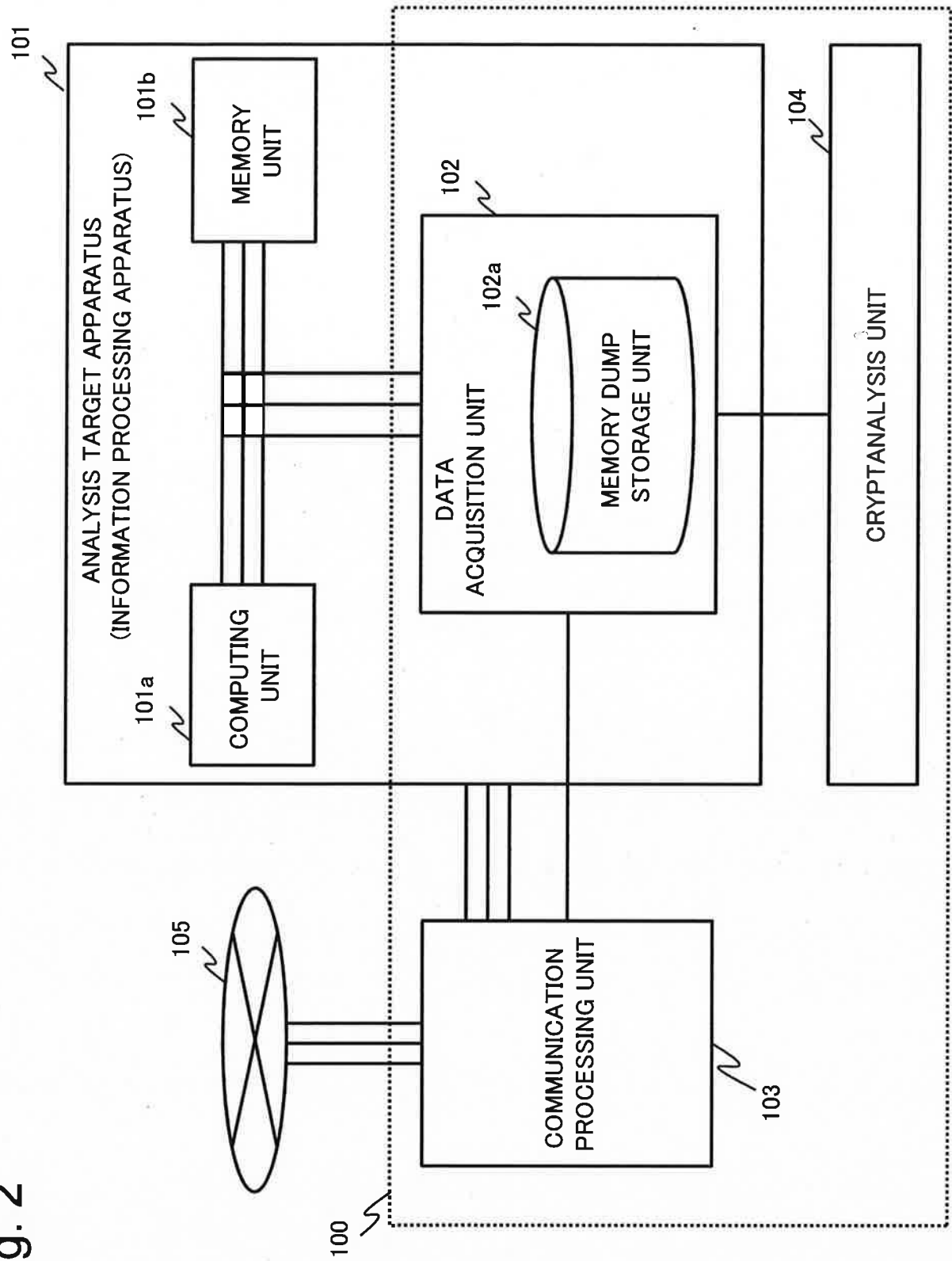


Fig. 3

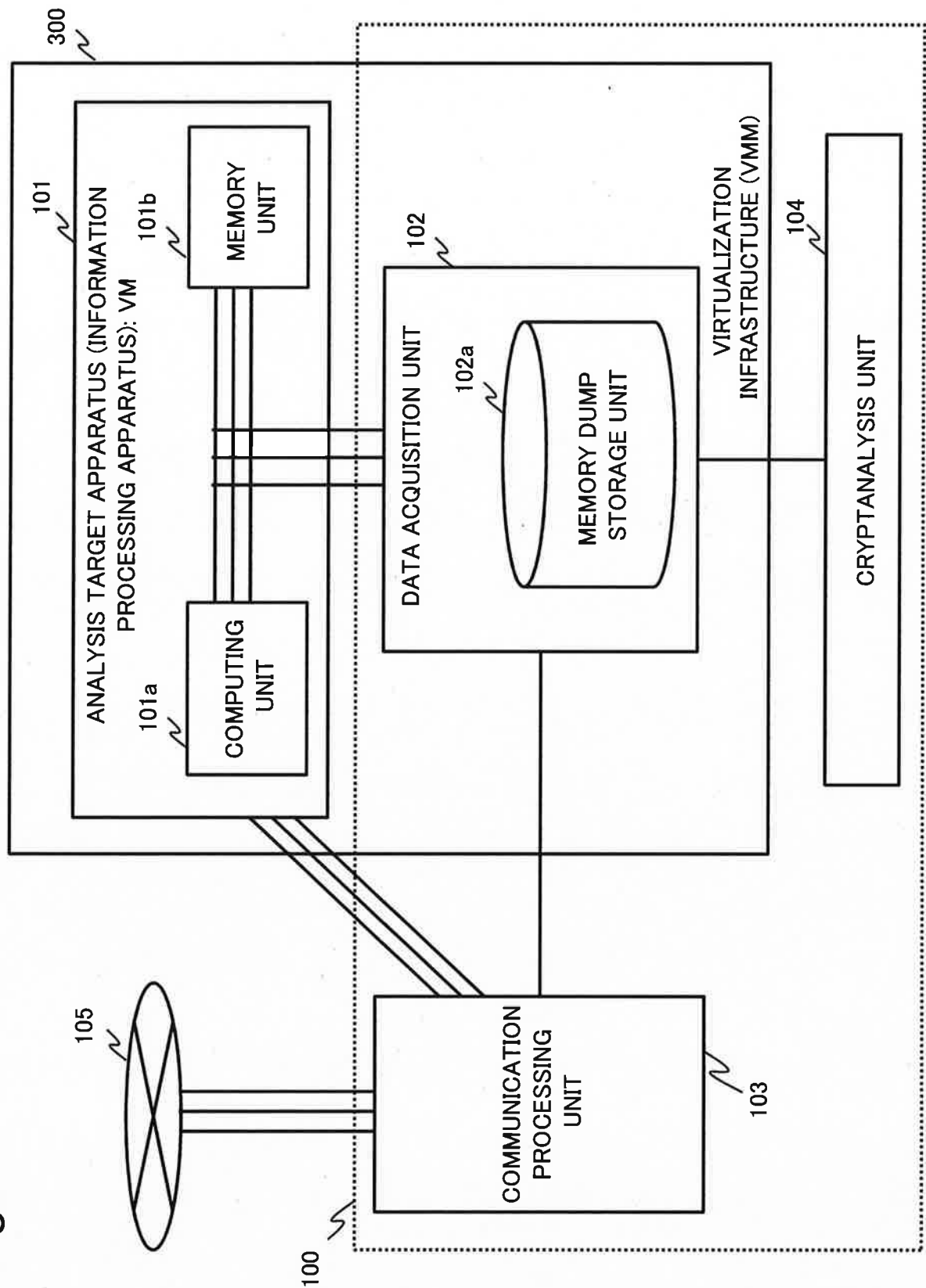


Fig. 4

103c

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

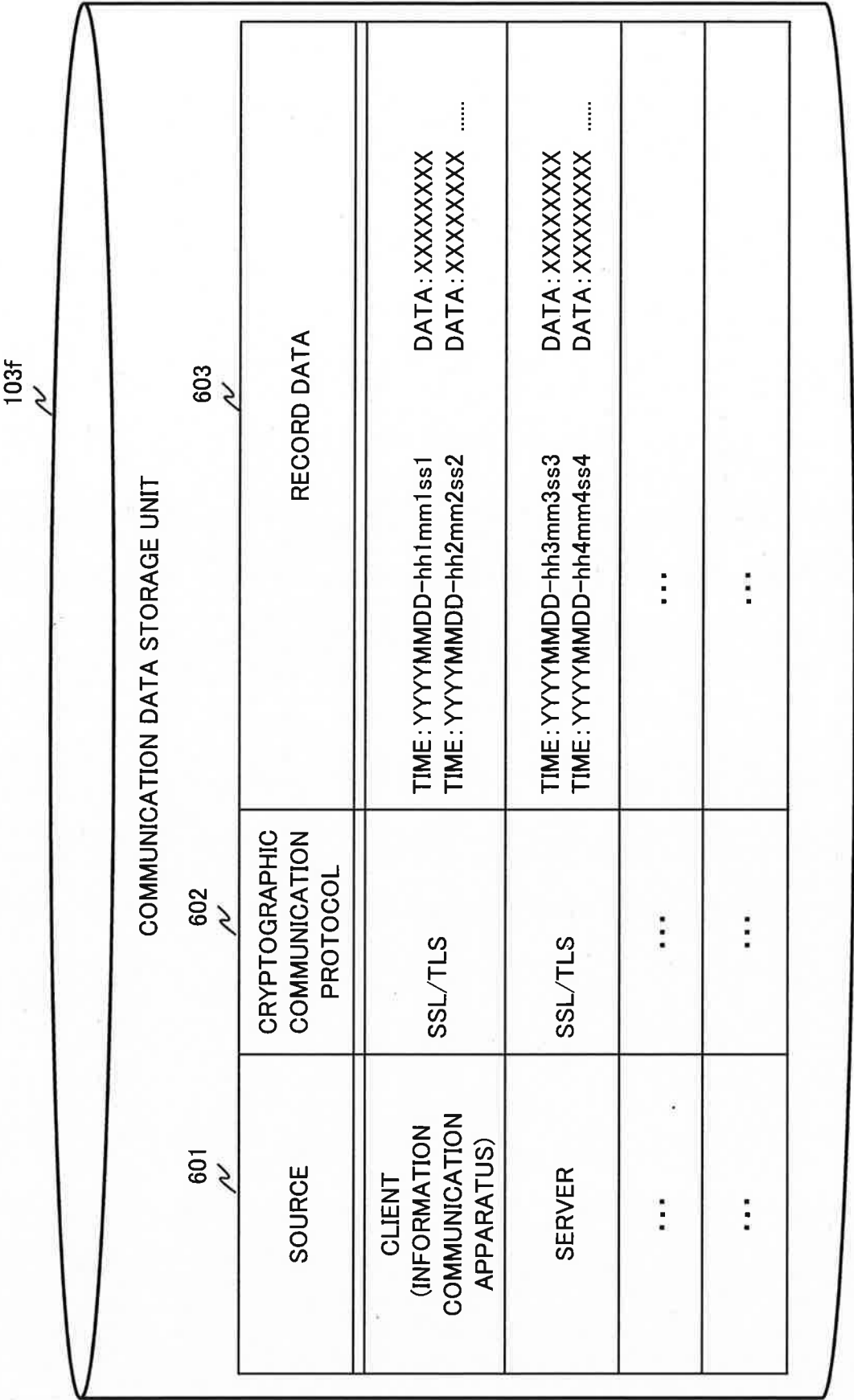


Fig. 7

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

104c

KEY CANDIDATE STORAGE UNIT			
801 ENCIPHERMENT ALGORITHM	802 ENCIPHERMENT PARAMETER		803 KEY DATA CANDIDATE
	KEY LENGTH (UNIT: BIT)	MODE	
AES	128	CBC	0x**,0x**,0x** ... (16 CONSECUTIVE BYTES OF DATA)
AES	256	CBC	0x**,0x**,0x** ... (32 CONSECUTIVE BYTES OF DATA)
AES	128	GCM	0x30,0x02,0x00,0x00,0x4b,0x53,0x53,0x4D ... (560 CONSECUTIVE BYTES OF DATA)
...	...	...	...

Fig. 9

104e 901 ANALYSIS RESULT DETERMINATION INFORMATION	902 <table> <tr> <th data-bbox="534 336 667 1003">ANALYSIS RESULT DETERMINATION CRITERION</th><th data-bbox="534 1003 667 1919">DETERMINATION RESULT</th></tr> <tr> <td data-bbox="667 336 805 1003">(ENTROPY OF DECODING PROCESSING RESULT) $\leq$ (SPECIFIC REFERENCE VALUE)</td><td data-bbox="667 1003 805 1919">DECRYPTION SUCCEEDED</td></tr> <tr> <td data-bbox="805 336 928 1003">(ENTROPY OF DECODING PROCESSING RESULT) $>$ (SPECIFIC REFERENCE VALUE)</td><td data-bbox="805 1003 928 1919">DECRYPTION FAILED</td></tr> <tr> <td data-bbox="928 336 1093 1003">(FIRST 4 BYTES OF PAYLOAD INCLUDED IN DECODING PROCESSING RESULT ARE "GET")</td><td data-bbox="928 1003 1093 1919">DECRYPTION SUCCEEDED</td></tr> <tr> <td data-bbox="1093 336 1216 1003">...</td><td data-bbox="1093 1003 1216 1919">...</td></tr> </table>	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	...	...
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

