ABSTRACT

"COMMUNICATION SYSTEM, COMMUNICATION APPARATUS, COMMUNICATION METHOD AND COMPUTER PROGRAM"

A source apparatus and a conditional access apparatus are disclosed. The source apparatus may transmit a command to the conditional access apparatus. The conditional access apparatus may transmit a response to the command to the source apparatus. When a time elapsed between transmission of the command by the source apparatus and reception of the response by the source apparatus does not exceed a predetermined round trip time (RTT), a first authorization signal to permit the conditional access apparatus to decrypt encrypted content may be generated. Additionally, whenever a non-RTT condition is met, a second authorization signal to permit the conditional access apparatus to decrypt the content may be generated.

We claim:

1. A conditional access apparatus for selectively generating a signal to permit decryption of encrypted content, the conditional access apparatus comprising:

a first authorization section configured to:

receive a command transmitted by a source apparatus;

transmit to the source apparatus a response to the command; and

generate a first authorization signal to permit decryption of the content, the first authorization signal being generated upon receipt of an indication signal indicating that a time elapsed between transmission of the command by the source apparatus and reception of the response by the source apparatus does not exceed a predetermined round trip time (RTT); and

a second authorization section configured to generate a second authorization signal to permit decryption of the content, the second authorization signal being generated whenever a non-RTT condition is met.

2. The conditional access apparatus of claim 1, further comprising a registration section configured to transmit a request to register the conditional access apparatus with the source apparatus.

3. The conditional access apparatus of claim 2, wherein the registration section is configured to:

receive a second command transmitted by the source apparatus; and

transmit to the source apparatus a second response to the second command.

4. The conditional access apparatus of claim 1, wherein at least one of the first and the second authorization signals includes a content key for decrypting the content.

5. The conditional access apparatus of claim 4, wherein at least one of the first and the second authorization sections is configured to generate the content key based on an exchange key.

6. The conditional access apparatus of claim 5, wherein the first authorization section is configured to generate the content key based on a nonce if:

the first authorization section receives the indication signal from the source apparatus; and

the received indication signal includes the nonce.

7. The conditional access apparatus of claim 1, wherein the predetermined RTT is 7 milliseconds.

8. A source apparatus for selectively generating a signal to permit a conditional access apparatus to decrypt encrypted content, the source apparatus comprising:

a first authorization section configured to:

transmit a command to the conditional access apparatus;

receive from the conditional access apparatus a response to the command; and

generate a first authorization signal to permit the conditional access apparatus to decrypt the content, the first authorization signal being generated when a time elapsed between transmission of the command and reception of the response does not exceed a predetermined round trip time (RTT); and

a second authorization section configured to generate a second authorization signal to permit the conditional access apparatus to decrypt the content, the second authorization signal being generated whenever a non-RTT condition is met.

9. The source apparatus of claim 8, further comprising a registration section configured to register at least one conditional access apparatus.

10. The source apparatus of claim 9, wherein the non-RTT condition is met when the conditional access apparatus has been registered with the source apparatus.

11. The source apparatus of claim 9, wherein the non-RTT condition is met when:

the conditional access apparatus has been registered with the source apparatus; and

the content has been:

designated as remotely accessible; or

not designated as remotely inaccessible.

12. The source apparatus of claim 11, wherein the non-RTT condition is met only when:

the conditional access apparatus has been registered with the source apparatus; and

the content has been designated as remotely accessible.

13. The source apparatus of claim 9, wherein the registration section is configured to:

transmit a second command to the conditional access apparatus; and

receive from the conditional access apparatus a second response to the second command.

14. The source apparatus of claim 13, wherein the conditional access apparatus is registered with the source apparatus when a second time elapsed between transmission of the second command and reception of the second response does not exceed a second predetermined RTT.

15. The source apparatus of claim 9, wherein only a number of conditional access apparatuses below a threshold value can be registered with the source apparatus at any one time.

16. The source apparatus of claim 8, wherein at least one of the first and the second authorization signals includes an exchange key for generating a content key for decrypting the content.

17. The source apparatus of claim 16, wherein the at least one of the first and the second authorization signals includes a nonce for generating the content key.

18. The source apparatus of claim 8, wherein:

the first authorization section is configured to transmit the first authorization signal to the conditional access apparatus; and the second authorization section is configured to transmit the second authorization signal to the conditional access apparatus.

19. The source apparatus of claim 8, wherein the predetermined RTT is 7 milliseconds.

20. A method for selectively generating a signal with a conditional access apparatus to permit decryption of encrypted content, the method comprising:

receiving a command transmitted by a source apparatus;

transmitting to the source apparatus a response to the command;

upon receipt of an indication signal indicating that a time elapsed between transmission of the command by the source apparatus and reception of the response by the source apparatus does not exceed a predetermined round trip time (RTT), generating a first authorization signal to permit decryption of the content; and whenever a non-RTT condition is met, generating a second authorization signal to permit decryption of the content.

21. A method for selectively generating a signal with a source apparatus to permit a conditional access apparatus to decrypt encrypted content, the method comprising:

transmitting a command to the conditional access apparatus;

receiving from the conditional access apparatus a response to the command;

when a time elapsed between transmission of the command and reception of the response does not exceed a predetermined round trip time (RTT), generating a first authorization signal to permit the conditional access apparatus to decrypt the content; and

whenever a non-RTT condition is met, generating a second authorization signal to permit the conditional access apparatus to decrypt the content.

22. A conditional access apparatus for selectively generating a signal to permit decryption of encrypted content, the conditional access apparatus comprising:

a memory storing a program; and

a processor configured to execute the program to cause the conditional access apparatus to perform a method for selectively generating the signal, the method comprising:

receiving a command transmitted by a source apparatus;

transmitting to the source apparatus a response to the command;

upon receipt of an indication signal indicating that a time elapsed between transmission of the command by the source apparatus and reception of the response by the source apparatus does not exceed a predetermined round trip time (RTT), generating a first authorization signal to permit decryption of the content; and whenever a non-RTT condition is met, generating a second authorization signal to permit decryption of the content.

23. A source apparatus for selectively generating a signal to permit a conditional access apparatus to decrypt encrypted content, the source apparatus comprising:

a memory storing a program; and

a processor configured to execute the program to cause the source apparatus to perform a method for selectively generating the signal, the method comprising:

transmitting a command to the conditional access apparatus;

receiving from the conditional access apparatus a response to the command;

when a time elapsed between transmission of the command and reception of the response does not exceed a predetermined round trip time (RTT), generating a first authorization signal to permit the conditional access apparatus to decrypt the content; and

whenever a non-RTT condition is met, generating a second authorization signal to permit the conditional access apparatus to decrypt the content.

24. A non-transitory, computer-readable storage medium storing a program that, when executed by a processor, causes a conditional access apparatus to perform a method for selectively generating a signal to permit decryption of encrypted content, the method comprising:

receiving a command transmitted by a source apparatus;

transmitting to the source apparatus a response to the command;

upon receipt of an indication signal indicating that a time elapsed between transmission of the command by the source apparatus and reception of the response by the source apparatus does not exceed a predetermined round trip time (RTT), generating a first authorization signal to permit decryption of the content; and

whenever a non-RTT condition is met, generating a second authorization signal to permit decryption of the content.

25. A non-transitory, computer-readable storage medium storing a program that, when executed by a processor, causes a source apparatus to perform a method for selectively generating a signal to permit a conditional access apparatus to decrypt encrypted content, the method comprising:

transmitting a command to the conditional access apparatus;

receiving from the conditional access apparatus a response to the command;

when a time elapsed between transmission of the command and reception of the response does not exceed a predetermined round trip time (RTT), generating a first authorization signal to permit the conditional access apparatus to decrypt the content; and whenever a non-RTT condition is met,

generating a second authorization signal to permit the conditional access apparatus to decrypt the content.

