

CLAIMS

1. A re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted without decryption, the re-encryption key generator comprising:

a first storage means (31) that stores a first private key corresponding to the first public key;

a second storage means (32) that stores a second re-encryption key generation key of the second user device that is different from a second public key corresponding to the second private key; and

a re-encryption key generation means (34) that generates the re-encryption key based on the first private key and the second re-encryption key generation key.

2. The re-encryption key generator according to claim 1, wherein

the first public key is generated based on the first private key and a plurality of system fixed values and

the second public key is generated based on the second private key and the plurality of system fixed values.

3. The re-encryption key generator according to claim 2, wherein

when the first private key is represented by $sk_i=(x_i, y_i, z_i)$, the second private key is represented by $sk_j=(x_j, y_j, z_j)$, the plurality of system fixed values are represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when bilinear map groups as groups of an order p for which a

bilinear map $e:G \times G \rightarrow G_T$ exists are represented by G, G_T), and the first public key is represented by pk_i , the first public key pk_i contains data X_i, Y_{1i}, Z_i, Z_{1i} (where

[Equation 1]

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$$

),

when the second public key is represented by pk_j , the second public key pk_j contains data X_j, Y_{1j}, Z_j, Z_{1j} (where

[Equation 2]

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$$

),

when a random number related to the second re-encryption key generation key is represented by π , a value based on the random number π and the system fixed value g is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3 = g^\pi$, $g_4 = g_1^\pi$, and $g_5 = g_2^\pi$), and the second re-encryption key generation key is

represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

[Equation 3]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is represented by r , and the ciphertext data is represented by

C_i (where the bilinear map $e:G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains data $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3$ (where

[Equation 4]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_3 = e(g_4 g_5, g)^r \cdot m.$$

),

when the random number related to the re-encryption key is represented by θ , an exponent related to the system fixed values g, g_2 is represented by β (where $g_2 = g^\beta$), and the re-encryption key is represented by R_{ij} ,

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

holds (where

[Equation 5]

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}$$

),

when the re-encrypted data is represented by C_j (where three random numbers are represented by s, t, k), the re-

encrypted data C_j includes data C_{2X}'' , C_{2Y}'' , C_{2Z}'' , C_{2Z1}'' ,
 C_{5X} , C_{5Y} , C_{5Z} , C_3 (where
 [Equation 6]

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

), and

the plaintext data m , the re-encrypted data C_j , and
 the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

4. The re-encryption key generator according to
 claim 2, wherein

when the first private key is represented by
 $sk_i = (x_i, y_i, z_i, w_i)$, the second private key is represented by
 $sk_j = (x_j, y_j, z_j, w_j)$, the plurality of system fixed values are
 represented by g , g_1 , and g_2 (where $g, g_1, g_2 \in G$ when
 bilinear map groups as groups of an order p for which a

bilinear map $e:G \times G \rightarrow G_T$ exists are represented by G, G_T), and the first public key is represented by pk_i , the first public key pk_i contains data $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ (where [Equation 7]

$$\begin{aligned} X_i &= g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, \\ Z_{1i} &= g_1^{z_i}, W_i = g^{w_i} \end{aligned}$$

),

when the second public key is represented by pk_j , the second public key pk_j contains data $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$ (where [Equation 8]

$$\begin{aligned} X_j &= g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, \\ Z_{1j} &= g_1^{z_j}, W_j = g^{w_j} \end{aligned}$$

),

when a random number related to the second re-encryption key generation key is represented by π , a value based on the random number π and the system fixed value g is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3=g^\pi$, $g_4=g_1^\pi$, and $g_5=g_2^\pi$), and the second re-encryption key generation key is represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

[Equation 9]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is represented by r , a multiplicative group for the order p is represented by Z_p^* , a time parameter showing a period of updating the re-encryption key is represented by L , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data

10 C_i contains $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3$ (where [Equation 10]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_{2F} = F_i(L)^r, C_3 = e(g_4 g_5, g)^r \cdot m.$$

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in Z_p^*)$$

15),

when three random numbers related to the re-encryption key are represented by $\theta, \delta_x, \delta_y$, an exponent related to the system fixed values g, g_1 is represented by α , the exponent related to the system fixed values g, g_2 is represented by β (where $g_1 = g^\alpha$ and $g_2 = g^\beta$), and the re-encryption key is represented by R_{ijL} ,