ANALYSIS RESULT STORAGE 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

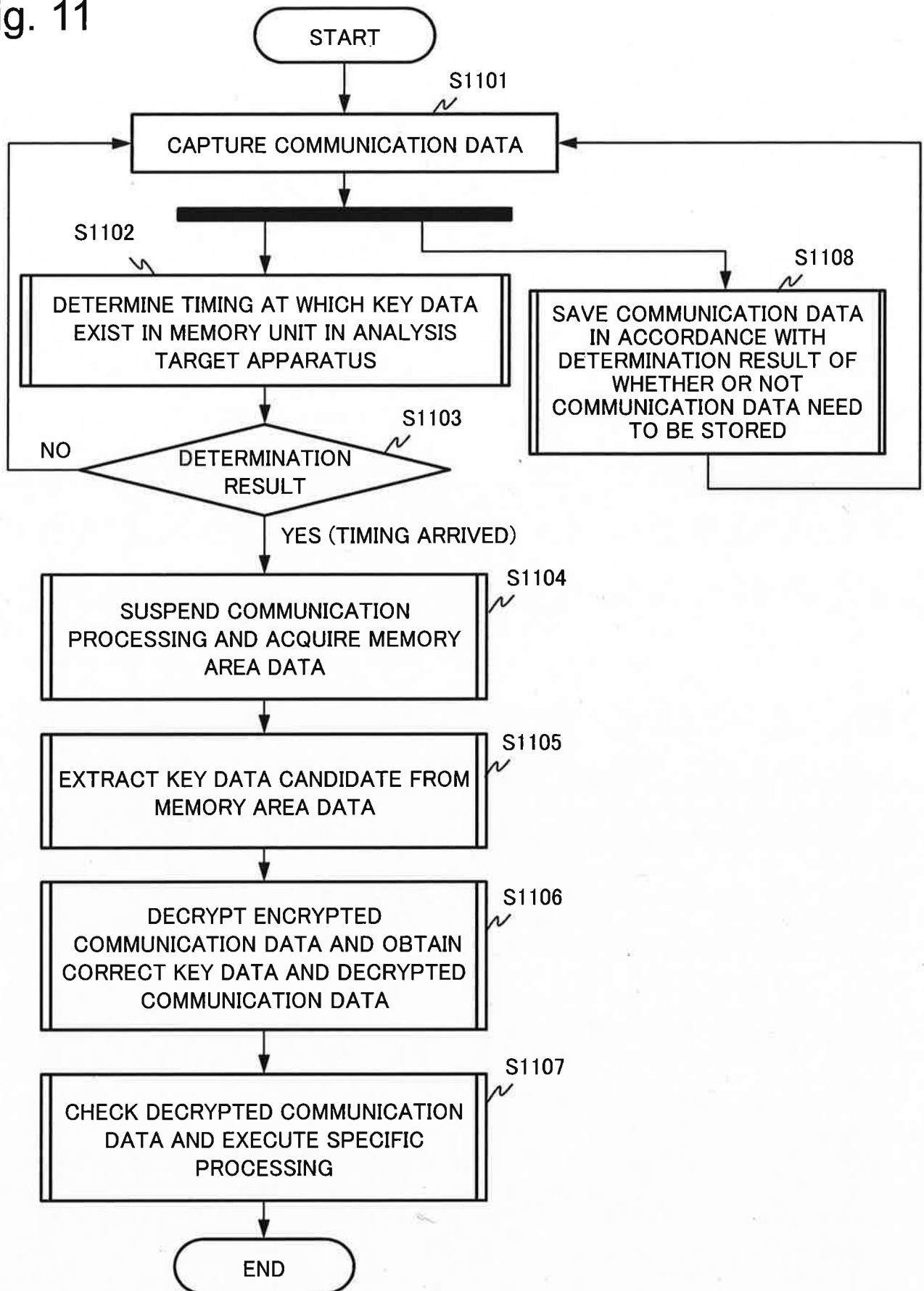


Fig. 12A

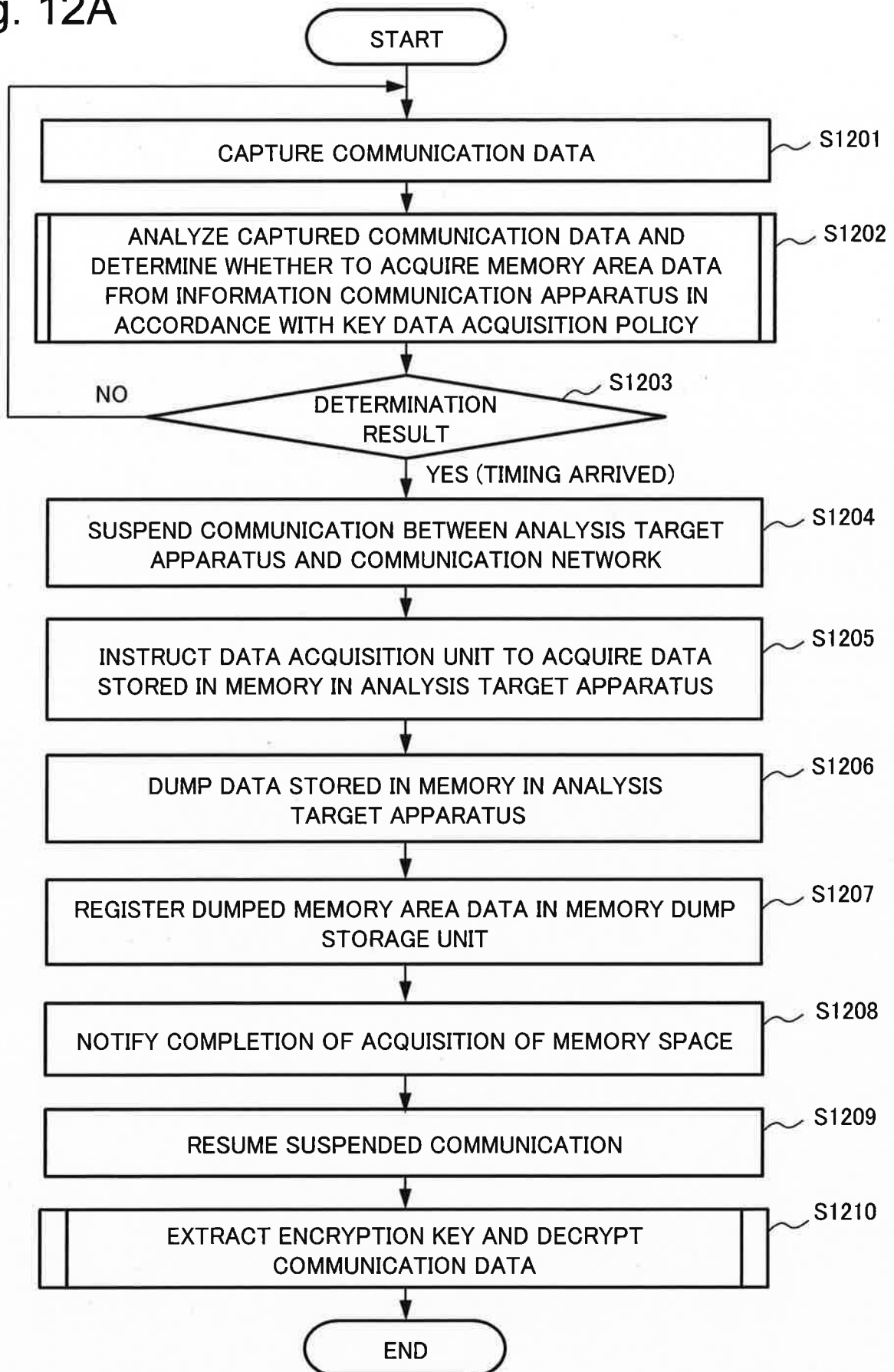


Fig. 12B

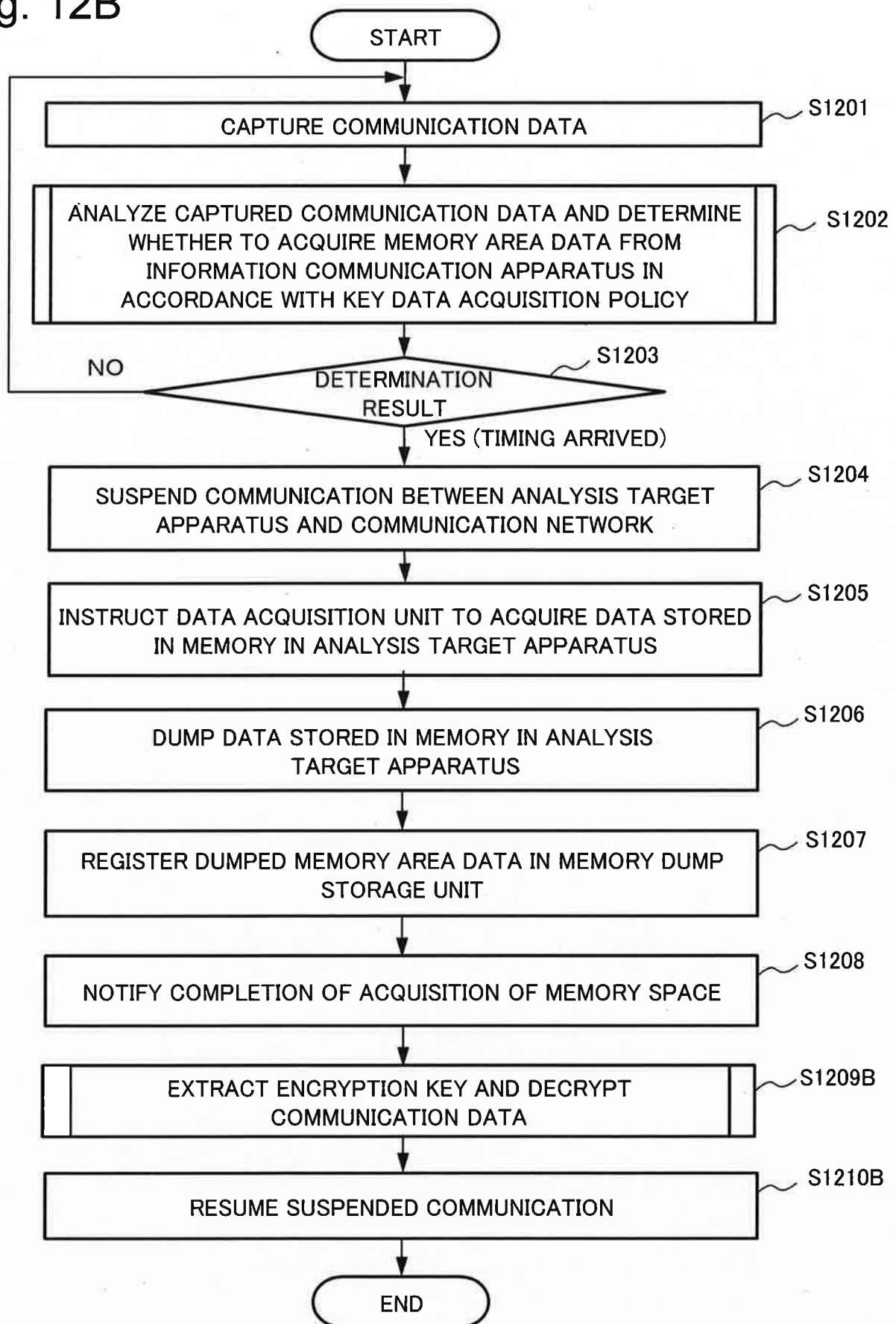


Fig. 13