Dated this 02/03/2012

HRISHIKESH RAY CHAUDHURY
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANT[S]

[Fig. 1]

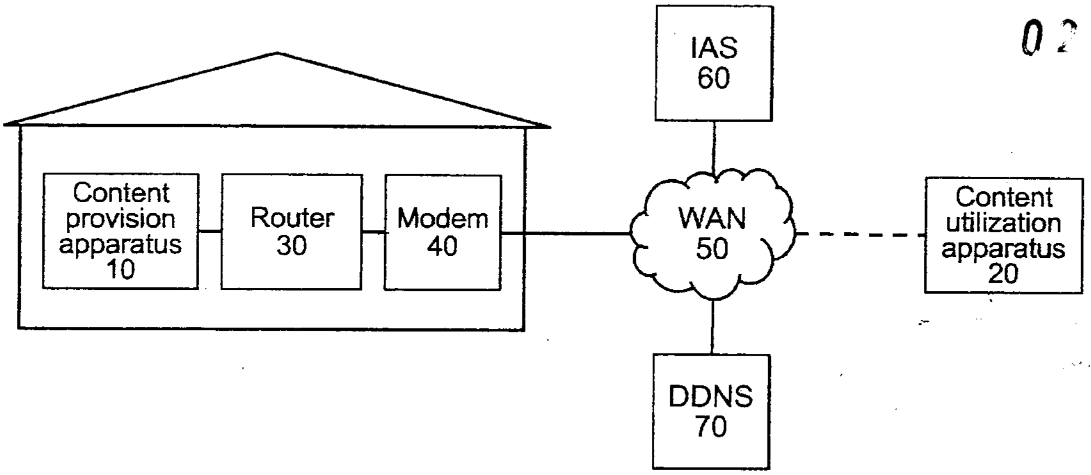

FIG.1

[Fig. 2]

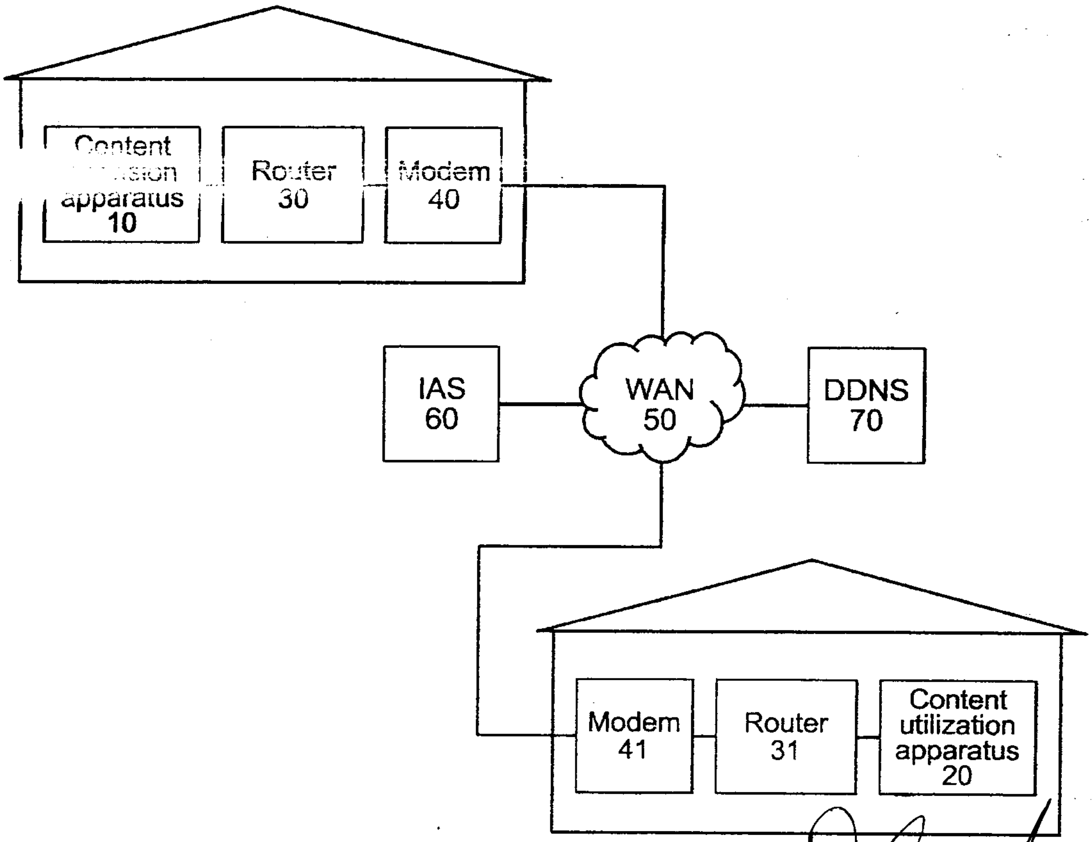

FIG.2

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 3]

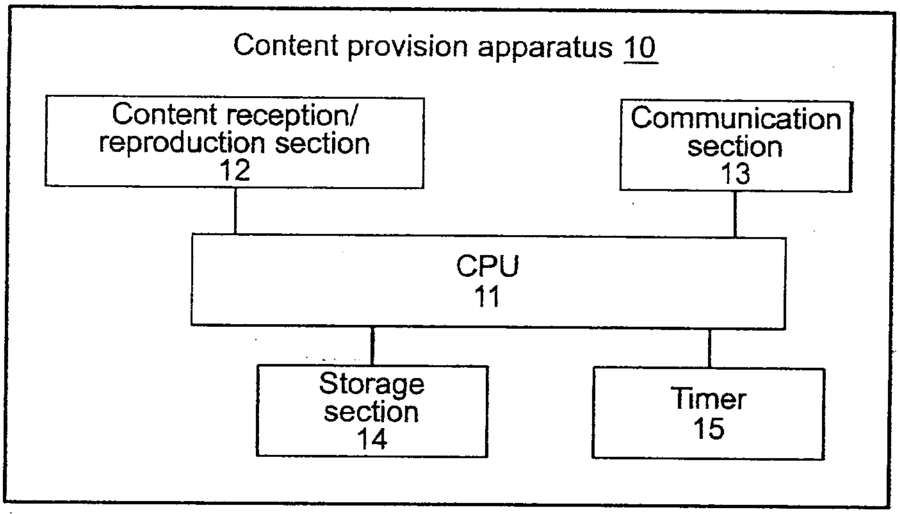
Content provision apparatus 10
Content reception/ reproduction section 12
Communication section 13
CPU 11
Storage section 14
Timer 15

FIG.3

[Fig. 4]

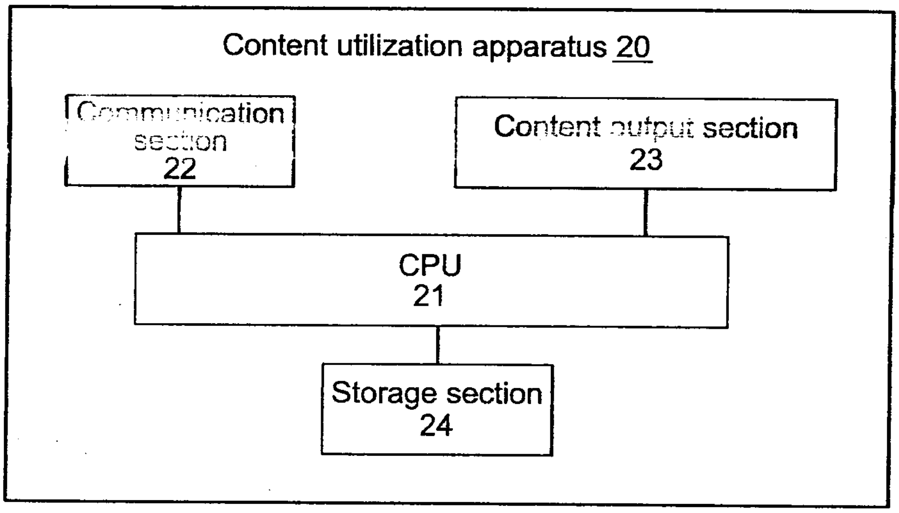

FIG.4

[Fig. 5]