20

$$R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$$

holds (where

[Equation 11]

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i\delta_x}, R_{ijL5} = g^{y_i\delta_y} = g^{\alpha y_i\delta_y}$$

),

when the re-encrypted data is represented by C_j (where four random numbers are represented by s, t, k, h), the re-encrypted data C_j contains data C_{2X}'' , C_{2Y}'' , C_{2Z}'' , C_{2Z1}'' , C_{2F}'' , C_{5X} , C_{5Y} , C_{5Z} , C_{5FX} , C_{5FY} , C_3 (where [Equation 12]

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{2F}'' = C_{2F}^h = F_i(L)^{rh},$$

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

5

5. A program executed by a processor of a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium (M3), the program comprising:

15

a first program code causing the processor to perform processing (33) to write a first private key corresponding to the first public key into a first storage means (31) of the re-encryption key generator;

20

a second program code causing the processor to perform the processing (33) to write a second re-encryption key generation key of the second user device that is different from a second public key corresponding to the second private key into a second storage means (32) of the re-encryption key generator; and

25

a third program code causing the processor to perform processing (34) to generate the re-encryption key based on

the first private key and the second re-encryption key generation key.

5 6. The program according to claim 5, wherein
the first public key is generated based on the first private key and a plurality of system fixed values and
the second public key is generated based on the second private key and the plurality of system fixed values.

10 7. The program according to claim 6, wherein
when the first private key is represented by $sk_i=(x_i, y_i, z_i)$, the second private key is represented by $sk_j=(x_j, y_j, z_j)$, the plurality of system fixed values are represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when
15 bilinear map groups as groups of an order p for which a bilinear map $e:G \times G \rightarrow G_T$ exists are represented by G, G_T), and the first public key is represented by pk_i , the first public key pk_i contains data X_i, Y_{1i}, Z_i, Z_{1i} (where
[Equation 13])

20
$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$$

),

when the second public key is represented by pk_j , the second public key pk_j contains data X_j, Y_{1j}, Z_j, Z_{1j} (where
[Equation 14])

25
$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$$

),

when a random number related to the second re-encryption key generation key is represented by n , a value based on the random number n and the system fixed value g

is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3=g^\pi$, $g_4=g_1^\pi$, and $g_5=g_2^\pi$), and the second re-encryption key generation key is represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

[Equation 15]

$$X_{3j} = g_3^{X_j}, Y_{5j} = g_5^{Y_j}$$

),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is represented by r , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains data $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3$ (where

[Equation 16]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_3 = e(g_4 g_5, g)^r \cdot m$$

),

when the random number related to the re-encryption key is represented by θ , an exponent related to the system fixed values g, g_2 is represented by β (where $g_2=g^\beta$), and the re-encryption key is represented by R_{ij} ,

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

holds (where

[Equation 17]

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j+\theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j+\theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}}$$

),

5 when the re-encrypted data is represented by C_j (where three random numbers are represented by s, t, k), the re-encrypted data C_j includes data $C_{2X}''', C_{2Y}''', C_{2Z}''', C_{2Z1}'''$, $C_{5X}, C_{5Y}, C_{5Z}, C_3$ (where [Equation 18]

$$10 \quad C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

15), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

5 8. The program according to claim 6, wherein
when the first private key is represented by
 $sk_i=(x_i, y_i, z_i, w_i)$, the second private key is represented by
 $sk_j=(x_j, y_j, z_j, w_j)$, the plurality of system fixed values is
represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when
10 bilinear map groups as groups of an order p for which a
bilinear map $e:G \times G \rightarrow G_T$ exists are represented by G, G_T), and
the first public key is represented by pk_i , the first
public key pk_i contains data $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ (where
[Equation 19]

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i},$$
$$15 \quad Z_{1i} = g_1^{z_i}, W_i = g^{w_i}$$

),

when the second public key is represented by pk_j , the
second public key pk_j contains data $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$
(where
20 [Equation 20]

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, \\ Z_{1j} = g_1^{z_j}, W_j = g^{w_j}$$

),

when a random number related to the second re-encryption key generation key is represented by π , a value based on the random number π and the system fixed value g is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3=g^\pi$, $g_4=g_1^\pi$, and $g_5=g_2^\pi$), and the second re-encryption key generation key is represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

