C L A I M S

1. A re-encryption key generator (30), which generates a re-encryption key required to obtain re-encrypted text data, which is configured to be decrypted by means of a second private key of a second user device, by re-encrypting, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first public key of a first user device, the generator characterized by comprising:

first storage means (31) for storing a first private key corresponding to the first public key;

second storage means (32) for storing a second public key corresponding to the second private key;

first random number generation means (36) for generating a first random number; and

re-encryption key generation means (34) for generating the re-encryption key based on the first private key, the second public key, and the first random number,

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

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

the re-encryption key includes a power index which consists of a numerator portion and a denominator portion,

the numerator portion of the power index of the re-encryption key has a form of linear coupling based on a power index related to the respective system fixed values, the second private key corresponding to the second public key, and the first random number,

the denominator portion of the power index of the re-encryption key consists of the first private key,

the ciphertext data is generated based on the first public key and the second random number, and

the re-encrypted text data is generated based on the ciphertext data, the re-encryption key, a third random number, a fourth random number, and a fifth random number.

2. The re-encryption key generator of claim 1, characterized in that the re-encryption key generation means (34) generates the re-encryption key based on the first private key, the second public key, and the first random number independently of ciphertext data before re-encryption.

~~3. The re-encryption key generator of claim 1, characterized in that 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.~~

34. The re-encryption key generator of claim 2, characterized in that 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 θ, the plurality of system fixed value are represented by g, g_1, and g_2 (for g, g_1, and $g_2 \in G$ if bilinear map groups as groups of prime orders p including a bilinear map $e: G \times G \rightarrow G_1$ are represented by G and G_T), letting β be thea power index related to the respective system fixed values (for $g_2 = g^{\beta}$), and R_{ij} be the re-encryption key, the re-encryption key R_{ij} is described by:

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

(for

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

),

when the first public key is represented by pk_i, the first public key pk_i is described by:

$$pk_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i})$$

(for

$$X_i = g^{x_i}, Y_{1i} = g_1{}^{y_i}, Y_{2i} = g_2{}^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1{}^{z_i}$$

),

when the second public key is represented by pk_j, the first public key pk_j is described by:

$$pk_j = \left(X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j}\right)$$

(for

$$X_j = g^{xj}, Y_{1j} = g_1^{yj}, Y_{2j} = g_2^{yj}, Z_j = g^{zj}, Z_{1j} = g_1^{zj}$$

),

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

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

(for

$$C_{2X} = X_i^r,\ C_{2Y} = Y_{1i}^r,\ C_{2Z} = Z_i^r,\ C_{2Z1} = Z_{1i}^r,\ C_3 = e(g_1 g_2, g)^r \cdot m$$

),

when the re-encrypted text data is represented by C_j (the third random number, the fourth random number, and the fifth random numbers are represented by s, t, and k), the re-encrypted text data C_j is described by:

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

(for

$$C_{2X}'' = C_{2X}{}^{s} = X_i{}^{rs}, \quad C_{2Y}'' = C_{2Y}{}^{t} = Y_{1i}{}^{rt}, \quad C_{2Z}'' = C_{2Z}{}^{k} = Z_i{}^{rk}, \quad C_{2Z1}'' = C_{2Z1}{}^{k} = Z_{1i}{}^{rk},$$

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

), and

a relationship among the plaintext data m, the re-encrypted text data C_j, and the second private key sk_j is expressed by:

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

45. A re-encryption apparatus (40) configured to communicate with a re-encryption key generator (30), which generates a re-encryption key required to obtain re-encrypted text data, which is configured to be decrypted by means of a second private key of a second user device, by re-encrypting, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first

public key of a first user device, the apparatus characterized by comprising:

storage means (41) for storing the re-encryption key received from the re-encryption key generator;

re-encryption means (44) for obtaining the re-encrypted text data by re-encrypting, without decrypting, the ciphertext data received from the first user device by means of the re-encryption key in the storage means; and

means (43) for transmitting the obtained re-encrypted text data to the second user device,

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

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

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

the re-encryption key includes a power index which consists of a numerator portion and a denominator portion,

the numerator portion of the power index of the re-encryption key has a form of linear coupling based on a

power index related to the respective system fixed values, the second private key corresponding to the second public key, and the first random number,

the denominator portion of the power index of the re-encryption key consists of the first private key,

the ciphertext data is generated based on the first public key and the second random number, and

the re-encrypted text data is generated based on the ciphertext data, the re-encryption key, a third random number, a fourth random number, and a fifth random number.

5~~6~~. The re-encryption apparatus of claim 4~~5~~, characterized in that the re-encryption key is generated independently of ciphertext data before re-encryption.