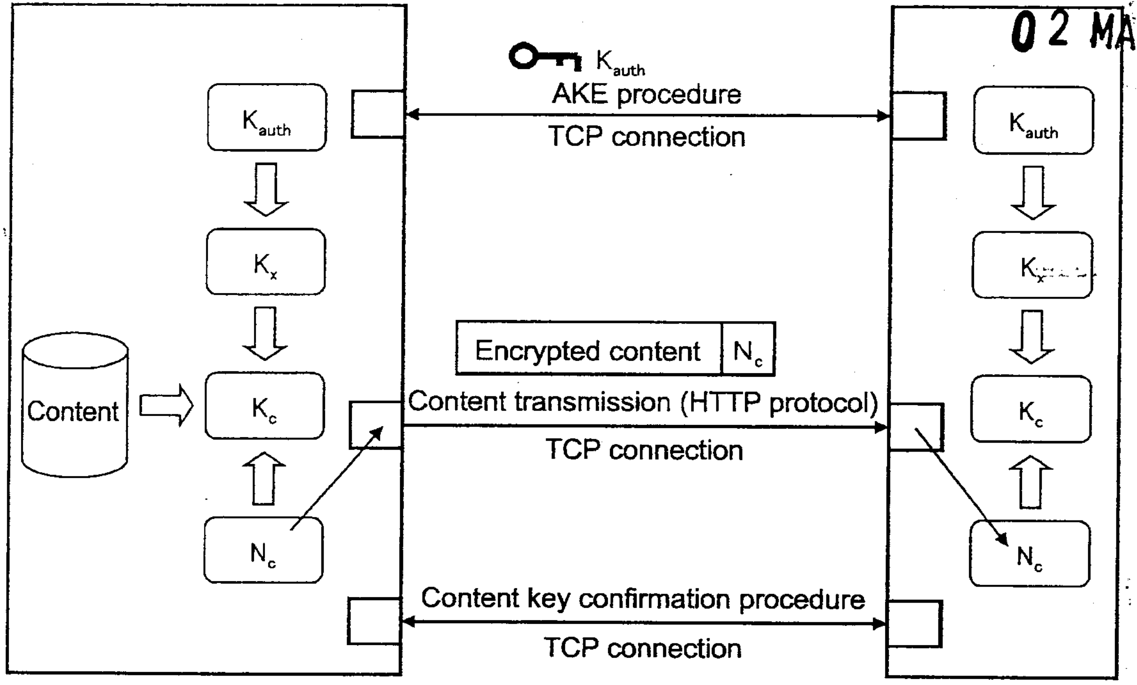

FIG.5

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 6]

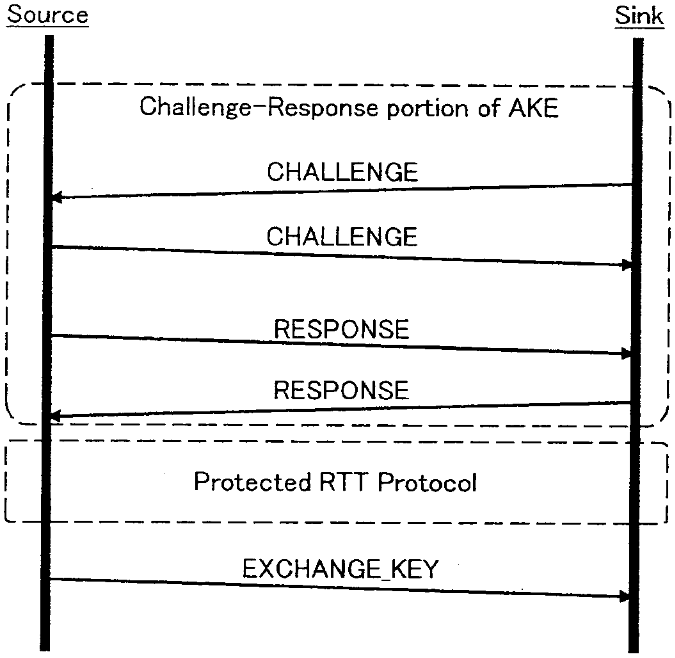

FIG.6

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 7]

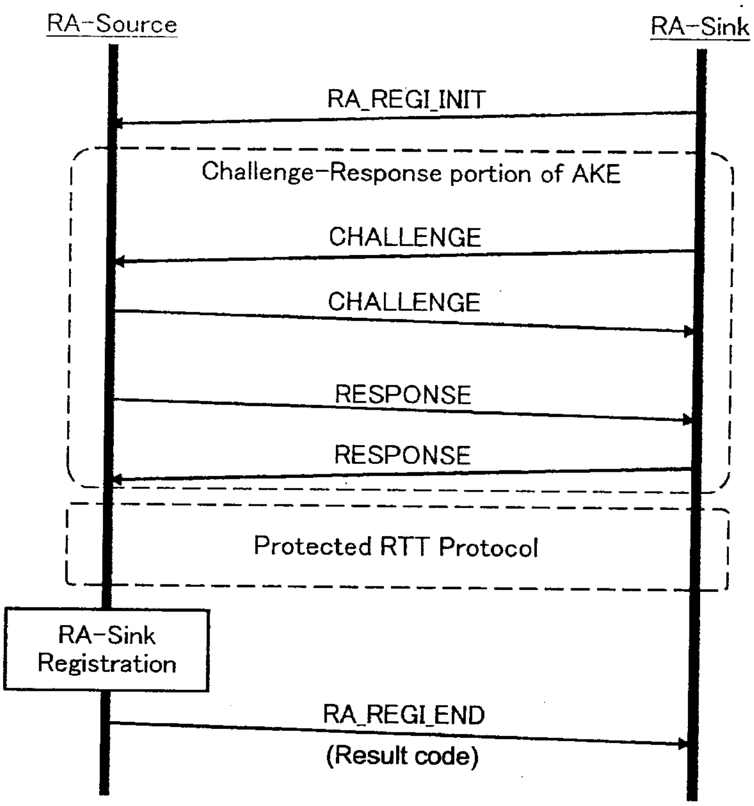

FIG.7

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 8]

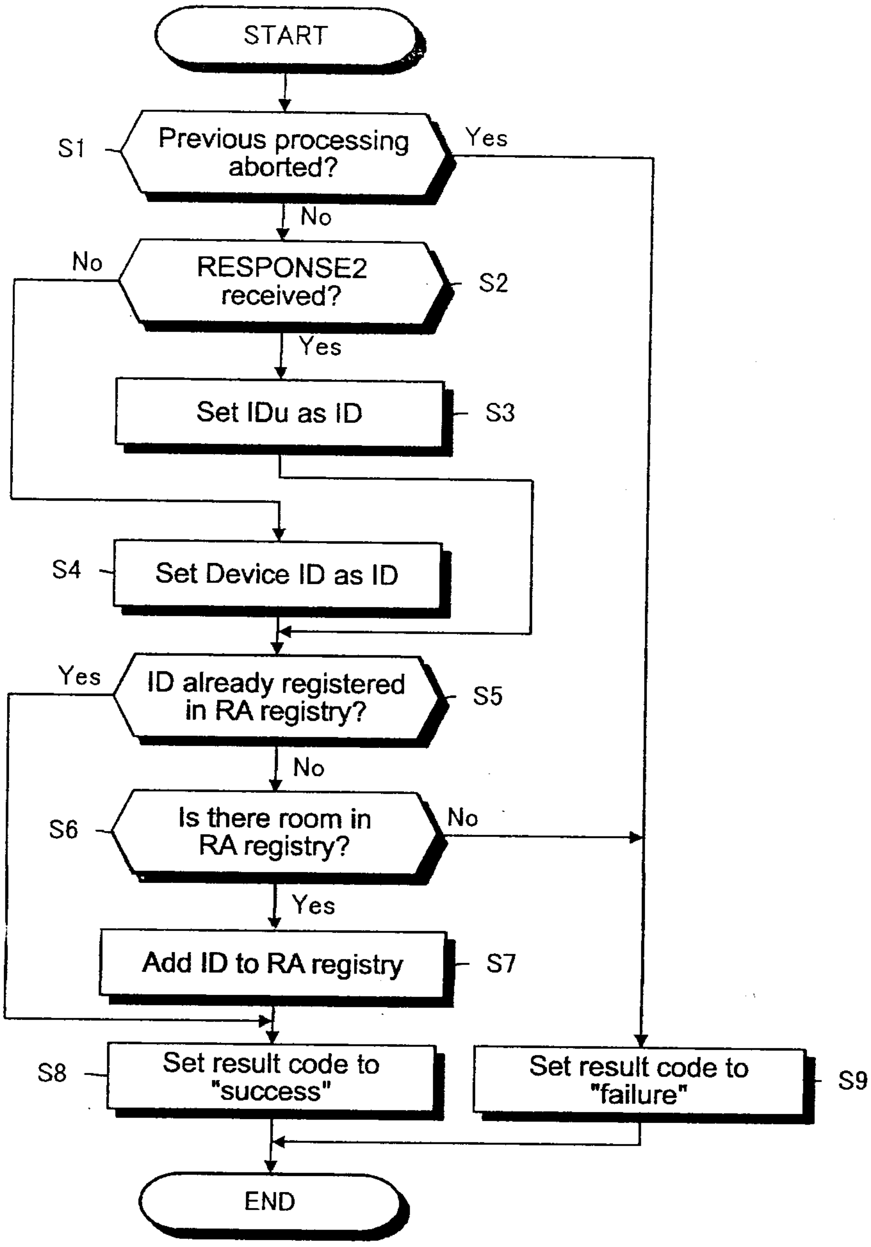
START
S1
Previous processing aborted?
Yes
No
RESPONSE2 received?
S2
No
Yes
Set IDu as ID
S3
S4
Set Device ID as ID
Yes
ID already registered in RA registry?
S5
No
S6
Is there room in RA registry?
No
Yes
Add ID to RA registry
S7
S8
Set result code to "success"
Set result code to "failure"
S9
END