[Equation 21]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is represented by r , a multiplicative group for the order p is represented by Z_p^* , a time parameter showing a period of updating the re-encryption key is represented by L , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3$ (where

[Equation 22]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_{2F} = F_i(L)^r, C_3 = e(g_4g_5, g)^r \cdot m.$$

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

),

when three random numbers related to the re-encryption
key are represented by $\theta, \delta_x, \delta_y$, an exponent related to
the system fixed values g, g_1 is represented by α , the
exponent related to the system fixed values g, g_2 is
represented by β (where $g_1=g^\alpha$ and $g_2=g^\beta$), and the re-
encryption key is represented by R_{ijL} ,

$$R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$$

holds (where

[Equation 23]

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i\delta_x}, R_{ijL5} = g_1^{y_i\delta_y} = g^{\alpha y_i\delta_y}$$

),

when the re-encrypted data is represented by C_j (where
four random numbers are represented by s, t, k, h), the re-

encrypted data C_j contains data C_{2X}'' , C_{2Y}'' , C_{2Z}'' , C_{2Z1}'' , C_{2F}'' , C_{5X} , C_{5Y} , C_{5Z} , C_{5FX} , C_{5FY} , C_3 (where
[Equation 24]

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{2F}'' = C_{2F}^h = F_i(L)^{rh},$$

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{z_j}} \right\}$$

15

9. A re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data

by a public key for encryption of a first user device is re-encrypted without decryption, the re-encryption key generator comprising:

5 a first storage means (31) that stores a first private key corresponding to the public key for encryption;

 a second storage means (32) that stores public information for generating a re-encryption key corresponding to the second private key;

10 a first random number generation means (36) that generates a first random number; and

 a re-encryption key generation means (34) that generates the re-encryption key based on the first private key, the public information for generating a re-encryption key, and the first random number.

15 10. The re-encryption key generator according to claim 9, wherein

 the re-encryption key generation means generates the re-encryption key based on the first private key, the public information for generating a re-encryption key, and the first random number independently of ciphertext data before re-encryption.

25 11. The re-encryption key generator according to claim 9, wherein

 the public key for encryption is generated based on the first private key and a plurality of system fixed values and

30 the public information for generating a re-encryption key is generated based on the second private key and the plurality of system fixed values.

12. The re-encryption key generator according to claim 11, wherein

when the first private key is represented by $sk_i=(x_i, y_i, z_i)$, the second private key is represented by $sk_j=(x_j, y_j, z_j)$, the first random number is represented by γ , the plurality of system fixed values are represented by g, g_1, g_2, g_3, g_4 (where $g, g_1, g_2, g_3, g_4 \in G$ when bilinear map groups as groups of an order p for which a bilinear map $e:G \times G \rightarrow G_T$ exists are represented by G, G_T), exponents related to the system fixed values are represented by α, β, ξ (where $g_1=g^\alpha, g_2=g^\beta, g_3=g^\xi$, and $g_4=g^{\alpha\xi}$), and the re-encryption key is represented by R_{ij} ,

[Equation 25]

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

holds (where

[Equation 26]

$$R_{ij1} = g^{\frac{\xi x_j + \gamma}{x_i}}, R_{ij2} = g^{\frac{\beta y_j + \gamma}{y_i}}, R_{ij3} = g^{\frac{\xi x_j + \beta y_j + \gamma}{z_i}}$$

),

when the public key for encryption of the first user device is represented by pk_i ,

[Equation 27]

$$pk_i = (X_i, Y_{1i}, Z_i, Z_{1i})$$

holds (where

[Equation 28]

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$$

),

when the public information for generating a re-encryption key corresponding to the first private key is represented by pi_i ,

[Equation 29]

$$pi_i = (X_{3i}, Y_{2i})$$

holds (where

[Equation 30]

$$X_{3i} = g^{x_i}, Y_{2i} = g_2^{y_i}$$

),

when the public key for encryption of the second user device is represented by pk_j ,

[Equation 31]

$$pk_j = (X_j, Y_{1j}, Z_j, Z_{1j})$$

holds (where

[Equation 32]

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$$

),

when the public information for generating a re-encryption key corresponding to the second private key is represented by pi_j ,

[Equation 33]

$$pi_j = (X_{3j}, Y_{2j})$$

5

holds (where

[Equation 34]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

),

10

when the plaintext data is represented by m (where $m \in G_T$), a second random number is represented by r , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(g, h)$ (where $g, h \in G$)),

$$C_i = (C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)$$

15

holds (where

[Equation 35]

$$C_{2X} = X_i^r, C_{2Y} = Y_{li}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{li}^r, C_3 = e(g_2 g_4, g)^r \cdot m$$