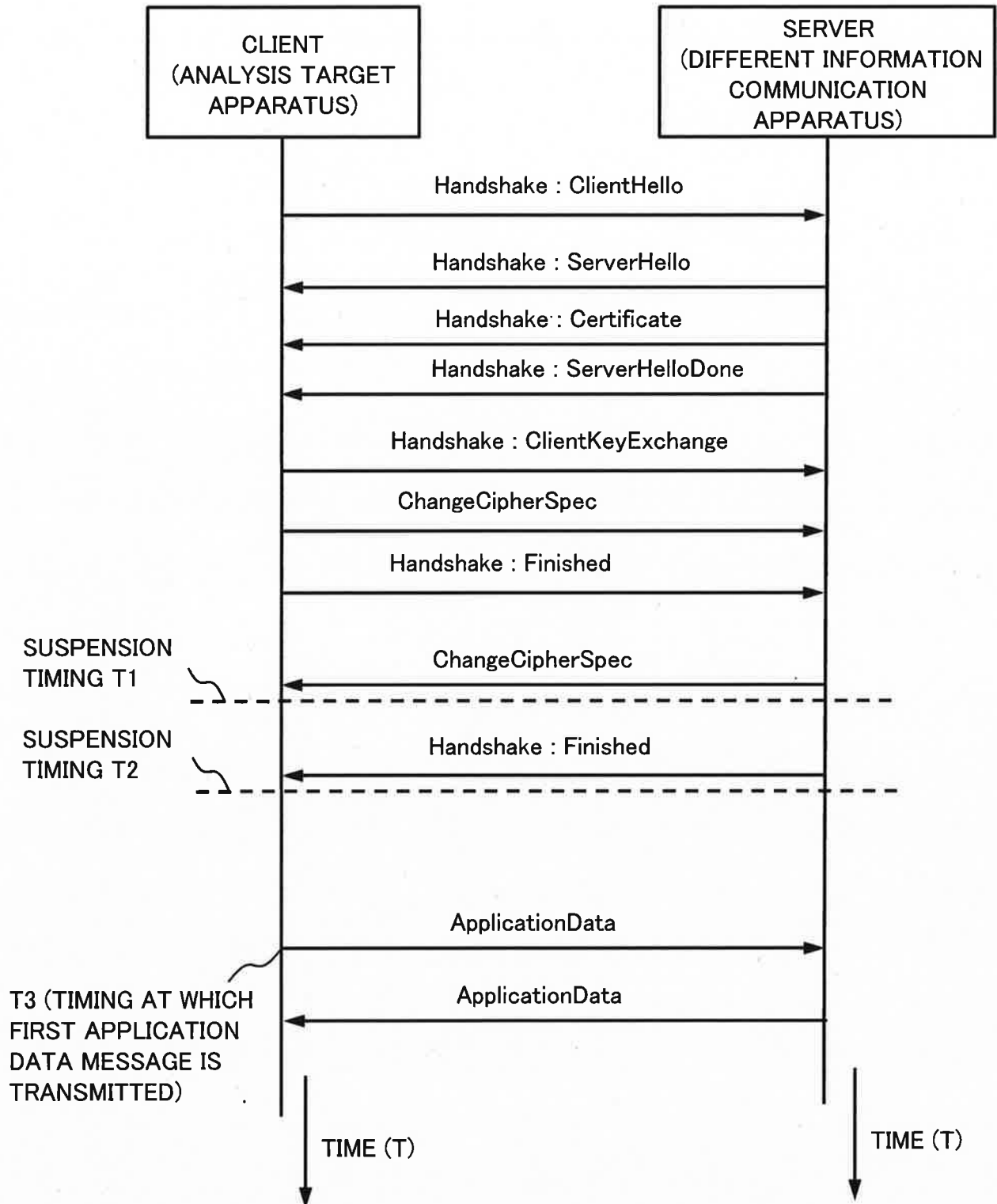


Fig. 14

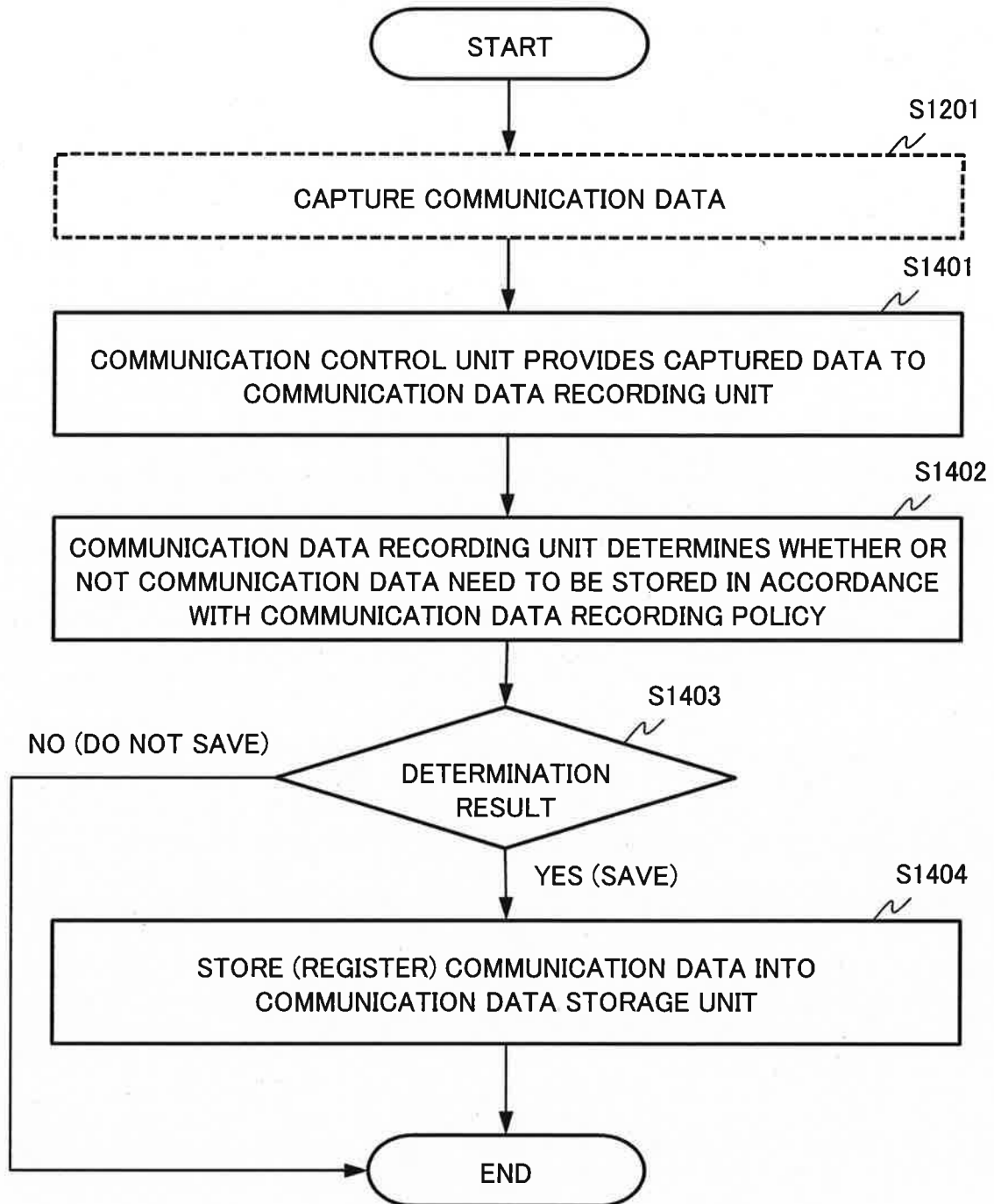


Fig. 15

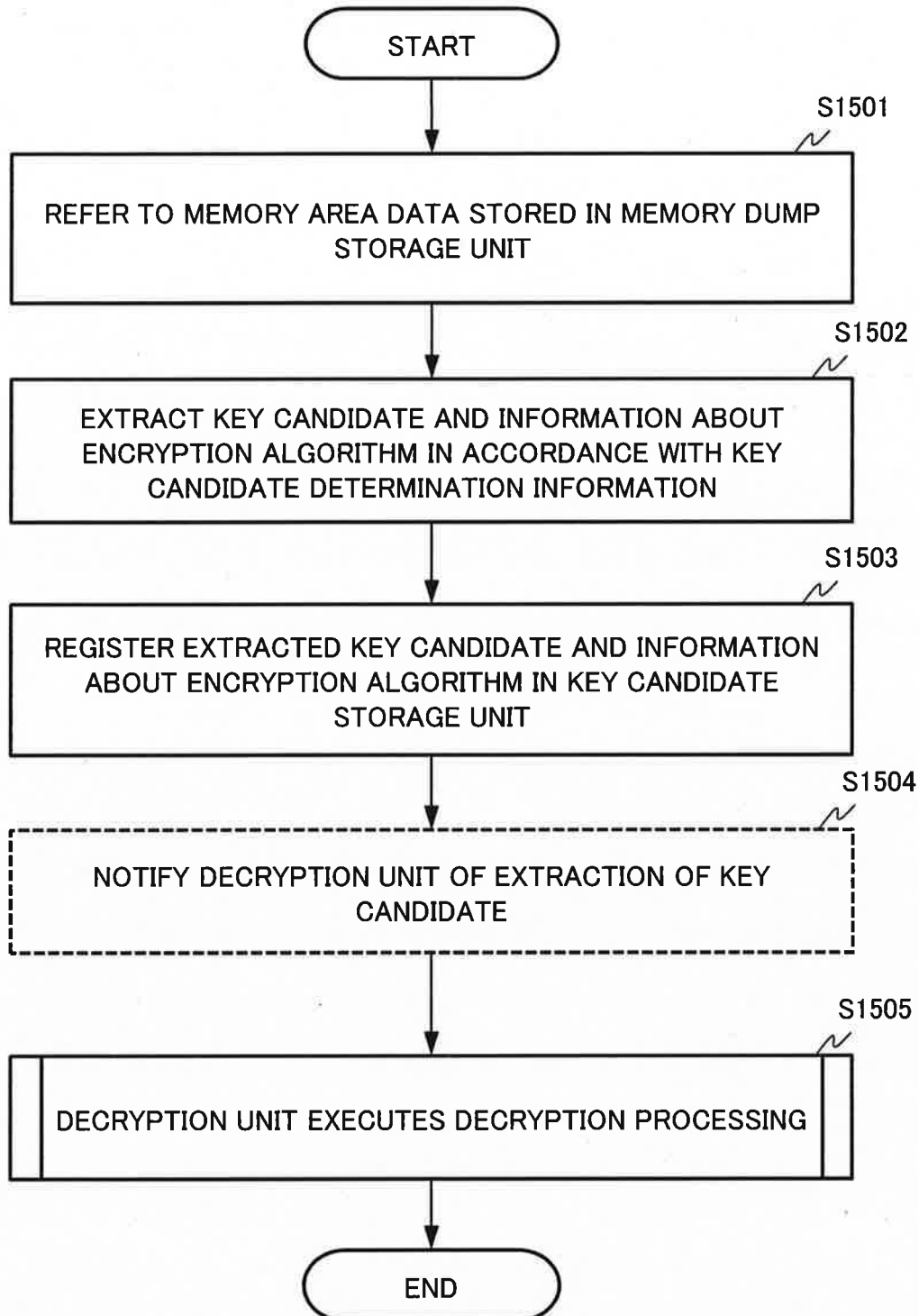


Fig. 16

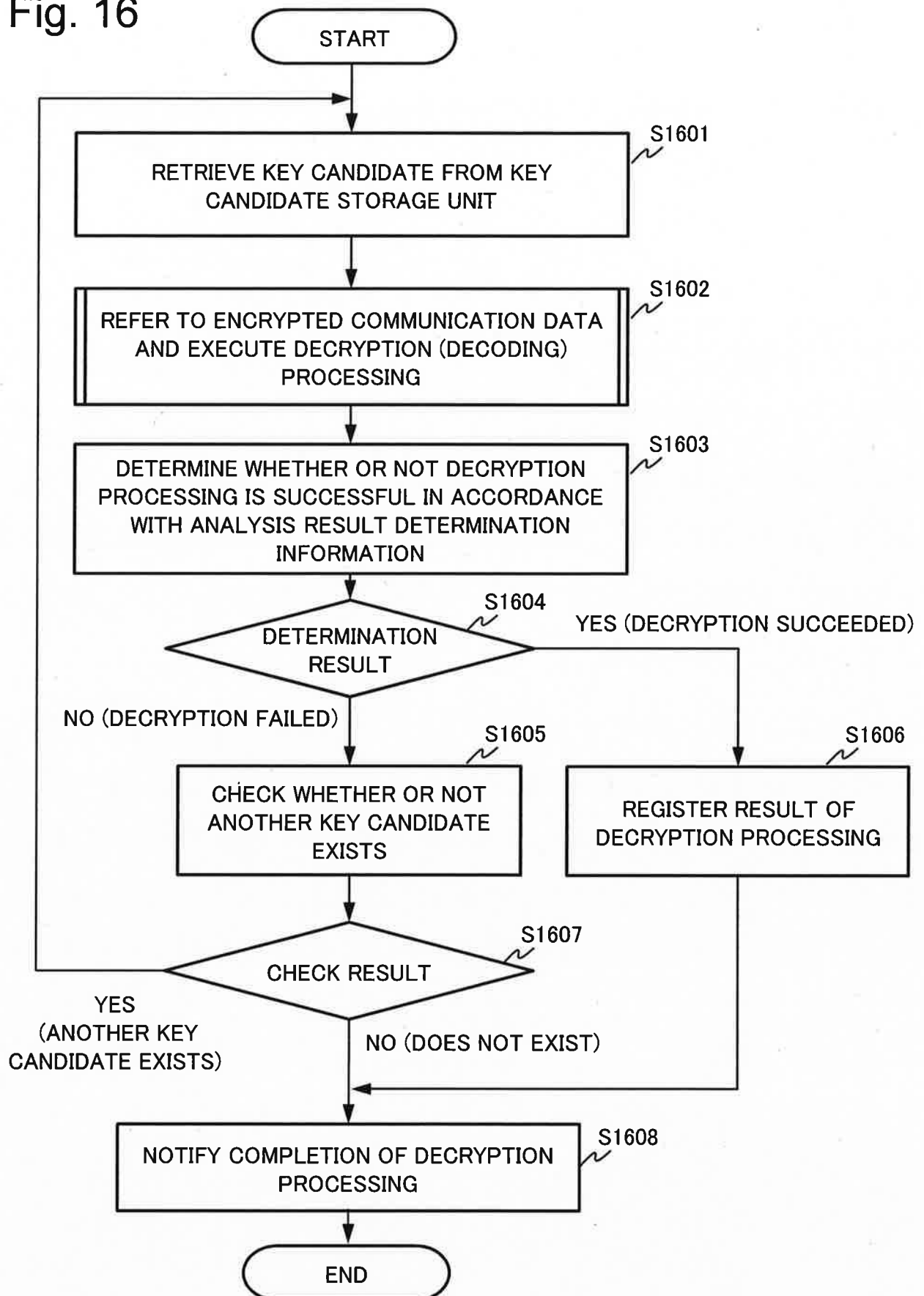


Fig. 17

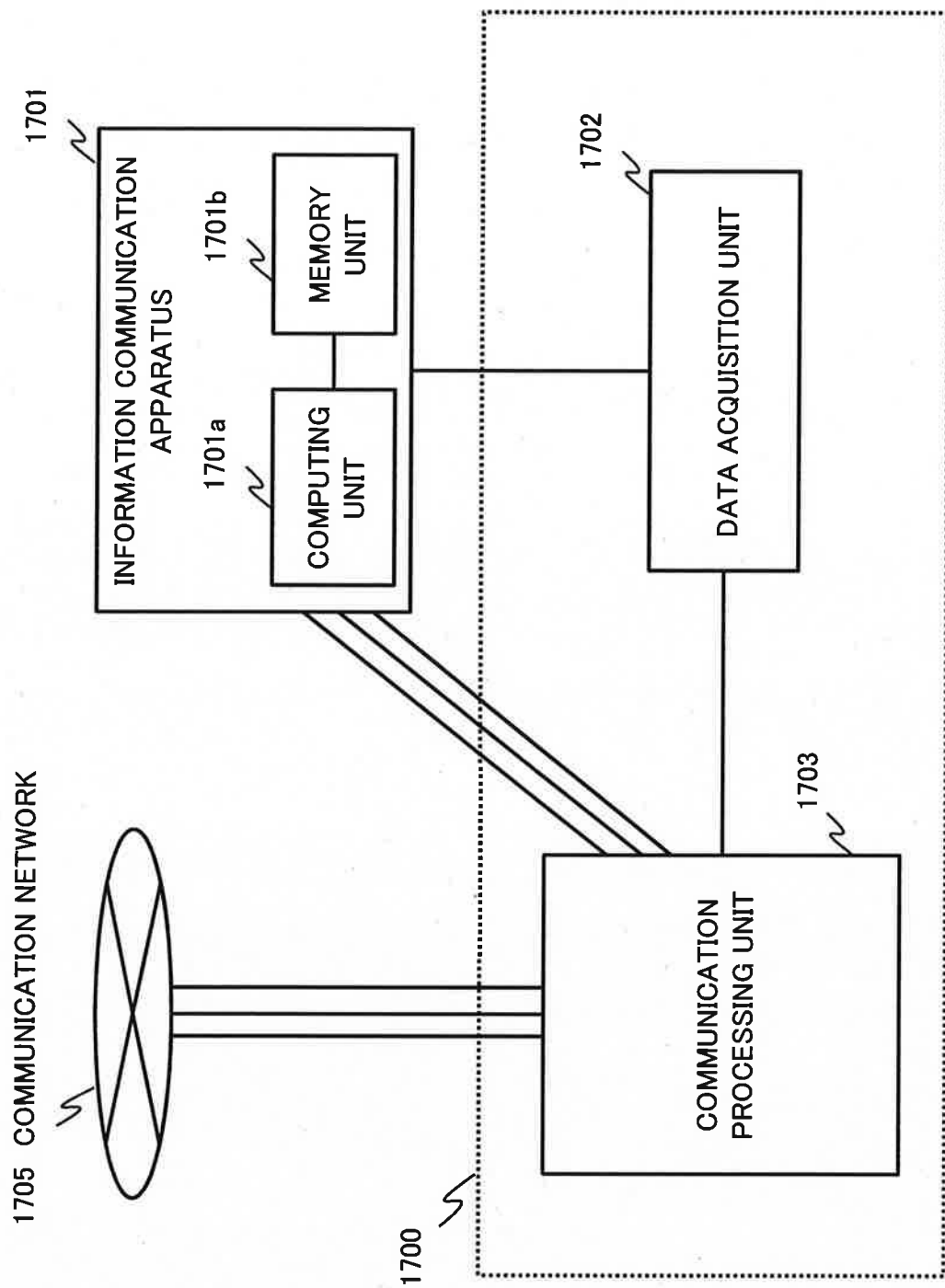


