

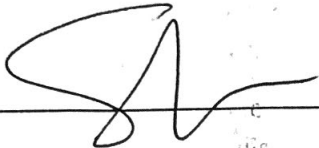
I, SHAUN WU, hereby declare:

That I possess advanced knowledge of the Japanese and English languages. The attached Japanese into English translation has been translated by me and to the best of my knowledge and belief, it is a true and accurate translation of the Japanese Patent Publication No. 2004-166153.

I declare that all statements made above of my own knowledge are true and that all statements made on information and belief are believed to be true. I have been warned and understand that willful false statements and the like are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code.

I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct.

Executed on May 14, 2024 in Los Angeles, California.

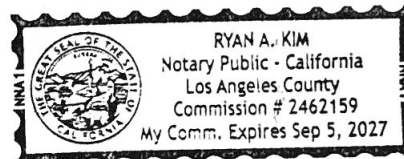


Shaun Wu



Notary Public

Notary Commission Expiry 09/05/2027



(19) Japan Patent Office (JP)

(12) Japanese Unexamined Patent Application Publication (A)

(11) Patent Application Publication Number
Laid-Open Patent Application
No. 2004-166153
(P2004-166153A)

(43) Publication Date: **June 10, 2004 (2004.6.10)**

| | | | | |
|------------------|----|----------|------|------------------------|
| (51) Int.C1.7 | F1 | | | Theme Code (Reference) |
| HO4L 9/08 | | HO4L9/00 | 601B | 5J10A |
| HO4L 9/14 | | HO4L9/00 | 641 | |

Request for Review: Yes

Number of Claims: 8 OL (Total 25 pages)

(21) Application Number JP2002-332404 (P2002-332404)
 (22) Application Date November 15, 2002 (2002.11.15)

(71) Applicant 000004237
 NEC Corporation
 5-7-1 Shiba, Minato-Ku, Tokyo

(71) Applicant 000232254
 NEC Communication Systems, Ltd.
 1-4-28 Mita, Minato-Ku, Tokyo

(74) Agent 100088890
 Patent Attorney: Junichi Kawahara

(72) Inventor Kazuya Suzuki
 NEC Corporation, 5-7-1 Shiba, Minato-Ku, Tokyo

(72) Inventor Jibiki Masahiro
 NEC Corporation, 5-7-1 Shiba, Minato-Ku, Tokyo

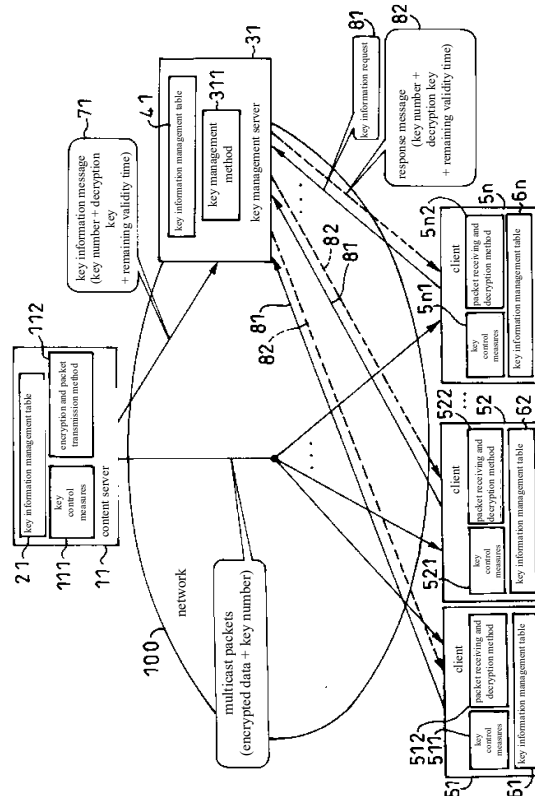
Continue to the last page

(54) [Name of Invention] KEY EXCHANGE METHOD IN MULTICAST DISTRIBUTION SYSTEM

(57)[Abstract]