),

20

when the re-encrypted data is represented by C_j (where third to fifth random numbers are represented by s, t, k),

$$C_j = (C_{2X}''', C_{2Y}''', C_{2Z}''', C_{2Z1}''', C_{5X}, C_{5Y}, C_{5Z}, C_3)$$

holds (where

[Equation 36]

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

[Equation 37]

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

13. A program executed by a processor of a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-

transitory computer-readable storage medium (M3), the program comprising:

5 a first program code causing the processor to perform processing to write a first private key corresponding to the public key for encryption into a first storage means (31) of the re-encryption key generator;

10 a second program code causing the processor to perform the processing to write public information for generating a re-encryption key corresponding to the second private key into a second storage means (32) of the re-encryption key generator;

a third program code causing the processor to perform processing (36) to generate a first random number; and

15 a fourth program code causing the processor to perform processing (34) to generate the re-encryption key based on the first private key, the public information for generating a re-encryption key, and the first random number.

20 14. The program according to claim 13, wherein

the processor is caused to perform the processing to generate the re-encryption key independently of the ciphertext data before re-encryption.

C L A I M S

1. A re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted without decryption, the re-encryption key generator comprising:

5 a first storage means (31) that stores a first private key corresponding to the first public key;

10 a second storage means (32) that stores a second re-encryption key generation key of the second user device that is different from a second public key corresponding to the second private key; and

15 a re-encryption key generation means (34) that generates the re-encryption key based on the first private key and the second re-encryption key generation key.

2. The re-encryption key generator according to claim 1, wherein

20 the first public key is generated based on the first private key and a plurality of system fixed values and

the second public key is generated based on the second private key and the plurality of system fixed values.

25 3. The re-encryption key generator according to claim 2, wherein

when the first private key is represented by $sk_1=(x_1, y_1, z_1)$, the second private key is represented by

$sk_j = (x_j, y_j, z_j)$, the plurality of system fixed values are represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when bilinear map groups as groups of an order p for which a bilinear map $e: G \times G \rightarrow G_T$ exists are represented by G, G_T), and the first public key is represented by pk_i , the first public key pk_i contains data X_i, Y_{1i}, Z_i, Z_{1i} (where $X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$),

when the second public key is represented by pk_j , the second public key pk_j contains data X_j, Y_{1j}, Z_j, Z_{1j} (where $X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$),

when a random number related to the second re-encryption key generation key is represented by π , a value based on the random number π and the system fixed value g is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3 = g^\pi, g_4 = g_1^\pi$, and $g_5 = g_2^\pi$), and the second re-encryption key generation key is represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

),

when the plaintext data is represented by m (where

$m \in G_T$), the random number related to the ciphertext data is represented by r , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains data $C_{2X}, C_{2Y}, C_{2Z},$
5 C_{2Z1}, C_3 (where

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_5, g)^r \cdot m.$$

),

when the random number related to the re-encryption
10 key is represented by θ , an exponent related to the system fixed values g, g_2 is represented by β (where $g_2 = g^\beta$), and the re-encryption key is represented by R_{ij} ,

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

holds (where

15

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}$$

),

when the re-encrypted data is represented by C_j (where
20 three random numbers are represented by s, t, k), the re-encrypted data C_j includes data $C_{2X}'', C_{2Y}'', C_{2Z}'', C_{2Z1}'',$

$C_{5X}, C_{5Y}, C_{5Z}, C_3$ (where

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

5

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

10

4. The re-encryption key generator according to claim 2, wherein

when the first private key is represented by

$sk_i = (x_i, y_i, z_i, w_i)$, the second private key is represented by

15

$sk_j = (x_j, y_j, z_j, w_j)$, the plurality of system fixed values are

represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when

bilinear map groups as groups of an order p for which a

bilinear map $e: G \times G \rightarrow G_T$ exists are represented by G, G_T), and

the first public key is represented by pk_i , the first

20

public key pk_i contains data $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ (where

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i},$$

$$Z_{1i} = g_1^{z_i}, W_i = g^{w_i}$$

),

when the second public key is represented by pk_j , the second public key pk_j contains data $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$