Fig. 18

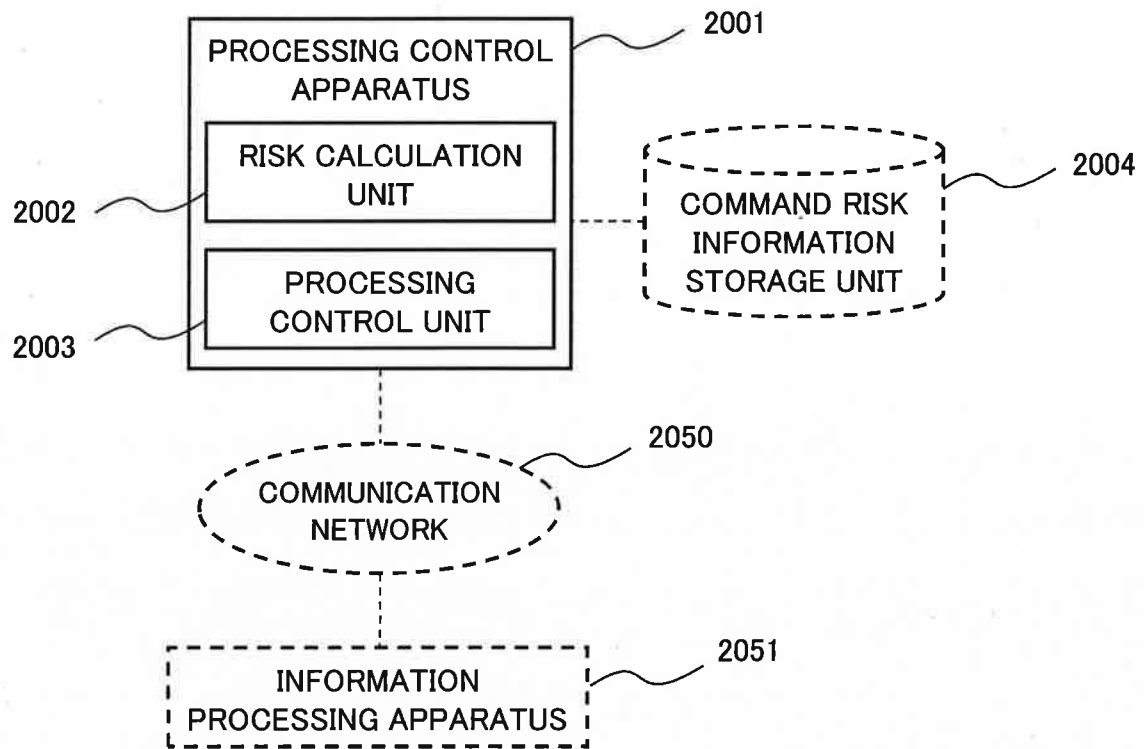


Fig. 19

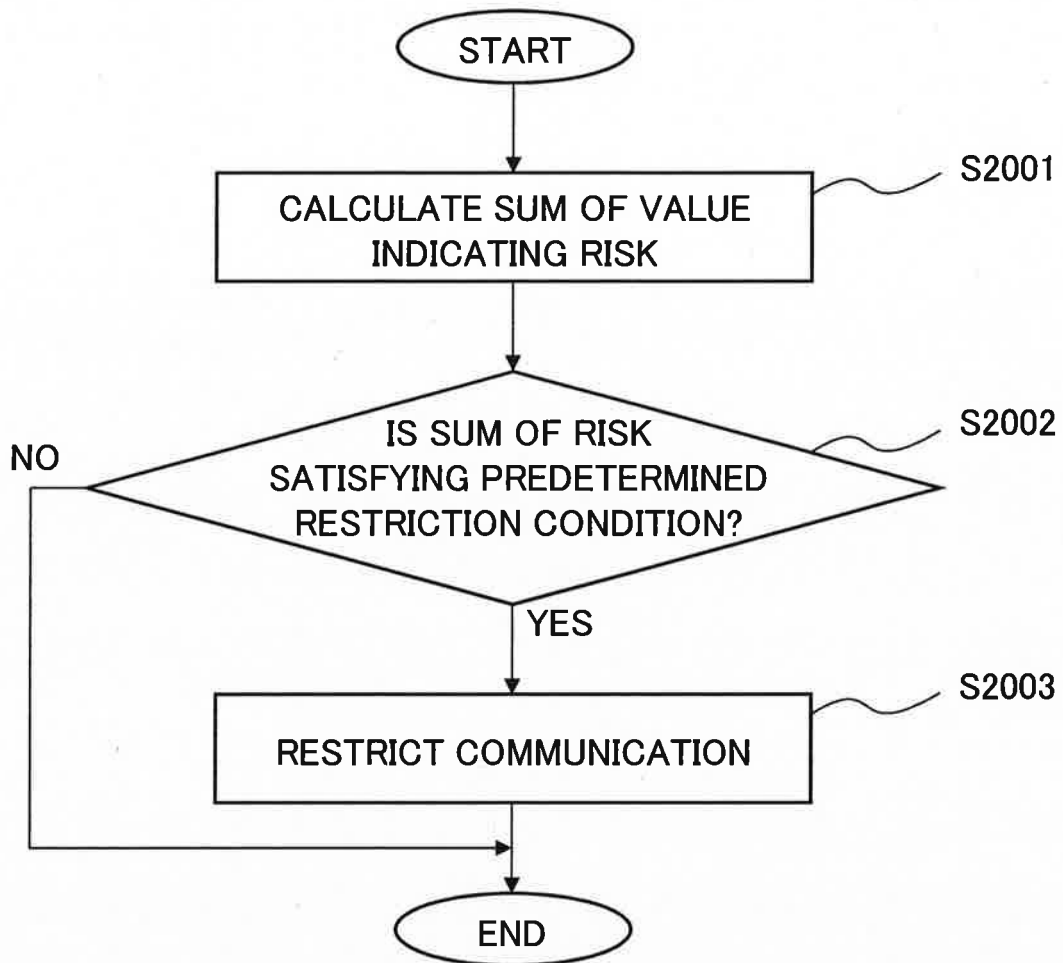


Fig. 20

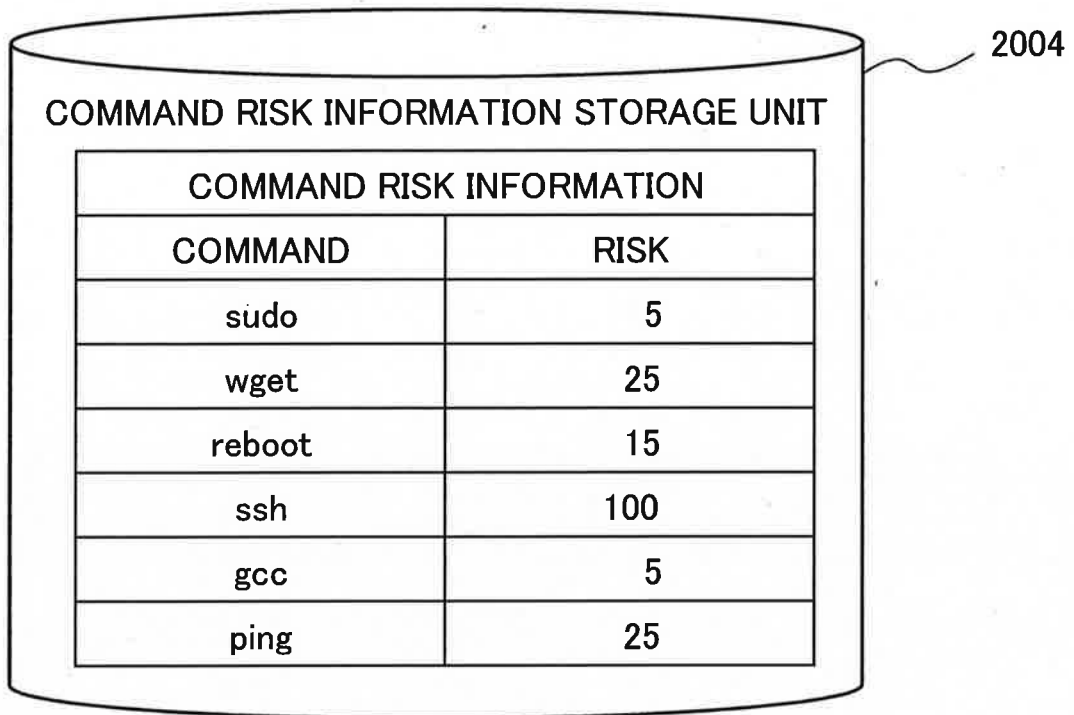


Fig. 21

PROCESSING INFORMATION		
COMMAND	OPTION	ARGUMENT
sudo	-s	
ping		A.B.C.D
