

WHAT IS CLAIMED IS:

1. A method of generating a digital signature comprising:

receiving a message;

5 computing a particular solution in which a result of calculating the particular solution in a public key becomes a function-processed output value predetermined in the received message; and

generating digital signature information for the message using the computed particular solution,

10 wherein the public key is computed using a ring having a dimension (d) represented by a multiplication of a power of 2 and an integer, the integer being 3 or more, not a power of 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

15 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 public key based on the second random matrix (A).

20 2. The method of claim 1, wherein in the generating of the digital signature information, the digital signature information is generated by reducing the computed particular solution using a secret key.

3. The method of claim 1, further comprising:

25 computing a trapdoor (T); and

determining the computed trapdoor (T) as a secret key.

4. The method of claim 3, wherein in the computing of the second random matrix, a $d \times d$ 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) ,
 5 thereby computing $a_1^{-1} \cdot (a_1, a_2, \dots, a_d)$ as the second random matrix.

5. The method of claim 4, wherein the computing of the trapdoor (T) includes sampling of vector $(\vec{F} \in R_q^d)$ 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
 10 trapdoor (T).

6. The method of claim 5, wherein in the sampling of the vector, a result vector value is output after reducing elements of the vector by using the elements $(\vec{f}_h)$.

15 7. The method of claim 6, wherein in the sampling of the vector, the elements of the vector are reduced by removing a direction component of the elements by subtracting a constant multiple of the elements $(\vec{f}_h)$ from the elements $(\vec{F} = (F_1, \dots, F_d))$ of the vector.

8. The method of claim 6, wherein in the sampling of the vector, the elements of
 20 the vector are reduced using an extended Euclidean algorithm.

9. The method of claim 1, wherein the predetermined function-processing is a hash processing.

25 10. A method of verifying a message comprising:

receiving a message and digital signature information;

checking whether a result of calculating the digital signature information received in a public key becomes a function-processed output value predetermined in the message;

determining whether the received digital signature information has a value smaller than

5 a predetermined parameter; and

verifying the received message based on the check result and the determination result,

wherein the public key is computed using a ring having a dimension (d) represented by a multiplication of a power of 2 and an integer, the integer being 3 or more, not a power of 2,

further comprising:

10 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

15 computing the public key based on the second random matrix (A).

11. The method of claim 10, wherein the predetermined function-processing is a hash processing.

20 12. A calculation device comprising:

a memory storing at least one instruction; and

a processor performing the at least one instruction,

wherein the processor computes a particular solution in which a result of calculating the particular solution in a public key becomes a function-processed output value predetermined in a message, and generates digital signature information for the message using
25 the computed particular solution, and the public key is computed using a ring having a

dimension (d) represented by a multiplication of a power of 2 and an integer, the integer being 3 or more, not a power of 2,

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 ($\vec{f}_i$) linearly independent from each other in the ring;

the processor 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; and

the processor computes the public key based on the second random matrix (A).

13. The calculation device of claim 12, wherein the processor reduces the computed particular solution using a secret key, and generates the digital signature information by using the reduced particular solution.

14. The calculation device of claim 12, wherein receiving the message and the digital signature information, the processor checks whether a result of calculating the digital signature information received in a public key becomes a function-processed output value predetermined in the message, determines whether the received digital signature information has a value smaller than a predetermined parameter, and verifies the received message based on the check result and the determination result.

15. A non-transitory computer-readable recording medium comprising a program performing a method of generating a digital signature, wherein the method comprising:

receiving a message;

computing a particular solution in which a result of calculating the particular solution in a public key becomes a function-processed output value predetermined in the received message; and

generating digital signature information for the message using the computed particular solution,

wherein the public key is computed using a ring having a dimension (d) represented by a multiplication of a power of 2 and an integer, the integer being multiplication of 3 or more,
5 not a power of 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;

10 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 public key based on the second random matrix (A).