5 (where

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j},$$

$$Z_{1j} = g_1^{z_j}, W_j = g^{w_j}$$

),

when a random number related to the second re-encryption key generation key is represented by π , a value based on the random number π and the system fixed value g is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3 = g^\pi$, $g_4 = g_1^\pi$, and $g_5 = g_2^\pi$), and the second re-encryption key generation key is represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

20),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is

represented by r , a multiplicative group for the order p is represented by $\mathbb{Z}_p^*$, a time parameter showing a period of updating the re-encryption key is represented by L , and the ciphertext data is represented by C_i (where the bilinear map $e:G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 (where

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_{2F} = F_i(L)^r, C_3 = e(g_4 g_5, g)^r \cdot m$$

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

10),

when three random numbers related to the re-encryption key are represented by θ , δ_x , δ_y , an exponent related to the system fixed values g , g_1 is represented by α , the exponent related to the system fixed values g , g_2 is represented by β (where $g_1 = g^\alpha$ and $g_2 = g^\beta$), and the re-encryption key is represented by R_{ijL} ,

$$R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$$

holds (where

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i \delta_x}, R_{ijL5} = g_1^{y_i \delta_y} = g^{\alpha y_i \delta_y}$$

),

when the re-encrypted data is represented by C_j (where four random numbers are represented by s, t, k, h), the re-encrypted data C_j contains data C_{2X}'' , C_{2Y}'' , C_{2Z}'' , C_{2Z1}'' ,

C_{2F}'' , C_{5X} , C_{5Y} , C_{5Z} , C_{5FX} , C_{5FY} , C_3 (where

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{2F}'' = C_{2F}^h = F_i(L)^{rh},$$

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

5. A re-encryption device (40) to obtain re-encrypted

data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted by a re-encryption key without decryption, the re-encryption device comprising:

a storage means (41) that stores the re-encryption key generated by a re-encryption key generator in advance and

a re-encryption means (44) that obtains the re-encrypted data by re-encrypting the ciphertext data by the re-encryption key in the storage means without decrypting the ciphertext data, wherein

the re-encryption key is generated based on a second re-encryption key generation key of the second user device that is different from a first private key corresponding to the first public key and a second public key corresponding to the second private key.

6. An encryption device (20) that generates ciphertext data for a re-encryption device to obtain re-encrypted data that can be decrypted by a second private key of a second user device after the ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted by a re-encryption key without decryption, the encryption device comprising:

a storage means (21) that stores the first public key and

an encryption means (24) that obtains the ciphertext data by encrypting the plaintext data using the

first public key in the storage means, wherein

5 the re-encryption key is generated based on a second re-encryption key generation key of the second user device that is different from a first private key corresponding to the first public key and a second public key corresponding to the second private key.

10 7. A decryption device (50) that decrypts re-encrypted data after obtaining the re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted by a re-encryption device based on a re-encryption key without decryption, the decryption device comprising:

15 a storage means (51) that stores the second private key and

 a decryption means (54) that obtains the plaintext data by decrypting the re-encrypted data based on the second private key in the storage means, wherein

20 the re-encryption key is generated based on a second re-encryption key generation key of the second user device that is different from a first private key corresponding to the first public key and a second public key corresponding to the second private key.

25 8. A program executed by a processor of a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be

decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium (M3), the program
5 comprising:

a first program code causing the processor to perform processing (33) to write a first private key corresponding to the first public key into a first storage means (31) of
10 the re-encryption key generator;

a second program code causing the processor to perform the processing (33) to write a second re-encryption key generation key of the second user device that is different from a second public key corresponding to the second
15 private key into a second storage means (32) of the re-encryption key generator; and

a third program code causing the processor to perform processing (34) to generate the re-encryption key based on the first private key and the second re-encryption key
20 generation key.

9. The program according to claim 8, wherein
the first public key is generated based on the first private key and a plurality of system fixed values and
the second public key is generated based on the second
25 private key and the plurality of system fixed values.