FIG.8

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

ORIGINAL

[Fig. 9]

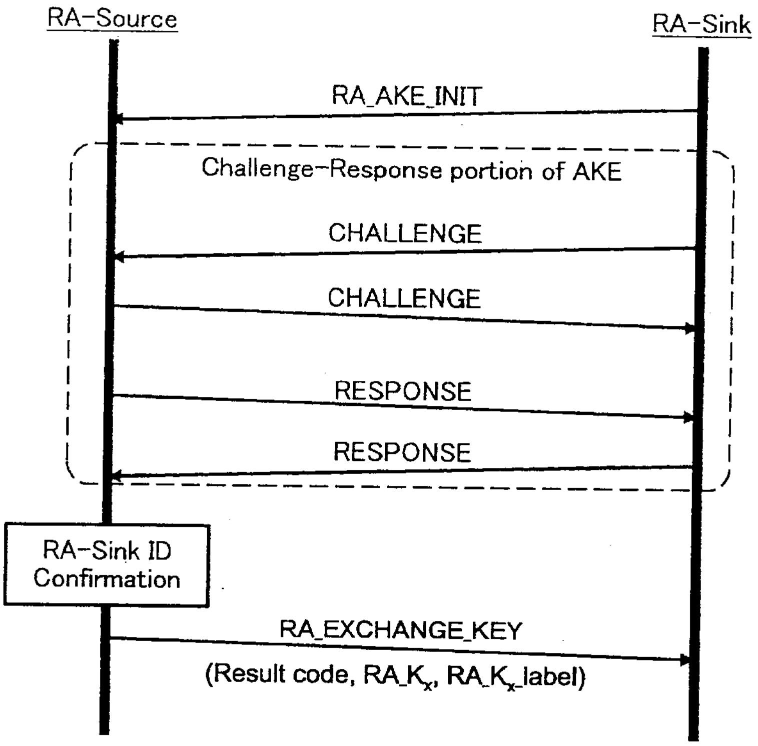

FIG.9

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 10]

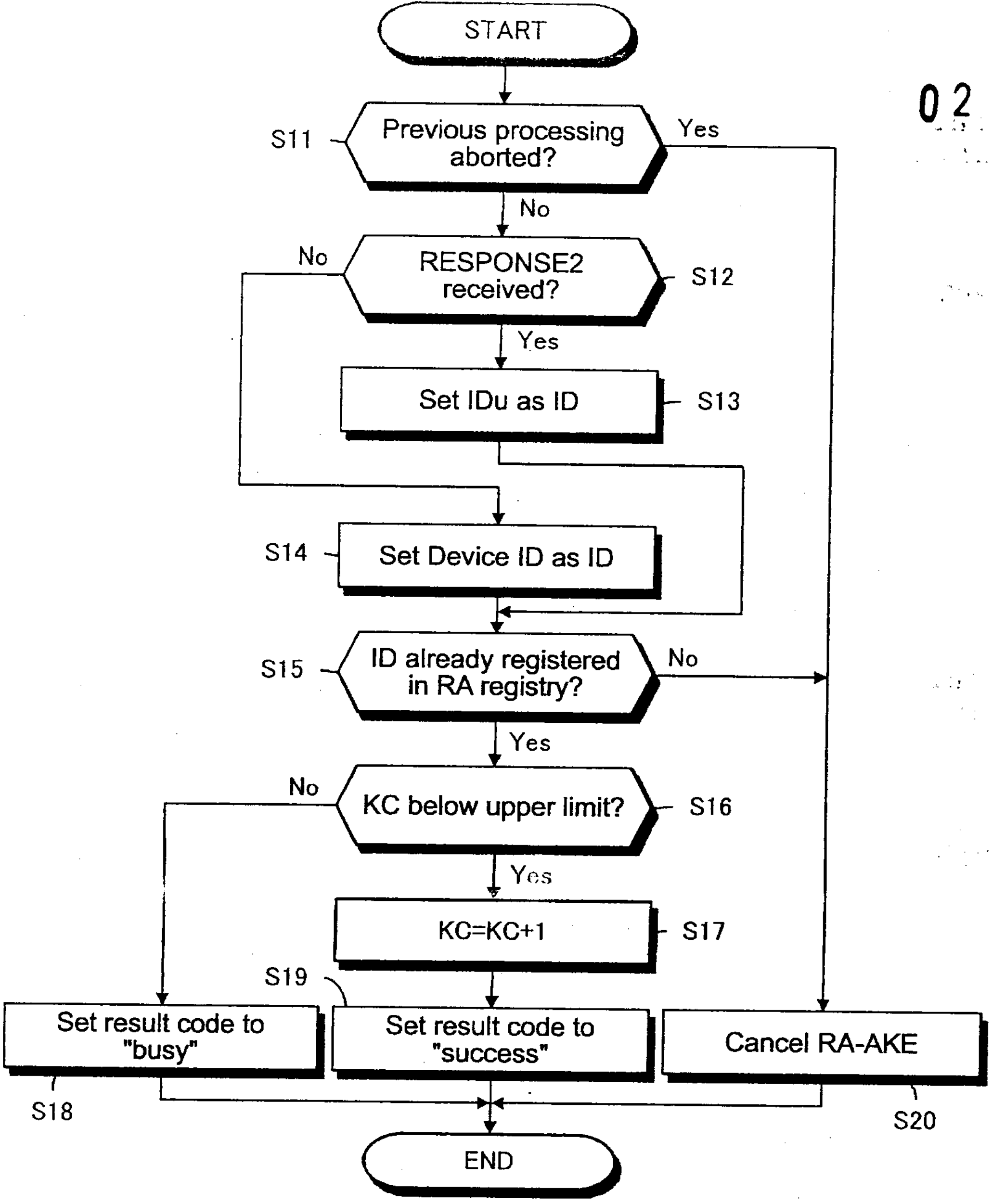

FIG.10

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 11]

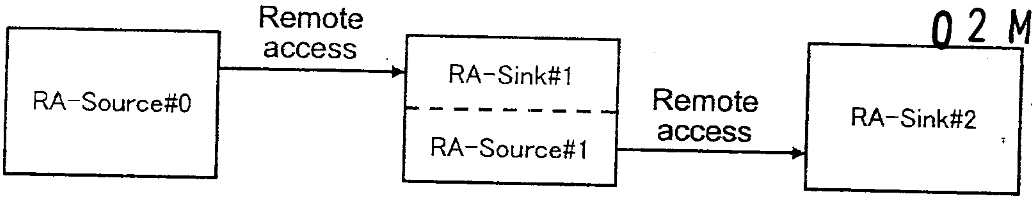

FIG.11

[Fig. 12]

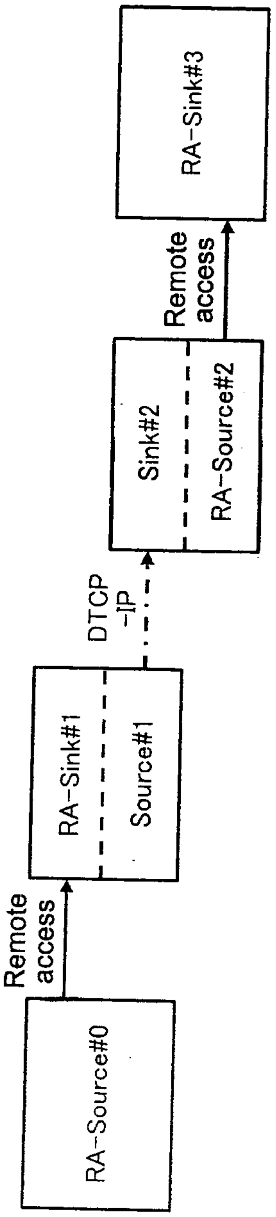

FIG.12

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

ORIGINAL

[Fig. 13]