wget		A.B.C.D/File.bin
ssh		test@A.B.C.D

Fig. 22

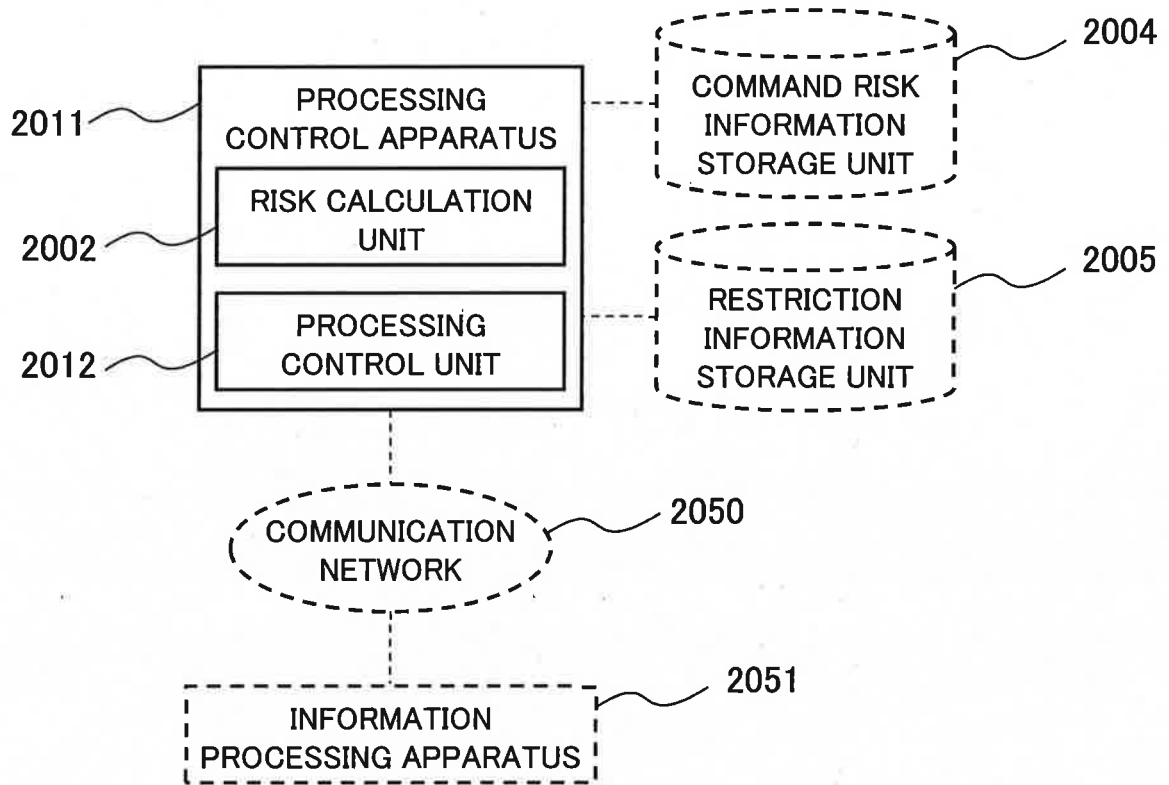


Fig. 23

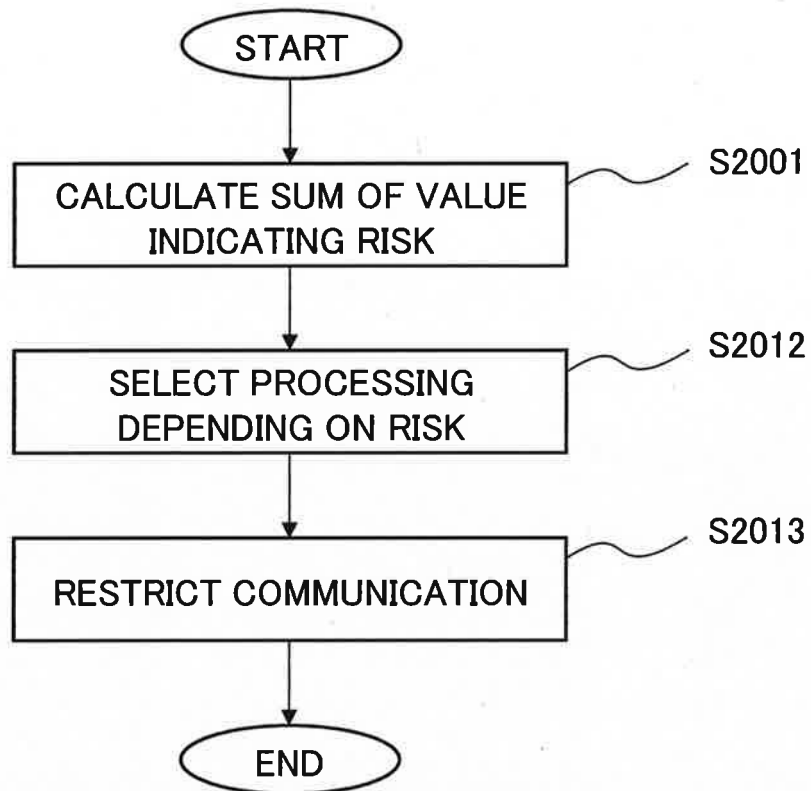


Fig. 24

2005

RESTRICTION INFORMATION STORAGE UNIT	
RESTRICTION INFORMATION	
CRITERIA	PROCESSING CONTENT
$0 \leq \text{RISK} < 50$	
$50 \leq \text{RISK} < 75$	RESTRICT COMMUNICATION BANDWIDTH
$75 \leq \text{RISK} < 100$	RESTRICT ALLOCATION RESOURCE
$100 \leq \text{RISK} < 200$	OBSTRUCT COMMUNICATION
$200 \leq \text{RISK}$	SHUTDOWN