10. The program according to claim 9, wherein
when the first private key is represented by

$sk_i = (x_i, y_i, z_i)$, the second private key is represented by
 $sk_j = (x_j, y_j, z_j)$, the plurality of system fixed values are
 represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when
 bilinear map groups as groups of an order p for which a
 5 bilinear map $e: G \times G \rightarrow G_T$ exists are represented by G, G_T), and
 the first public key is represented by pk_i , the first
 public key pk_i contains data X_i, Y_{1i}, Z_i, Z_{1i} (where

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$$

10 when the second public key is represented by pk_j , the
 second public key pk_j contains data X_j, Y_{1j}, Z_j, Z_{1j} (where

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$$

when a random number related to the second re-
 15 encryption key generation key is represented by n , a value
 based on the random number n and the system fixed value g
 is represented by g_3 , the value based on the random number
 n and the system fixed value g_1 is represented by g_4 , the
 value based on the random number n and the system fixed
 20 value g_2 is represented by g_5 (where $g_3 = g^n$, $g_4 = g_1^n$, and
 $g_5 = g_2^n$), and the second re-encryption key generation key is
 represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is represented by r , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains data C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_3 (where

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_5, g)^r \cdot m.$$

10),

when the random number related to the re-encryption key is represented by θ , an exponent related to the system fixed values g , g_2 is represented by β (where $g_2 = g^\beta$), and the re-encryption key is represented by R_{ij} ,

15 $R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$

holds (where

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}$$

20),

when the re-encrypted data is represented by C_j (where

three random numbers are represented by s, t, k), the re-encrypted data C_j includes data $C_{2X}''', C_{2Y}''', C_{2Z}''', C_{2Z1}'''$,

$C_{5X}, C_{5Y}, C_{5Z}, C_3$ (where

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

11. The program according to claim 9, wherein

when the first private key is represented by

$sk_i = (x_i, y_i, z_i, w_i)$, the second private key is represented by

$sk_j = (x_j, y_j, z_j, w_j)$, the plurality of system fixed values is

represented by g, g_1 , and g_2 (where $g, g_1, g_2 \in G$ when

bilinear map groups as groups of an order p for which a

bilinear map $e: G \times G \rightarrow G_T$ exists are represented by G, G_T), and

the first public key is represented by pk_i , the first

public key pk_i contains data $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ (where

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i},$$

$$Z_{1i} = g_1^{z_i}, W_i = g^{w_i}$$

),

when the second public key is represented by pk_j , the second public key pk_j contains data $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$

5 (where

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j},$$

$$Z_{1j} = g_1^{z_j}, W_j = g^{w_j}$$

),

when a random number related to the second re-encryption key generation key is represented by π , a value based on the random number π and the system fixed value g is represented by g_3 , the value based on the random number π and the system fixed value g_1 is represented by g_4 , the value based on the random number π and the system fixed value g_2 is represented by g_5 (where $g_3 = g^\pi$, $g_4 = g_1^\pi$, and
15 $g_5 = g_2^\pi$), and the second re-encryption key generation key is represented by rk_j ,

$$rk_j = (X_{3j}, Y_{5j})$$

holds (where

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

20),

when the plaintext data is represented by m (where $m \in G_T$), the random number related to the ciphertext data is

represented by r , a multiplicative group for the order p is represented by $\mathbb{Z}_p^*$, a time parameter showing a period of updating the re-encryption key is represented by L , and the ciphertext data is represented by C_i (where the bilinear map $e:G \times G \rightarrow G_T$ is represented by $e(,)$), the ciphertext data C_i contains C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 (where

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_{2F} = F_i(L)^r, C_3 = e(g_4 g_5, g)^r \cdot m,$$

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

10),

when three random numbers related to the re-encryption key are represented by θ , δ_x , δ_y , an exponent related to the system fixed values g , g_1 is represented by α , the exponent related to the system fixed values g , g_2 is represented by β (where $g_1 = g^\alpha$ and $g_2 = g^\beta$), and the re-encryption key is represented by R_{ijL} ,

$$R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$$

holds (where

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i \delta_x}, R_{ijL5} = g^{y_i \delta_y} = g^{\alpha y_i \delta_y}$$

),

when the re-encrypted data is represented by C_j (where four random numbers are represented by s, t, k, h), the re-encrypted data C_j contains data $C_{2X}''', C_{2Y}''', C_{2Z}''', C_{2Z1}'''$,

$C_{2F}''', C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3$ (where

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{2F}'' = C_{2F}^h = F_i(L)^{rh},$$

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

12. A program executed by a processor of a re-

encryption device (40) to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted by a re-encryption key without decryption and stored in a non-transitory computer-readable storage medium (M4), the program comprising:

a first program code causing the processor to perform processing (43) to write the re-encryption key generated by a re-encryption key generator in advance into a storage means (41) of the re-encryption device; and

a second program code causing the processor to perform processing (44) to obtain the re-encrypted data by re-encrypting the ciphertext data by the re-encryption key in the storage means without decrypting the ciphertext data, wherein

the re-encryption key is generated based on a second re-encryption key generation key of the second user device that is different from a first private key corresponding to the first public key and a second public key corresponding to the second private key.