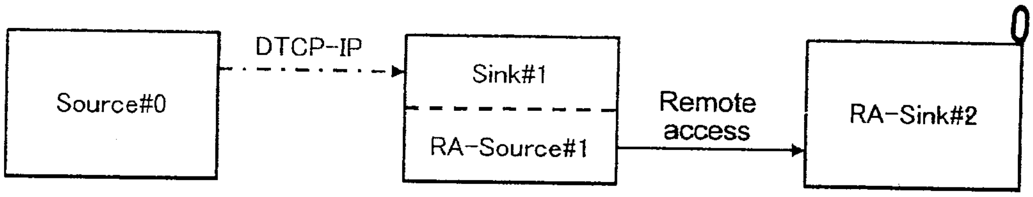

FIG.13

[Fig. 14]

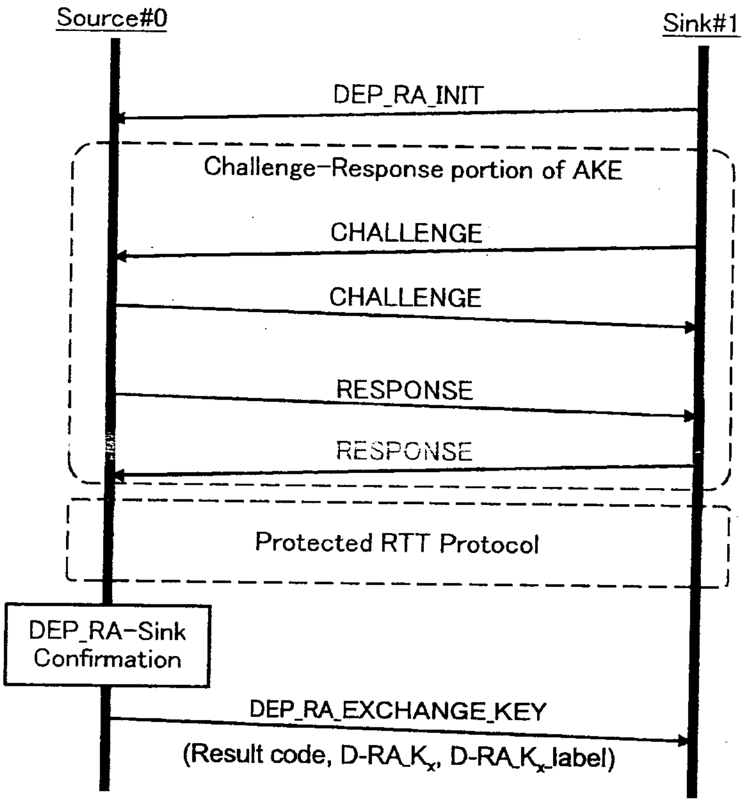

FIG.14

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 15]

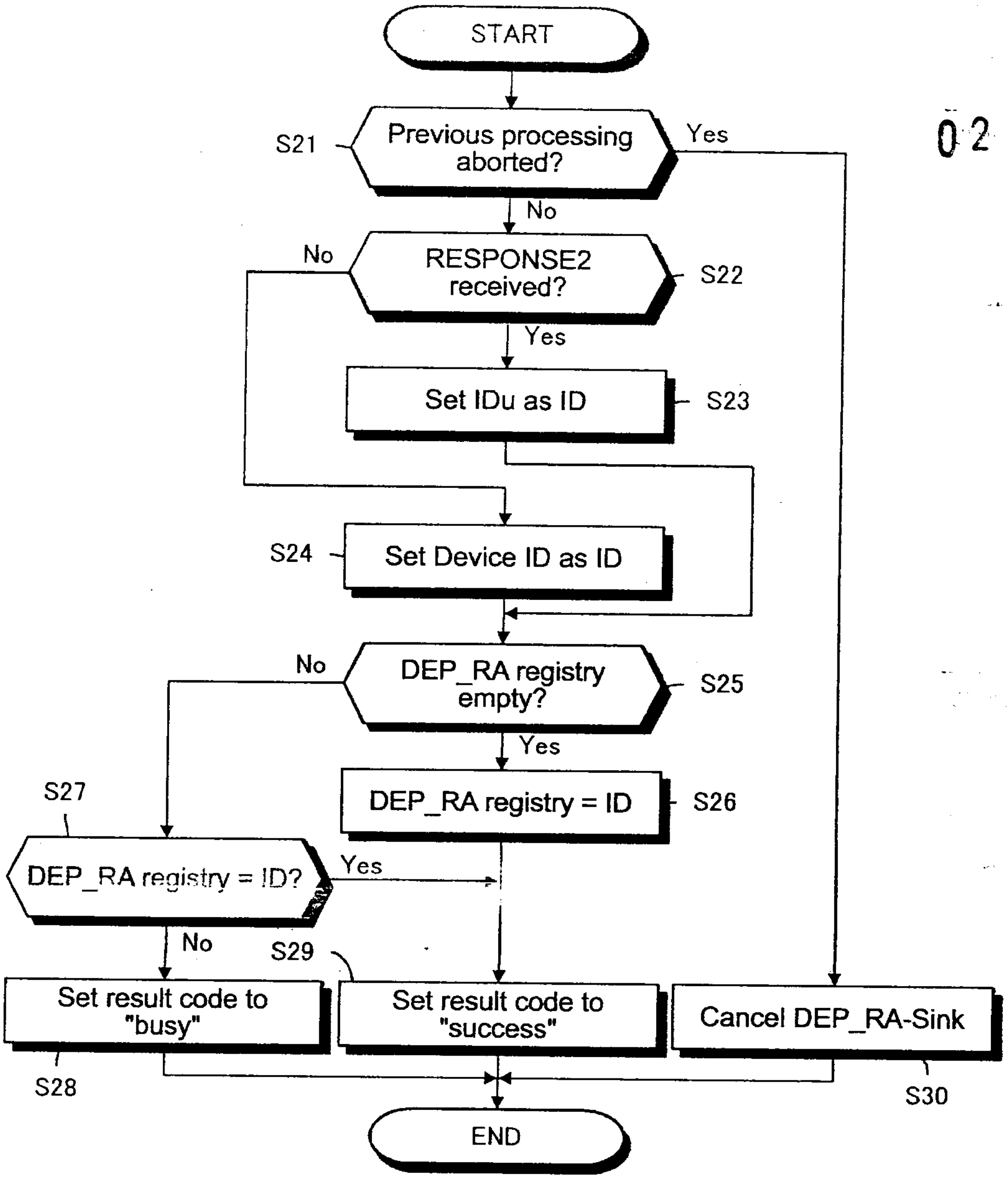

FIG.15

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 16]

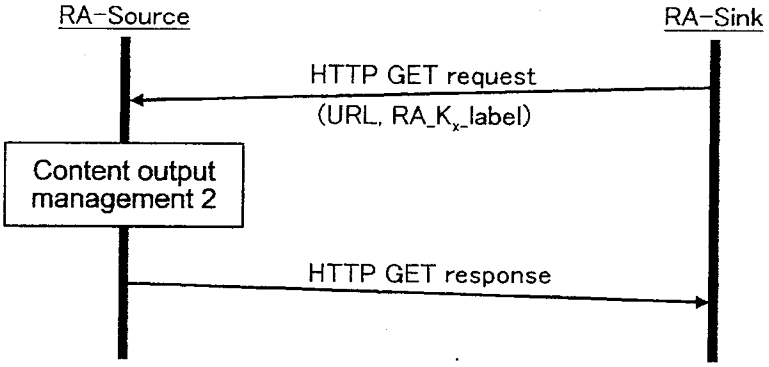

FIG.16

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 17]

