# C L A I M S

~~1. A re-encryption system comprising a file sharing apparatus (10) and a re-encryption apparatus (30) which are communicable with a client apparatus (20) operated by a member belonging to a group,~~

~~the file sharing apparatus comprising~~

~~file storage means (15) for storing a first encrypted file obtained by encrypting a file based on a public key of the group,~~

~~means (11) for acquiring, upon receiving a file request including a member ID for identifying the member and a file name of the first encrypted file from the client apparatus, the first encrypted file from the file storage means based on the file name included in the file request,~~

~~means (13) for transmitting a re-encryption request including the acquired first encrypted file and the member ID included in the file request to the re-encryption apparatus, and~~

~~means (11) for transmitting, upon receiving a second encrypted file obtained by encrypting the file based on the public key of the member ID from the re-encryption apparatus, the second encrypted file to the client apparatus, and~~

~~the re-encryption apparatus comprising~~

~~re-encryption key storage means (35) for storing the member ID for identifying the member and a re-encryption key for re-encrypting, without decrypting, the first encrypted file to the second encrypted file in association with each other,~~

~~means (33) for acquiring, upon receiving the re-encryption request from the file sharing apparatus, the re-encryption key from the re-encryption key storage means~~

~~based on the member ID included in the re-encryption request,~~

~~means (33) for re-encrypting the first encrypted file included in the re-encryption request to the second encrypted file based on the acquired re-encryption key, and~~

~~means (31) for transmitting the second encrypted file obtained by the re-encryption to the file sharing apparatus,~~

~~wherein the client apparatus obtains the file by decrypting the second encrypted file from the file sharing apparatus based on a private key corresponding to the public key of the member.~~

---

1~~2~~. A re-encryption system comprising a file sharing apparatus (10) and a re-encryption apparatus (30) which are communicable with a client apparatus (20) operated by a member belonging to a group,

the file sharing apparatus comprising

file storage means (15) for storing an encrypted file including a first encrypted symmetric key portion obtained by encrypting a symmetric key based on a public key of the group and an encrypted data portion obtained by encrypting data based on the symmetric key,

first means (11) for acquiring, upon receiving a file request including a member ID for identifying the member and a file name of the encrypted file from the client apparatus, the encrypted file from the file storage means based on the file name included in the file request,

second means (13) for separating the acquired encrypted file into the first encrypted symmetric key portion and the encrypted data portion,

third means (13) for transmitting a re-encryption request including the first encrypted symmetric key portion

and the member ID included in the file request to the re-encryption apparatus simultaneously with encrypted data transmission processing whichof transmitsting the separated encrypted data portion to the client apparatus, and

fourth means (11) for transmitting, upon receiving a second encrypted symmetric key portion obtained by encrypting the symmetric key based on the public key of the member ID from the re-encryption apparatus simultaneously with the encrypted data transmission processing, the second encrypted symmetric key portion to the client apparatus after the encrypted data transmission processing, and

the re-encryption apparatus comprising

re-encryption key storage means (35) for storing the member ID for identifying the member and a re-encryption key for re-encrypting, without decrypting, the first encrypted symmetric key portion to the second encrypted symmetric key portion in association with each other,

means (33) for acquiring, upon receiving the re-encryption request from the file sharing apparatus, the re-encryption key from the re-encryption key storage means based on the member ID included in the re-encryption request,

means (33) for re-encrypting the first encrypted symmetric key portion included in the re-encryption request to the second encrypted symmetric key portion based on the acquired re-encryption key, and

means (31) for transmitting the second encrypted symmetric key portion obtained by the re-encryption to the file sharing apparatus,

wherein the client apparatus obtains the data by obtaining the symmetric key by decrypting the second encrypted symmetric key portion from the file sharing apparatus based on a private key corresponding to the

public key of the member, and decrypting the encrypted data portion from the file sharing apparatus based on the obtained symmetric key.

2~~3~~. The~~A~~ re-encryption system according to Claim 1, wherein the first means, the second means, the third means, and the fourth means are implemented using a filter function which adds predetermined processing~~apparatus (30) communicable with a file sharing apparatus (10) which is communicable with a client apparatus (20) operated by a member belonging to a group, stores, in a memory, a first encrypted file obtained by encrypting a file based on a public key of the group, acquires, upon receiving a file request including a member ID for identifying the member and a file name of the first encrypted file from the client apparatus, the first encrypted file from the memory based on the file name included in the file request, transmits a re-encryption request including the acquired first encrypted file and the member ID included in the file request to the re-encryption apparatus, and transmits, upon receiving a second encrypted file obtained by encrypting the file based on the public key of the member ID from the re-encryption apparatus, the second encrypted file to the client apparatus, the re-encryption apparatus comprising:~~

~~re-encryption key storage means (35) for storing the member ID for identifying the member and a re-encryption key for re-encrypting, without decrypting, the first encrypted file to the second encrypted file in association with each other,~~

~~means (33) for acquiring, upon receiving the re-encryption request from the file sharing apparatus, the re-encryption key from the re-encryption key storage means~~

~~based on the member ID included in the re-encryption request,~~

~~means (33) for re-encrypting the first encrypted file included in the re-encryption request to the second encrypted file based on the acquired re-encryption key, and~~

~~means (31) for transmitting the second encrypted file obtained by the re-encryption to the file sharing apparatus,~~

~~wherein the client apparatus obtains the file by decrypting the second encrypted file from the file sharing apparatus based on a private key corresponding to the public key of the member~~.