13. A program executed by a processor of an encryption device (20) that generates ciphertext data for a re-encryption device (40) to obtain re-encrypted data that can be decrypted by a second private key of a second user device after the ciphertext data obtained by encrypting plaintext data by a first public key of a first user device

is re-encrypted by a re-encryption key without decryption and stored in a non-transitory computer-readable storage medium (M2), the program comprising:

5 a first program code causing the processor to perform processing (22) to write the first public key into a storage means (21) of the encryption device; and

10 a second program code causing the processor to perform processing (24) to obtain the ciphertext data by encrypting the plaintext data using the first public key in the storage means, wherein

the re-encryption key is generated based on a second re-encryption key generation key of the second user device that is different from a first private key corresponding to the first public key and a second public key corresponding to the second private key.

15 14. A program executed by a processor of a decryption device (50) that decrypts re-encrypted data after obtaining the re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a first public key of a first user device is re-encrypted by a re-encryption device (40) based on a re-encryption key without decryption and stored in a non-transitory computer-readable storage medium (M5), the decryption device comprising:

25 a first program code causing the processor to perform processing (53) to write the second private key into a storage means (51) of the decryption device; and

a second program code causing the processor to perform processing (54) to obtain the plaintext data by decrypting the re-encrypted data based on the second private key in the storage means, wherein

5 the re-encryption key is generated based on a second re-encryption key generation key of the second user device that is different from a first private key corresponding to the first public key and a second public key corresponding to the second private key.

10 15. A re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is
15 re-encrypted without decryption, the re-encryption key generator comprising:

 a first storage means (31) that stores a first private key corresponding to the public key for encryption;

20 a second storage means (32) that stores public information for generating a re-encryption key corresponding to the second private key;

 a first random number generation means (36) that generates a first random number; and

25 a re-encryption key generation means (34) that generates the re-encryption key based on the first private key, the public information for generating a re-encryption key, and the first random number.

16. The re-encryption key generator according to claim 15, wherein

the re-encryption key generation means generates the re-encryption key based on the first private key, the public information for generating a re-encryption key, and the first random number independently of ciphertext data before re-encryption.

17. The re-encryption key generator according to claim 15, wherein

the public key for encryption is generated based on the first private key and a plurality of system fixed values and

the public information for generating a re-encryption key is generated based on the second private key and the plurality of system fixed values.

18. The re-encryption key generator according to claim 16, wherein

when the first private key is represented by $sk_i=(x_i, y_i, z_i)$, the second private key is represented by $sk_j=(x_j, y_j, z_j)$, the first random number is represented by γ , the plurality of system fixed values are represented by g, g_1, g_2, g_3, g_4 (where $g, g_1, g_2, g_3, g_4 \in G$ when bilinear map groups as groups of an order p for which a bilinear map $e: G \times G \rightarrow G_T$ exists are represented by G, G_T), exponents related to the system fixed values are represented by α, β, ξ (where $g_1=g^\alpha, g_2=g^\beta, g_3=g^\xi$, and $g_4=g^{\alpha\xi}$), and the re-encryption key is represented by R_{ij} ,

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

holds (where

$$R_{ij1} = g^{\frac{\xi x_j + \gamma}{x_i}}, R_{ij2} = g^{\frac{\beta y_j + \gamma}{y_i}}, R_{ij3} = g^{\frac{\xi x_j + \beta y_j + \gamma}{z_i}}$$