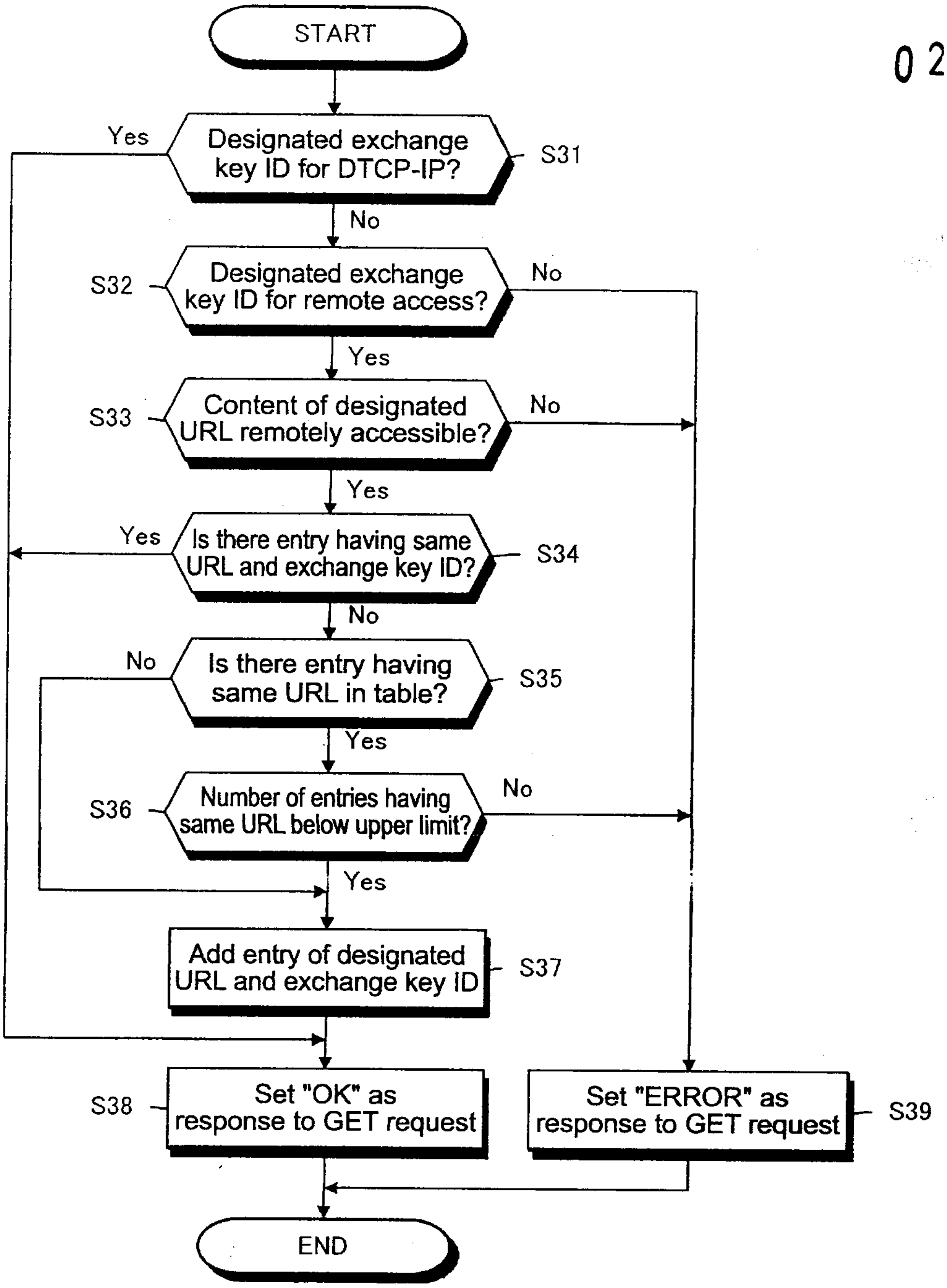
START
Designated exchange key ID for DTCP-IP?
S31
Yes
No
S32
Designated exchange key ID for remote access?
No
Yes
S33
Content of designated URL remotely accessible?
No
Yes
Yes
Is there entry having same URL and exchange key ID?
S34
No
No
Is there entry having same URL in table?
S35
Yes
S36
Number of entries having same URL below upper limit?
No
Yes
Add entry of designated URL and exchange key ID
S37
S38
Set "OK" as response to GET request
Set "ERROR" as response to GET request
S39
END

FIG.17

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 18]

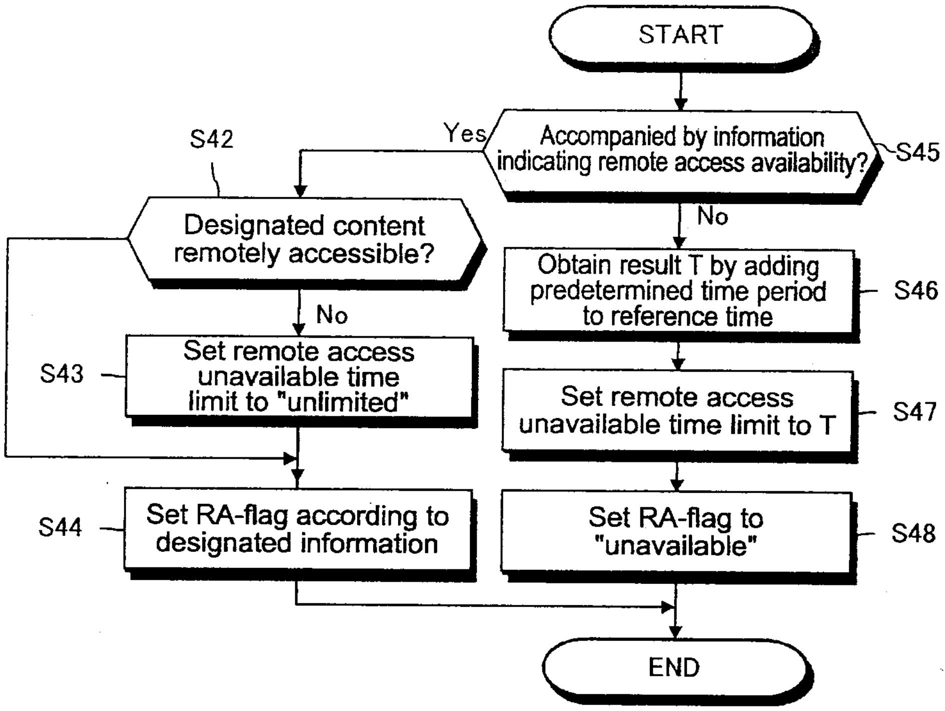
START
Accompanied by information indicating remote access availability?
S45
Yes
No
S42
Designated content remotely accessible?
No
S43
Set remote access unavailable time limit to "unlimited"
S44
Set RA-flag according to designated information
Obtain result T by adding predetermined time period to reference time
S46
Set remote access unavailable time limit to T
S47
Set RA-flag to "unavailable"
S48
END

FIG.18

[Fig. 19]

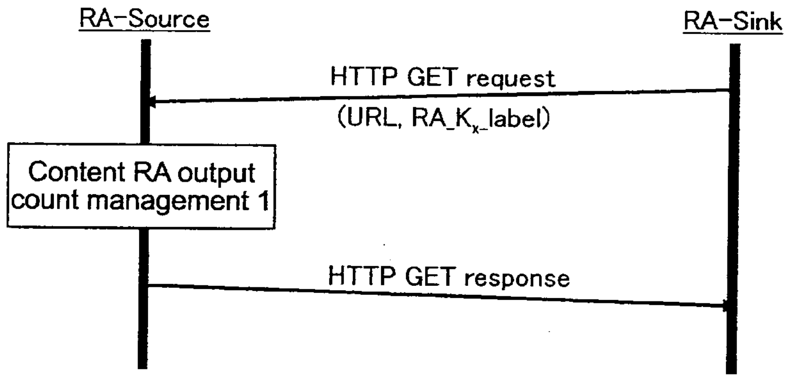

FIG.19

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 20]

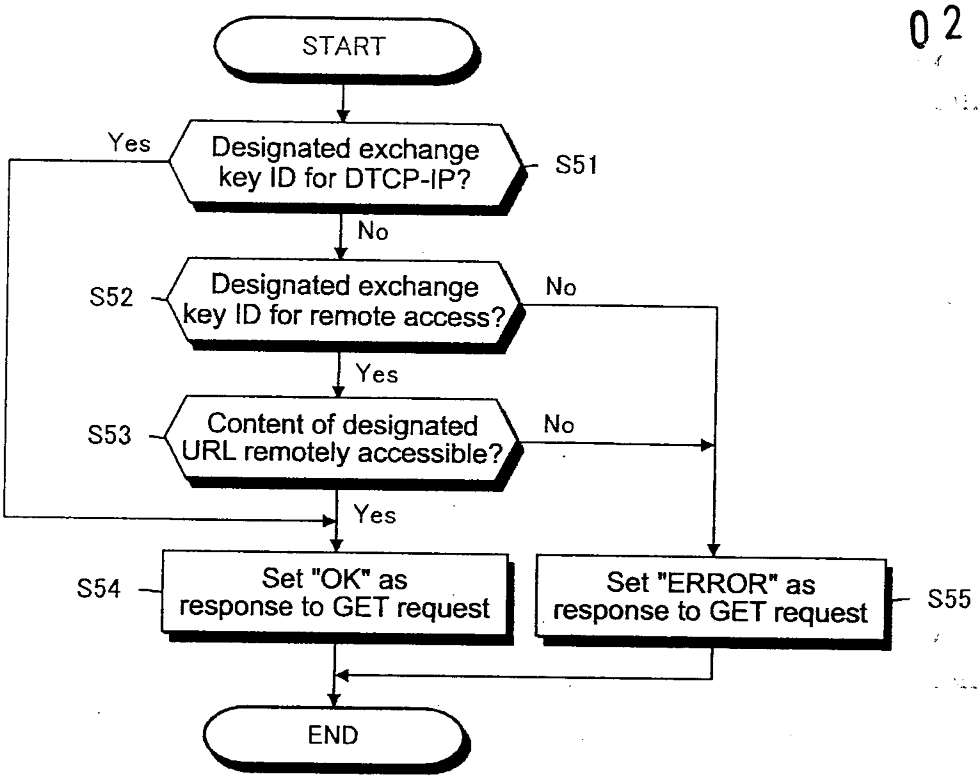
START
Designated exchange key ID for DTCP-IP?
S51
Yes
No
S52
Designated exchange key ID for remote access?
No
Yes
S53
Content of designated URL remotely accessible?
No
Yes
S54
Set "OK" as response to GET request
Set "ERROR" as response to GET request
S55
END