[Problem] The present invention aims to avoid processing delays that occur when a client acquires a new decryption key during key change (exchange).
 [Solution] A content server distributes a decryption key to be used next to a key management server within the validity time of the key currently in use, and transmits a multicast packet including the key number. Each of the clients 51 to 5n requests the key management server 31 to transmit the next decryption key to be used within the validity time of the key currently in use and after the content server 11 has distributed the next decryption key to be used to the key management server 31. Also, the encrypted data in the multicast packet is decrypted using a decryption key corresponding to the key number in the multicast packet. The key management server 31 receives the next decryption key to be used from the content server 11, and in response to a transmission request from each of the clients 51 to 5n, transmits the next decryption key to be used to the source of the request.

[Selected Drawing] Figure 1



CLAIMS

[Claim 1]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server that creates an encryption key/decryption key, manages the encryption key/decryption key and its key number and remaining validity time, distributes the decryption key to be used next to the key management server within the validity time of the key in use, and transmits a multicast packet containing encrypted data and the key number of the encryption key used in the encryption;

a client that requests the key management server to transmits the decryption key to be used next within the validity time of the key in use after the content server distributes the decryption key to be used next to the key management server, and decrypts the encrypted data in the multicast packet using the decryption key corresponding to the key number in the multicast packet received from the content server; and

the key management server that manages the the decryption key, its key number and remaining validity time, receives a decryption key to be used next from the content server, and transmits the decryption key to be used next to the client in response to a request from the client.

[Claim 2]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server that manages the encryption key, its key number, and remaining validity time, requests the key management server to create the next encryption key/decryption key within the validity time of the key in use, receives the encryption key created in response to the request from the key management server, transmits a multicast packet containing encrypted data and the key number of the encryption key used in the encryption;

a client that requests the key management server to transmit the decryption key to be used next after the content server requests the key management server to create an encryption key/decryption key to be used next within the validity time of the key in use, decrypts the encrypted data in the multicast packet using the decryption key corresponding to the key number in the multicast packet received from the content server; and

the key management server that manages the encryption key, decryption key, their key numbers and remaining validity time, creates and stores an encryption key/decryption key to be used next in response to a request from the content server, and transmits the encryption key to be used next to the content server, and transmits the decryption key to be used next to the client in response to a request from the client.

[Claim 3]

A key exchange method in a multicast distribution system according to claim 1 or 2, wherein the address of a key management server is added to the information in a multicast packet transmitted from a content server to a client, thereby eliminating the need for the client to set a destination for querying and requesting a decryption key.

[Claim 4]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a key information management table in the content server that stores a set of the encryption key/decryption key in use, its key number, and its remaining validity time, and a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time;

a key management means within the content server that transmits a key information message regarding the decryption key to be used next to the key management server when the remaining validity time of the key in use reaches the first setting value, switches the key stored in the table as the next key to be used to the new key in use when the remaining validity time of the key in use reaches 0, creates a new encryption key/decryption key to be used next and saves the key information in the table;

an encryption/packet transmission means within the content server that encrypts the distributed data using the encryption key in use stored in its table at the time of multicast distribution, transmits a multicast packet containing encrypted data and the key number of the encryption key;

10

20

30

40

50

a key information management table in the client that stores a set of the decryption key in use, its key number, and its remaining validity time, and can store a set of the decryption key to be used next, its key number, and its remaining validity time;

a packet receiving/decryption means within the client that receives multicast packets sent from the content server, searches the decryption key from its table according to the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key of that key number;

a key management means within the client that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value, saves the set of the decryption key to be used next, its key number, and its remaining validity time in the response message in its own table, and switches the key that was previously stored in the table as the next key to be used to the new key in use based on the recognition of changes in key numbers in multicast packets sent from the content server;

10

a key information management table in the key management server that can store a set of the decryption key in use, its key number, and its remaining validity time, and can store a set of the decryption key to be used next, its key number, and its remaining validity time;

and a key management means within the key management server that saves a set of the decryption key to be used next, its key number, and its remaining validity time in the key information message received from the content server in its table, transmits a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time back to the client when receiving a key information request from the client when the remaining validity time of the key in use reaches the second setting value, switches the key stored in the table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0.