),

5 when the public key for encryption of the first user device is represented by pk_i ,

$$pk_i = (X_i, Y_{1i}, Z_i, Z_{1i})$$

holds (where

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$$

10),

when the public information for generating a re-encryption key corresponding to the first private key is represented by pi_i ,

$$pi_i = (X_{3i}, Y_{2i})$$

15 holds (where

$$X_{3i} = g_3^{x_i}, Y_{2i} = g_2^{y_i}$$

),

when the public key for encryption of the second user device is represented by pk_j ,

$$pk_j = (X_j, Y_{1j}, Z_j, Z_{1j})$$

holds (where

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$$

),

5 when the public information for generating a re-encryption key corresponding to the second private key is represented by pi_j ,

$$pi_j = (X_{3j}, Y_{2j})$$

holds (where

$$X_{3j} = g^{x_j}, Y_{2j} = g_2^{y_j}$$

10

),

when the plaintext data is represented by m (where $m \in G_T$), a second random number is represented by r , and the ciphertext data is represented by C_i (where the bilinear map $e: G \times G \rightarrow G_T$ is represented by $e(g, h)$ (where $g, h \in G$)),

15

$$C_i = (C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)$$

holds (where

$$C_{2X} = X_i^r, C_{2Y} = Y_{li}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{li}^r, C_3 = e(g_2 g_4, g)^r \cdot m$$

),

20 when the re-encrypted data is represented by C_j (where third to fifth random numbers are represented by s, t, k),

$$C_j = (C_{2X}''', C_{2Y}''', C_{2Z}''', C_{2Z1}''', C_{5X}, C_{5Y}, C_{5Z}, C_3)$$

holds (where

$$C_{2X}'' = C_{2X}^s = X_i^{rs},$$

$$C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk},$$

$$C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

), and

the plaintext data m , the re-encrypted data C_j , and the second private key sk_j are related by

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

19. A re-encryption device (40) capable of communicating with a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption, the re-encryption device comprising:

a storage means (41) that stores the re-encryption key received from the re-encryption key generator;

a re-encryption means (44) that obtains the re-

encrypted data by re-encrypting the ciphertext received from the first user device without decryption by the re-encryption key in the storage means; and

5 a means (43) that transmits the obtained re-encrypted data to the second user device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a re-encryption key corresponding to the second private key, and a first random
10 number generated by the re-encryption key generator.

20. A program executed by a processor of a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device
15 after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium (M3), the program comprising:

20 a first program code causing the processor to perform processing to write a first private key corresponding to the public key for encryption into a first storage means (31) of the re-encryption key generator;

25 a second program code causing the processor to perform the processing to write public information for generating a re-encryption key corresponding to the second private key into a second storage means (32) of the re-encryption key generator;

30 a third program code causing the processor to perform processing (36) to generate a first random number; and

a fourth program code causing the processor to perform processing (34) to generate the re-encryption key based on the first private key, the public information for

generating a re-encryption key, and the first random number.

21. A program executed by a processor of a re-encryption device (40) capable of communicating with a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium, the program comprising:

a first program code causing the processor to perform processing to write the re-encryption key received from the re-encryption key generator into a storage means (41) of the re-encryption device;

a second program code causing the processor to perform processing (44) to obtain the re-encrypted data by re-encrypting the ciphertext data received from the first user device by the re-encryption key in the storage means without decryption; and

a third program code causing the processor to perform processing (43) to transmit the obtained re-encrypted data to the second user device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a second re-encryption key corresponding to the second private key, and a first random number generated by the re-encryption key generator.

22. A program executed by a processor of an encryption device (20) capable of communicating with a re-encryption device (40) that uses a re-encryption key to obtain re-encrypted data that can be decrypted by a second

private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium (M2), the program comprising:

a first program code causing the processor to perform processing (22) to write the public key for encryption into a storage means (21) of the encryption device;

a second program code causing the processor to perform processing (24) to obtain the ciphertext data by encrypting the plaintext data using the public key for encryption in the storage means; and

a third program code causing the processor to perform processing (22) to transmit the obtained ciphertext data to the re-encryption device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a re-encryption key corresponding to the second private key, and a first random number generated by a re-encryption key generator that generates the re-encryption key.

23. A program executed by a processor of a decryption device (50) that decrypts re-encrypted data obtained from the re-encryption device after obtaining the re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted by a re-encryption device (40) based on a re-encryption key without decryption and stored in a non-transitory computer-readable storage medium (M5), the program comprising:

a first program code causing the processor to perform processing (53) to write the second private key into a storage means (51) of the decryption device; and

5 a second program code causing the processor to perform processing (54) to obtain the plaintext data by decrypting the re-encrypted data based on the second private key in the storage means after receiving the re-encrypted data from the re-encryption device, wherein

10 the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a re-encryption key corresponding to the second private key, and a first random number generated by a re-encryption key generator that generates the re-encryption key.

15