FIG.20

[Fig. 21]

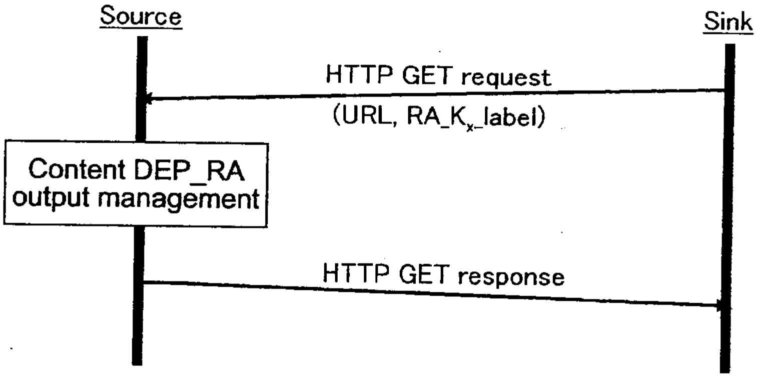

FIG.21

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 22]

0 2 MAR 2012

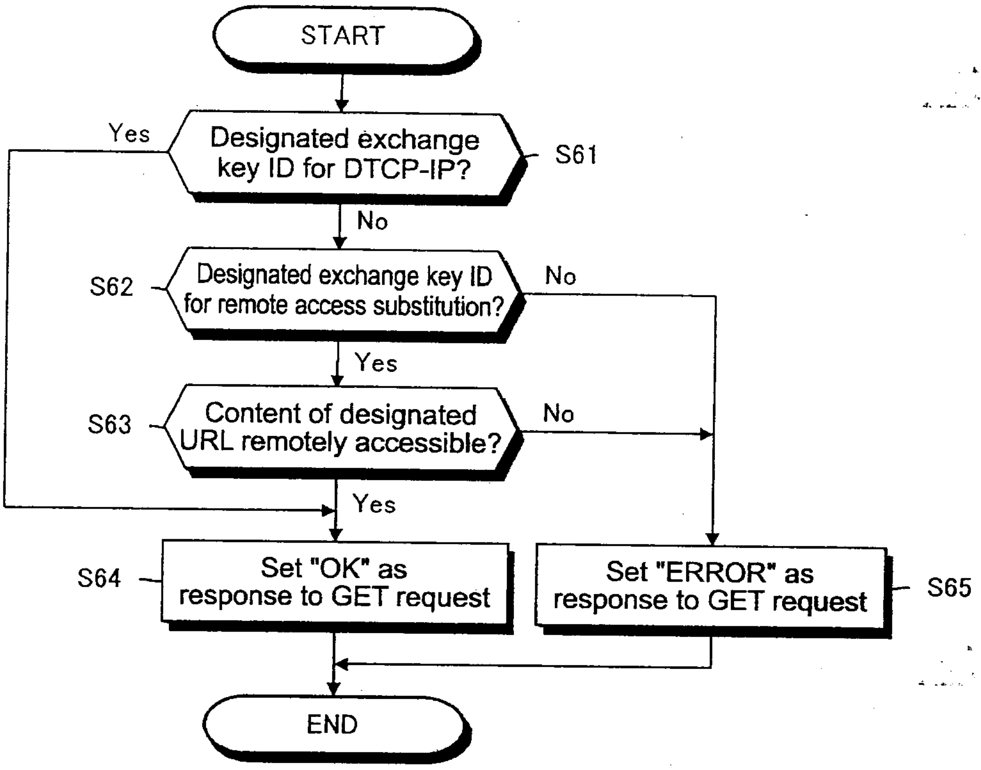
START
Designated exchange key ID for DTCP-IP?
S61
Yes
No
S62
Designated exchange key ID for remote access substitution?
No
Yes
S63
Content of designated URL remotely accessible?
No
Yes
S64
Set "OK" as response to GET request
Set "ERROR" as response to GET request
S65
END

FIG.22

[Fig. 23]

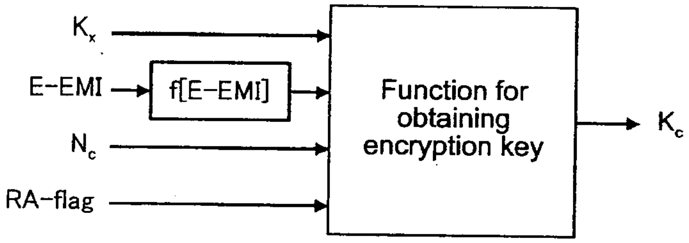

FIG.23

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 24]

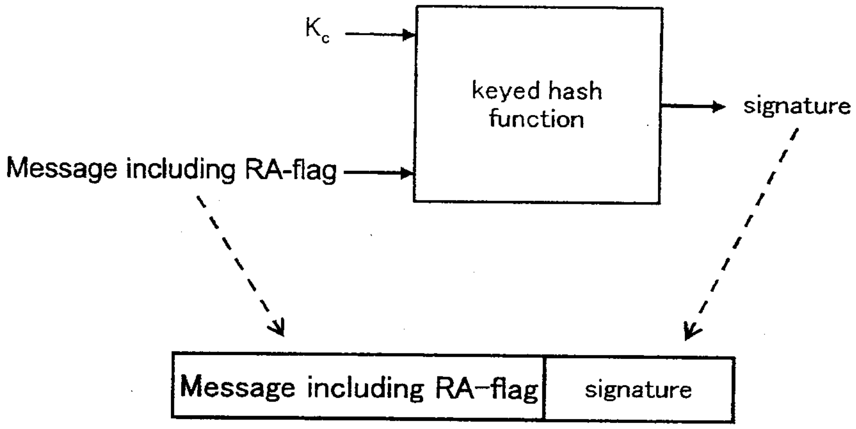

FIG.24

[Fig. 25]

Syntax	Size(bits)	Formats	Value
DTCP_descriptor (){			
descriptor_tag	8	uimsbf	0x88
descriptor_length	8	uimsbf	
CA_System_ID	16	uimsbf	0x0fff
for(i=0; i<descriptor_length-2; i++){			
private_data_byte	8	bslbf	
}			
}			

Syntax	Size(bits)	Formats
Private_data_type{		
Reserved	1	bslbf
Retention_Move_mode	1	bslbf
Retention_State	3	bslbf
EPN	1	bslbf
DTCP_CCI	2	bslbf
Reserved	5	bslbf
Image_Constraint_Token	1	bslbf
APS	2	bslbf
}		

FIG.25

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 26]

	msb							lsb
PCP−UR[0]	UR Mode		Content Type		APS		ICT	
PCP−UR[1]	Reserved							

FIG.26

[Fig. 27]

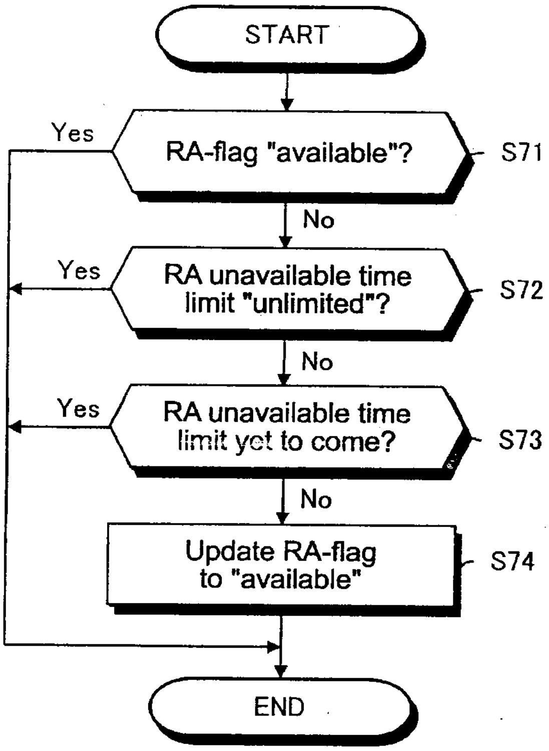
START
Yes
RA-flag "available"?
S71
No
Yes
RA unavailable time limit "unlimited"?
S72
No
Yes
RA unavailable time limit yet to come?
S73
No
Update RA-flag to "available"
S74
END

