

What is claimed is:

1. A key generation apparatus for generating a key from biometric information, the key generation apparatus comprising;

5 a processor; and

a memory,

the memory holding:

a first feature vector indicating a feature of first biometric information; and

10 a parameter for identifying one arrangement out of a sphere packing arrangement with a density less than 1 and more than a predetermined value, or a sphere covering arrangement with a density equal to or more than 1 and less than a predetermined value,

the processor being configured to:

15 identify one arrangement out of the sphere packing arrangement or the sphere covering arrangement based on the parameter;

select a first point included in the one arrangement identified out of the sphere packing arrangement or the sphere covering arrangement;

20 generate a first key by performing predetermined first conversion on the first point; and

generate, based on the first feature vector and the first point, a template associated with the first biometric information,

25 wherein the one arrangement identified in the parameter out of the sphere packing arrangement and the sphere covering arrangement is a lattice arrangement, and

wherein the processor is configured to:

multiply the first feature vector by an inverse matrix of a basis matrix of the lattice arrangement to calculate a vector Y;

round down or up each component of the vector Y to a closest

whole number to calculate an integer vector Z ; and

select, as the first point, a vector obtained by multiplying the basis matrix by the integer vector Z .

5 2. The key generation apparatus according to claim 1, wherein the predetermined first conversion includes conversion by at least one of a hash function, a keyed hash function, an encryption function, or a linear hash function.

10 3. The key generation apparatus according to claim 1, wherein the processor is configured to generate, when the first key is restored, verification information for verifying validity of the restored first key, by performing predetermined second conversion on the first key.

15 4. The key generation apparatus according to claim 3, wherein the predetermined second conversion includes conversion by at least one of a hash function, a keyed hash function, an encryption function, or a linear hash function.

20 5. A key generation method by a key generation apparatus for generating a key from biometric information, the key generation apparatus holding:

 a first feature vector indicating a feature of first biometric information;

and

25 a parameter for identifying one arrangement out of a sphere packing arrangement with a density less than 1 and more than a predetermined value, or a sphere covering arrangement with a density equal to or more than 1 and less than a predetermined value,

 the key generation method comprising:

identifying, by the key generation apparatus, one arrangement out of the sphere packing arrangement or the sphere covering arrangement based on the parameter;

5 selecting, by the key generation apparatus, a first point included in the one arrangement identified out of the sphere packing arrangement or the sphere covering arrangement;

generating, by the key generation apparatus, a first key by performing predetermined first conversion on the first point; and

10 generating, by the key generation apparatus, based on the first feature vector and the first point, a template associated with the first biometric information,

wherein the one arrangement identified in the parameter out of the sphere packing arrangement and the sphere covering arrangement is a lattice arrangement, and

15 wherein the key generation method further comprises:

multiplying the first feature vector by an inverse matrix of a basis matrix of the lattice arrangement to calculate a vector Y;

rounding down or up each component of the vector Y to a closest whole number to calculate an integer vector Z; and

20 selecting, as the first point, a vector obtained by multiplying the basis matrix by the integer vector Z.