[Claim 5]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

20

a key information management table in the content server that can hold a set of the encryption key in use, its key number, and its remaining validity time, and can also hold a set of the encryption key to be used next, its key number, and its remaining validity time;

a key management means within the content server that issues a key creation request requesting the key management server to create the next key to be used when the remaining validity time of the key in use reaches the first setting value, saves the set of the encryption key to be used next, its key number, and its remaining validity time in the key information response message in its own table, and switches the key stored in the table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0;

an encryption/packet transmission means within the content server that encrypts the distributed data using the encryption key in use stored in its own table at the time of multicast distribution, transmits a multicast packet containing encrypted data and the key number of the encryption key;

a key information management table in the client that stores a set of the decryption key in use, its key number, and its remaining validity time, and can store a set of the decryption key to be used next, its key number, and its remaining validity time;

30

a packet receiving/decryption means within the client that receives multicast packets sent from the content server, searches the decryption key from its table according to the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key of that key number;

a key management means within the client that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value, saves the set of decryption key to be used next, its key number, and its remaining validity time in the response message in its table, and switches the key that was previously stored in the table as the next key to be used to the new key in use based on recognition of changes in key numbers in multicast packets sent from the content server;

a key information management table in the key management server that can store a set of the encryption key/decryption key in use, its key number, and its remaining validity time, and can also store a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time; and

40

50

a key management means within the key management server that creates the encryption key/decryption key to be used next in response to the key creation request from the content server, saves the set of the encryption key/decryption key to be used next, its key number, and its remaining validity time in its table, returns a key information response message regarding the encryption key to be used next to the content server, transmits a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time back to the client, and switches the key stored in the table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0.

[Claim 6]

A key exchange method in a multicast distribution system according to claim 4 or claim 5, wherein the address of a key management server is added to the information in a multicast packet transmitted from a content server to a client, thereby eliminating the need for the client to set a destination for a key information request.

10

[Claim 7]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server key exchange control program in which the content server functions as

a key information management table that stores a set of an encryption key/decryption key in use, its key number, and its remaining validity time, and a set of an encryption key/decryption key to be used next, its key number, and its remaining validity time,

a key management means in which when the remaining validity time of the key in use reaches the first setting value, it transmits a key information message regarding the decryption key to be used next to the key management server and when the remaining validity time of the key in use reaches 0, switches the key stored in its own table as the next key to be used to a new key in use, creates a new encryption key/decryption key to be used next, and saves the key information in its own table, and

20

an encryption/packet transmission means that encrypts distributed data using the currently used encryption key stored in its own table during multicast distribution, and transmits a multicast packet containing the encrypted data and the key number of the encryption key;

a client key exchange control program in which the client functions as

a key information management table capable of holding a set of a decryption key in use, its key number, and its remaining validity time, and a set of a decryption key to be used next, its key number, and its remaining validity time,

a packet receiving/decryption means that receives a multicast packet sent from a content server, searches for a decryption key from its own table using the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key with that key number, and

a key management means in which when the remaining validity time of the key in use reaches the second setting value, it transmits a key information request to the key management server, saves the set of the decryption key to be used next, its key number, and its remaining validity time in the response message in its own table, and switches the key that was previously stored in its own table as the next key to be used to the new key in use based on the recognition of changes in key numbers in multicast packets sent from the content server; and

30

a key exchange control program for the key management server in which the key management server functions as

a key information management table capable of storing a set of a decryption key in use, its key number, and its remaining validity time, and a set of a decryption key to be used next, its key number, and its remaining validity time, and

a key management method that saves a set of the decryption key to be used next, its key number, and its remaining validity time in the key information message received from the content server in its own table, transmits a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time back to the client in response to the key information request from the client when the remaining validity time of the key in use reaches the second setting value, and switches the next key to be used from the key stored in the own table to the new key in use when the remaining validity time of the currently used key reaches 0.

40

[Claim 8]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server key exchange control program in which the content server functions as

50

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.