Fig. 25

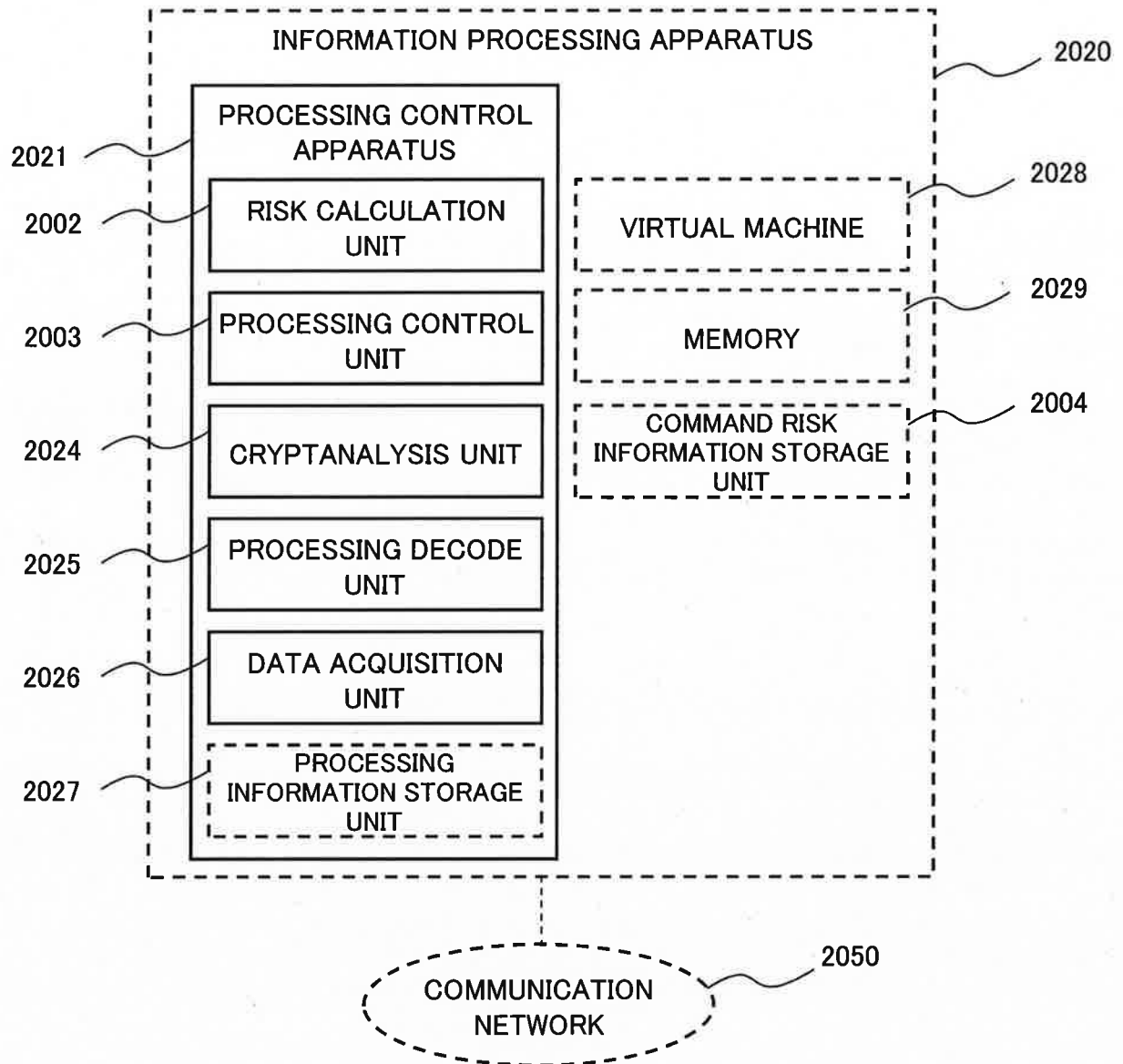


Fig. 26

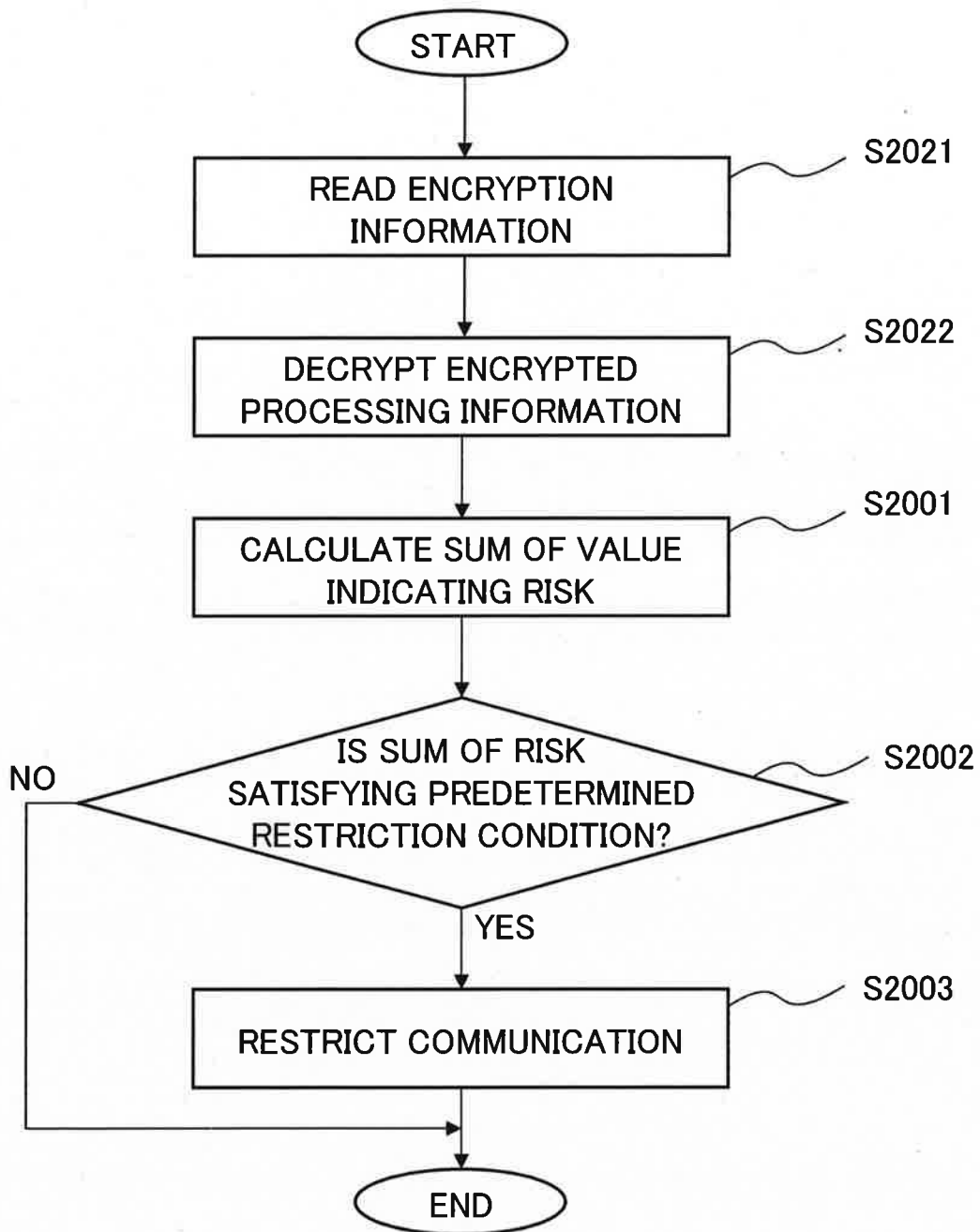


Fig. 27