6~~7~~. A program which is executed by a processor of a re-encryption key generator (30), which generates a re-encryption key required to obtain re-encrypted text data, which is configured to be decrypted by means of a second private key of a second user device, by re-encrypting, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first public key of a first user device, and which is stored in a non-transitory computer-readable storage medium (M3), the program characterized by comprising:

a first program code (33) for controlling the processor to execute processing for writing a first private

key corresponding to the first public key in first storage means (31) of the re-encryption key generator;

a second program code (ST31) for controlling the processor to execute processing for writing a second public key corresponding to the second private key in second storage means (32) of the re-encryption key generator;

a third program code (36) for controlling the processor to execute processing for generating a first random number; and

a fourth program code (32) for controlling the processor to execute processing for generating the re-encryption key based on the first private key, the second public key, and the first random number,

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

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

the re-encryption key includes a power index which consists of a numerator portion and a denominator portion,

the numerator portion of the power index of the re-encryption key has a form of linear coupling based on a power index related to the respective system fixed values,

the second private key corresponding to the second public key, and the first random number,

the denominator portion of the power index of the re-encryption key consists of the first private key,

the ciphertext data is generated based on the first public key and the second random number, and

the re-encrypted text data is generated based on the ciphertext data, the re-encryption key, a third random number, a fourth random number, and a fifth random number.

78. The program of claim 67, characterized in that the processing for generating the re-encryption key is executed by the processor independently of ciphertext data before re-encryption.

89. A program which is executed by a processor of a re-encryption apparatus (40) configured to communicate with a re-encryption key generator (30), which generates a re-encryption key required to obtain re-encrypted text data, which is configured to be decrypted by means of a second private key of a second user device, by re-encrypting, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first public key of a first user device, and which is stored in a non-transitory computer-readable storage medium (M4), the program characterized by comprising:

a first program code (43) for controlling the processor to execute processing for writing the re-encryption key received from the re-encryption key generator in storage means (41) of the re-encryption apparatus;

a second program code (44) for controlling the processor to execute processing for obtaining the re-encrypted text data by re-encrypting, without decrypting, the ciphertext data received from the first user device by means of the re-encryption key in the storage means; and

a third program code (ST43) for controlling the processor to execute processing for transmitting the obtained re-encrypted text data to the second user device,

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

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

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

the re-encryption key includes a power index which consists of a numerator portion and a denominator portion,

the numerator portion of the power index of the re-encryption key has a form of linear coupling based on a power index related to the respective system fixed values, the second private key corresponding to the second public key, and the first random number,

the denominator portion of the power index of the re-encryption key consists of the first private key,

the ciphertext data is generated based on the first public key and the second random number, and

the re-encrypted text data is generated based on the ciphertext data, the re-encryption key, a third random number, a fourth random number, and a fifth random number.

9~~10~~. A program which is executed by a processor of an encryption apparatus (20) configured to communicate with a re-encryption apparatus (40) using a re-encryption key required to obtain re-encrypted text data, which is configured to be decrypted by means of a second private key of a second user device, by re-encrypting, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first public key of a first user device, and which is stored in a non-transitory computer-readable storage medium (M2), the program characterized by comprising:

a first program code (22) for controlling the processor to execute processing for writing the first public key in storage means (21) of the encryption apparatus;

a second program code (ST22) for controlling the processor to execute processing for obtaining the ciphertext data by encrypting the plaintext data using the first public key in the storage means; and

a third program code (ST24) for controlling the processor to execute processing for transmitting the obtained ciphertext data to the re-encryption apparatus,

wherein the re-encryption key is generated based on a first private key corresponding to the first public key, a second public key corresponding to the second private key, and a first random number generated by the re-encryption key generator (30),

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

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

the re-encryption key includes a power index which consists of a numerator portion and a denominator portion,

the numerator portion of the power index of the re-encryption key has a form of linear coupling based on a

power index related to the respective system fixed values, the second private key corresponding to the second public key, and the first random number,

the denominator portion of the power index of the re-encryption key consists of the first private key,

the ciphertext data is generated based on the first public key and the second random number, and

the re-encrypted text data is generated based on the ciphertext data, the re-encryption key, a third random number, a fourth random number, and a fifth random number.

1011. A program which is executed by a decryption apparatus (50), which decrypts re-encrypted text data received from an re-encryption apparatus (40) after the re-encryption apparatus re-encrypts, without decrypting, plaintext data by means of a first public key of a first user device to obtain the re-encrypted text data configured to be decrypted by means of a second private key of a second user device, and which is stored in a non-transitory computer-readable storage medium (M5), the program characterized by comprising:

a first program code (53) for controlling the processor to execute processing for writing the second private key in storage means (51) of the decryption apparatus; and

a second program code (54) for controlling the processor to execute processing for decrypting the re-encrypted text data received from the re-encryption apparatus based on the second private key in the storage means to obtain the plaintext data,

wherein the re-encryption key is generated based on a first private key corresponding to the first public key, a second public key corresponding to the second private key, and a first random number generated by a re-encryption key generator (30) which generates the re-encryption key,

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

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

the re-encryption key includes a power index which consists of a numerator portion and a denominator portion,

the numerator portion of the power index of the re-encryption key has a form of linear coupling based on a power index related to the respective system fixed values, the second private key corresponding to the second public key, and the first random number,

the denominator portion of the power index of the re-encryption key consists of the first private key,

the ciphertext data is generated based on the first public key and the second random number, and

the re-encrypted text data is generated based on the ciphertext data, the re-encryption key, a third random number, a fourth random number, and a fifth random number.

11~~12~~. The program of any one of claims 8~~9~~ to 10~~11~~, characterized in that the re-encryption key is generated independently of ciphertext data before re-encryption.