34. A re-encryption apparatus (30) communicable with a file sharing apparatus (10) which is communicable with a client apparatus (20) operated by a member belonging to a group, stores, in a memory, an encrypted file including a first encrypted symmetric key portion obtained by encrypting a symmetric key based on a public key of the group and an encrypted data portion obtained by encrypting data based on the symmetric key, executes first processing which acquires, upon receiving a file request including a member ID for identifying the member and a file name of the encrypted file from the client apparatus, the encrypted file from the memory based on the file name included in the file request, executes second processing which separates the acquired encrypted file into the first encrypted symmetric key portion and the encrypted data portion, executes third processing which transmits a re-encryption request including the first encrypted symmetric key portion and the member ID included in the file request to the re-encryption apparatus simultaneously with encrypted data transmission processing which~~of~~ transmit~~sting~~ the separated

encrypted data portion to the client apparatus, and executes fourth processing which transmits, upon receiving a second encrypted symmetric key portion obtained by encrypting the symmetric key based on the public key of the member ID from the re-encryption apparatus simultaneously with the encrypted data transmission processing, the second encrypted symmetric key portion to the client apparatus after the encrypted data transmission processing, the re-encryption apparatus comprising:

re-encryption key storage means (35) for storing the member ID for identifying the member and a re-encryption key for re-encrypting, without decrypting, the first encrypted symmetric key portion to the second encrypted symmetric key portion in association with each other,

means (33) for acquiring, upon receiving the re-encryption request from the file sharing apparatus, the re-encryption key from the re-encryption key storage means based on the member ID included in the re-encryption request,

means (33) for re-encrypting the first encrypted symmetric key portion included in the re-encryption request to the second encrypted symmetric key portion based on the acquired re-encryption key, and

means (31) for transmitting the second encrypted symmetric key portion obtained by the re-encryption to the file sharing apparatus,

wherein the client apparatus obtains the data by obtaining the symmetric key by decrypting the second encrypted symmetric key portion from the file sharing apparatus based on a private key corresponding to the public key of the member, and decrypting the encrypted data portion from the file sharing apparatus based on the obtained symmetric key.

4. The re-encryption apparatus according to Claim 3, wherein the first processing, the second processing, the third processing, the encrypted data transmission processing, and the fourth processing are executed by using a filter function which adds predetermined processing.

5. A program stored in a non-transitory computer-readable storage medium (M3) and executed by a processor of a re-encryption apparatus (30) including re-encryption key storage means and communicable with a file sharing apparatus (10) which is communicable with the client apparatus (20) operated by a member belonging to a group, stores, in a memory, an encrypted file including a first encrypted symmetric key portion~~file~~ obtained by encrypting a symmetric key~~file~~ based on a public key of the group and an encrypted data portion obtained by encrypting data based on the symmetric key, executes first processing which acquires, upon receiving a file request including a member ID for identifying the member and a file name of the ~~first~~ encrypted file from the client apparatus, the ~~first~~ encrypted file from the memory based on the file name included in the file request, executes second processing which separates the acquired encrypted file into the first encrypted symmetric key portion and the encrypted data portion, executes third processing which transmits a re-encryption request including the ~~acquired~~ first encrypted symmetric key portion~~file~~ and the member ID included in the file request to the re-encryption apparatus simultaneously with encrypted data transmission processing which transmits the separated encrypted data portion to the client apparatus, and executes fourth processing which transmits, upon receiving a second encrypted symmetric key portion~~file~~

obtained by encrypting the symmetric key portion~~file~~ based on the public key of the member ID from the re-encryption apparatus simultaneously with the encrypted data transmission processing, the second encrypted symmetric key portion~~file~~ to the client apparatus after the encrypted data transmission processing, the program comprising:

a first program code for causing the processor to execute processing of writing the member ID for identifying the member and a re-encryption key for re-encrypting, without decrypting, the first encrypted symmetric key portion~~file~~ to the second encrypted symmetric key portion~~file~~ in the re-encryption key storage means (35) in association with each other;

a second program code (33) for causing the processor to execute processing of acquiring, upon receiving the re-encryption request from the file sharing apparatus, the re-encryption key from the re-encryption key storage means based on the member ID included in the re-encryption request;

a third program code (33) for causing the processor to execute processing of re-encrypting the first encrypted symmetric key portion~~file~~ included in the re-encryption request to the second encrypted symmetric key portion~~file~~ based on the acquired re-encryption key; and

a fourth program code (31) for causing the processor to execute processing of transmitting the second encrypted symmetric key portion~~file~~ obtained by the re-encryption to the file sharing apparatus,

wherein the client apparatus obtains the data by obtaining the symmetric key~~file~~ by decrypting the second encrypted symmetric key portion~~file~~ from the file sharing apparatus based on a private key corresponding to the public key of the member, and decrypting the encrypted data

portion from the file sharing apparatus based on the obtained symmetric key.

6. The re-encryption apparatus according to Claim 5, wherein the first processing, the second processing, the third processing, the encrypted data transmission processing, and the fourth processing are executed by using a filter function which adds predetermined processing.