

Claims

- [Claim 1] An identity-based encryption method based on a lattice, comprising:
 receiving identity information;
 randomly sampling small elements;
 generating a function-processed output value by function-processing the input identity information; and
 generating an encrypted text for a message by using the sampled small elements, the function-processed output value and a master public key, wherein the master public key is computed using a ring having a dimension (d) represented by a power of 2 and an integer multiplication of 3 or more.
- [Claim 2] The identity-based encryption method based on a lattice, as claimed in claim 1, further comprising:
 computing a trapdoor (T) used for the identity-based encryption method based on a lattice; and
 determining the computed trapdoor (T) as a master secret key.
- [Claim 3] The identity-based encryption method based on a lattice, as claimed in claim 2, further comprising:
 computing a first random matrix (S) in which the number of columns is smaller than the dimension by 1 and the number of rows is equal to the number of the dimension by sampling elements ($\vec{f}_i$) linearly independent from each other in the ring;
 computing a second random matrix (A) in which the number of columns is equal to the number of the dimension and the number of rows is 1; and
 computing the master public key based on the second random matrix (A).
- [Claim 4] The identity-based encryption method based on a lattice, as claimed in claim 3, wherein in the computing of the second random matrix, a dXd matrix (M_i) is computed by excluding an i-th row from a matrix $[\vec{f}_1 \cdots \vec{f}_{d-1}] \in R_q^{d \times (d-1)}$, and $(-1)^{i-1} \cdot \det(M_i)$ is determined as a determinant (a_i), thereby computing $a_1^{-1} \cdot (a_1, a_2, \dots, a_d)$ as the second random matrix.
- [Claim 5] The identity-based encryption method based on a lattice, as claimed in claim 4, wherein the computing of the trapdoor (T) includes sampling of vector ($\vec{P} \in R_q^d$) that satisfies the relationship of

$\det[\vec{f}_1 \parallel \cdots \parallel \vec{f}_{d-1} \parallel \vec{F}] = q$, in which $[\vec{f}_1 \parallel \cdots \parallel \vec{f}_{d-1} \parallel \vec{F}]$ is computed as the trapdoor (T).

- [Claim 6] The identity-based encryption method based on a lattice, as claimed in claim 5, wherein in the sampling of the vector ($\vec{F} \in R_q^d$), a result vector value is output after reducing elements of the vector by using the elements ($\vec{f}_i$).
- [Claim 7] The identity-based encryption method based on a lattice, as claimed in claim 6, wherein in the sampling of the vector ($\vec{F} \in R_q^d$), the elements of the vector are reduced by removing a direction component of the elements by subtracting a constant multiple of the elements ($\vec{f}_i$) from the elements ($\vec{F} = (F_1, \dots, F_d)$) of the vector.
- [Claim 8] The identity-based encryption method based on a lattice, as claimed in claim 6, wherein in the sampling of the vector ($\vec{F} \in R_q^d$), the elements of the vector are reduced using an extended Euclidean algorithm.
- [Claim 9] The identity-based encryption method based on a lattice, as claimed in claim 3, further comprising:
 computing a solution having a small size, in which the multiplication of the solution and the second random matrix (A) becomes a hash value, with respect to the function-processed output value; and
 determining a user secret key using the computed small solution.
- [Claim 10] The identity-based encryption method based on a lattice, as claimed in claim 9, further comprising: decrypting the message from the encrypted text by using the user secret key.
- [Claim 11] The identity-based encryption method based on a lattice, as claimed in claim 1, wherein the identity information is at least one of a social security number, an email address, a phone number, fingerprint information and iris information.
- [Claim 12] A calculation device comprising:
 a memory storing at least one instruction and identity information; and
 a processor performing the at least one instruction,
 wherein the processor randomly samples small elements,
 generates a function-processed output value by function-processing the stored identity information, and
 generates an encrypted text for a message by using a master public key computed using a ring having a dimension (d) represented by a power of 2 and an integer multiplication of 3 or more, the sampled small

- elements and the function-processed output value.
- [Claim 13] The calculation device as claimed in claim 12, wherein the processor computes a first random matrix (S) in which the number of columns is smaller than the dimension by 1 and the number of rows is equal to the number of the dimension, by sampling elements ($\vec{r}_i$) linearly independent from each other in the ring,
 computes a second random matrix (A) in which the number of columns is equal to the number of the dimension and the number of rows is 1,
 computes the master public key based on the second random matrix (A), and
 computes a trapdoor (T) used for the identity-based encryption method based on a lattice and determines the computed trapdoor (T) as a master secret key.
- [Claim 14] The calculation device as claimed in claim 13, wherein the processor samples a vector that satisfies a predetermined relationship, in which a result vector obtained by reducing elements of the vector is computed as the trap door.
- [Claim 15] A computer-readable recording medium including a program performing an identity-based encryption method based on a lattice, wherein the identity-based encryption method based on a lattice includes:
 receiving identity information;
 randomly sampling small elements;
 generating a function-processed output value by function-processing the input identity information; and
 generating an encrypted text for a message by using the sampled small elements, the function-processed output value and a master public key, wherein the master public key being computed using a ring having a dimension (d) represented by a power of 2 and an integer multiplication of 3 or more.