FIG.27

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 28]

	msb							lsb
Type[0]	0	0	0	0	0	0	0	1
Length[0]	(msb) Byte Length of Control and AKE_Info Fields (N+8)							
Length[1]	(lsb)							
Control[0]	reserved (zero)				ctype/response			
Control[1]	Category = 0000_2 (AKE)				AKE_ID = 0000_2			
Control[2]	subfunction							
Control[3]	AKE_procedure							
Control[4]	exchange_key							
Control[5]	subfunction_dependent							
Control[6]	AKE_label							
Control[7]	number (option)				status			
AKE_Info[0..N-1]	AKE_Info							

FIG.28

[Fig. 29]

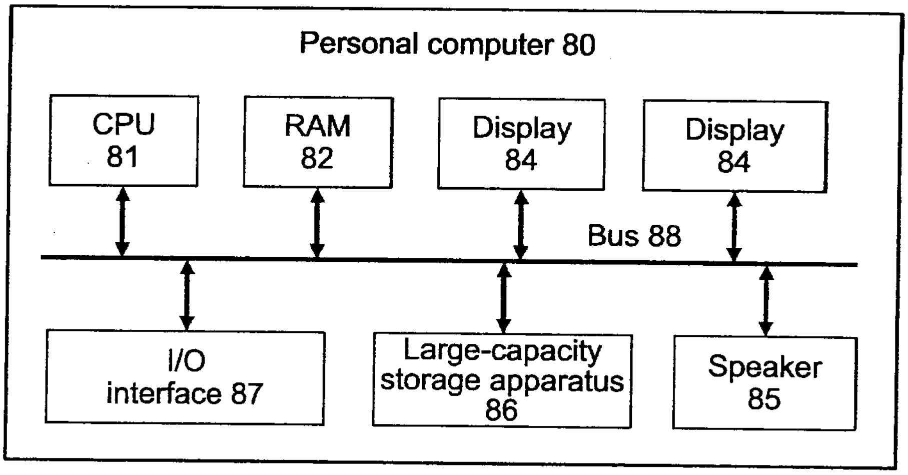

FIG.29

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

[Fig. 30]

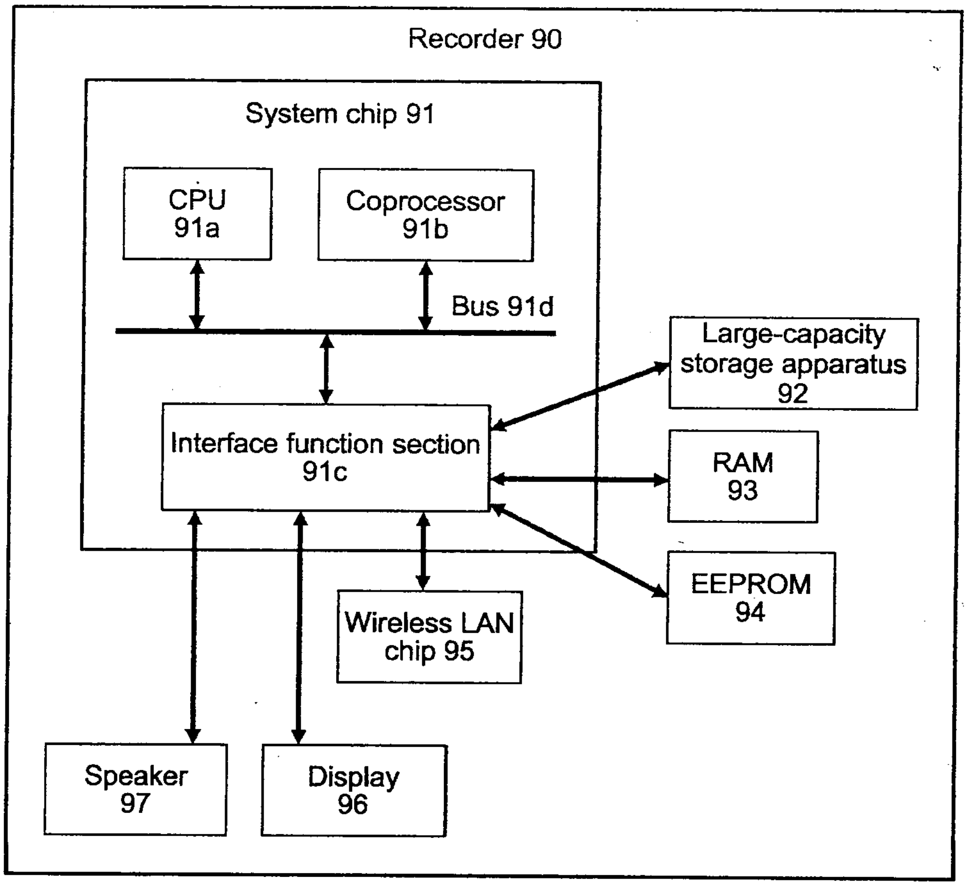

FIG.30

(HRISHIKESH RAY CHAUDHURY)
OF REMFRY & SAGAR
ATTORNEY FOR THE APPLICANTS

The present invention relates to a communication system, a communication apparatus, a communication method, and a computer program for preventing an illegal use in a content transmission, more particularly, to a communication system, a communication apparatus, a communication method, and a computer program for exchanging a decryption key for an encrypted content in accordance with a predetermined mutual authentication and key exchange (AKE: Authentication and Key Exchange) algorithm as well as transmit the encrypted content.

[0002]

More specifically, the present invention relates to a communication system for safely transmitting a content via a remote access (RA) that uses an external network such as a WAN, and a communication apparatus, a communication method, and a computer program for safely transmitting a content via a remote access while exceeding limits on a round-trip time (RTT), a hop count of an IP (Internet Protocol) router, and the like, more particularly, to a communication system, a communication apparatus, a communication method, and a computer program.

[Background Art]

[0003]

From the past, broadcast contents and contents in package media have been basically used at a location where a reception apparatus or a reproduction apparatus is installed or in an apparatus connected to those apparatuses via a home network (hereinafter, also referred to as "local access (LA)"). For example, it has been difficult to connect to the reception apparatus or the reproduction apparatus from outside using a portable apparatus and use a content transmitted via an external network such as a WAN (Wide Area Network) (hereinafter, also referred to as "remote access (RA)") from a technical viewpoint of a communication path, a codec, and the like. However, it is expected that in the future, a data communication technique such as LTE (Long Term Evolution) and WiMAX (World Interoperability for Microwave Access) and a high-compression codec such as H.264 will prevail. Thus, there is a possibility that the remote access will be realized by using those techniques. For example, a user may remotely access a home server from outside and reproduce a content.

[0004]

On the other hand, a digitized content is relatively-easily manipulated as in copying, falsifications, and the like. Above all, in the remote access, there is a need for a mechanism for preventing an illegal use that occurs in a content transmission, that is, for a copyright protection while permitting an individual or domestic use of a content.

[0005]

As an industrially-standard technique regarding a transmission protection of digital contents, there is a DTCP (Digital Transmission Content Protection) developed by DTLA (Digital Transmission Licensing Administrator). In DTCP, an inter-apparatus authentication protocol used in a content transmission and a transmission protocol of an encrypted content are arranged. In short, it is regulated that a DTCP-compliant apparatus does not transmit an easily-handled compressed content to an external apparatus in an unencrypted state, an exchange key necessary for decrypting an encrypted content is generated in accordance with a predetermined mutual authentication and key exchange (AKE) algorithm, a range of apparatuses to exchange keys based on an AKE command is limited, and the like. A server as a content provider (source) and a client as a content provision destination (sink) share a key via an authentication processing by exchanging an AKE command and thus perform a content transmission by encrypting a transmission path using that key. Therefore, since an unauthorized client is unable to obtain an encryption key unless succeeding in the authentication with the