

WHAT IS CLAIMED IS:

1. A method of generating a cryptographic algorithm, the method comprising:

generating one or more key tables on the basis of a seed value;

generating, by using a round tweak bit string and ~~an~~ a first input bit string that is input to one of input branches of a Feistel structure, a first transformation function that converts the first input bit string into a first random bit string having a length that extends beyond a length of the ~~input bit string~~; first input bit string, the length of the first input bit string being varied according to a length of a unit input required in an environment to which the cryptographic algorithm is applied;

generating a second transformation function that converts a second random bit string generated by referencing the one or more key tables into a third random bit string having a length that is the same as the length of the first input bit string; and

generating a block cryptographic algorithm of a Feistel structure which includes a round function to which the one or more key tables, the first transformation function, and the second transformation function are applied;

wherein the round function is configured to: convert the first input bit string input to one of the input branches into the first random bit string using the first transformation function, convert the first random bit string into the second random bit string by referencing the one or more key tables according to a predetermined number of times of referencing a key table, and convert the second random bit string into the third random bit string using the second transformation function, and

wherein the third random bit string is used to perform an exclusive OR operation with a second input bit string that is input to another of the input branches of the Feistel structure.

2. The method of claim 1, wherein ~~the~~a length of ~~the~~an input bit string and a length of an output bit string for the one or more key tables are dynamically determined on the basis of a size of an available memory.

3. The method of claim 1, wherein the length of the first random bit string is determined on the basis of a predetermined number of times of referencing a key table and ~~the~~a length of ~~the~~an input bit string for the one or more key tables.

~~4. The method of claim 1, wherein the round function is configured to:~~

~~convert an input bit string input to one of the input branches into the first random bit string using the first transformation function;~~

~~convert the first random bit string into the second random bit string by referencing the one or more key tables according to a predetermined number of times of referencing a key table, and~~

~~convert the second random bit string into the third random bit string using the second transformation function.~~

~~54.~~ The method of claim ~~4~~1, wherein the round function is further configured to:

divide the first random bit string into d (where d is the number of times of referencing a key table) bit strings each having a length of L bits (where L is a length of an input bit string for the one or more key tables) on the basis of the number of times of referencing a key table,

convert the d bit strings, each having a length of L bits, into d bit strings, each having m bits (where m is a length of an output bit string for the one or more key tables), by referencing

the one or more key tables as many times as the number of times of referencing a key table, and

generate the second random bit string by concatenating the d bit strings, each having a length of m bits.

65. An apparatus for generating a cryptographic algorithm, comprising:

one or more processors;

a memory; and

one or more programs,

wherein the one or more programs are stored in the memory and are configured to be executed by the one or more processors and

the one or more programs include commands for

generating one or more key tables on the basis of a seed value,

generating, by using a round tweak bit string and ~~an~~ first input bit string that is input to one of input branches of a Feistel structure, a first transformation function that converts the first input bit string into a first random bit string having a length that extends beyond a length of the ~~input bit string~~ first input bit string, the length of the first input bit string being varied according to a length of a unit input required in an environment to which the cryptographic algorithm is applied,

generating a second transformation function that converts a second random bit string generated by referencing the one or more key tables into a third random bit string having a length that is the same as the length of the first input bit string, and

generating a block cryptographic algorithm of a Feistel structure which includes a round function to which the one or more key tables, the first transformation function, and the second

transformation function are applied.

wherein the round function is configured to: convert the first input bit string input to one of the input branches into the first random bit string using the first transformation function, convert the first random bit string into the second random bit string by referencing the one or more key tables according to a predetermined number of times of referencing a key table, and convert the second random bit string into the third random bit string using the second transformation function, and

wherein the third random bit string is used to perform an exclusive OR operation with a second input bit string that is input to another of the input branches of the Feistel structure.

76. The apparatus of claim 56, wherein ~~the~~a length of ~~the~~a input bit string and a length of an output bit string for the one or more key tables are dynamically determined on the basis of a size of an available memory.

87. The apparatus of claim 65, wherein the length of the first random bit string is determined on the basis of a predetermined number of times of referencing a key table and ~~the~~a length of ~~the~~a input bit string for the one or more key tables.

~~9. The apparatus of claim 6, wherein the round function is configured to:~~
~~convert an input bit string input to one of the input branches into the first random bit string using the first transformation function;~~
~~convert the first random bit string into the second random bit string by referencing the one or more key tables according to a predetermined number of times of referencing a key table;~~
~~and~~

~~convert the second random bit string into the third random bit string using the second transformation function.~~

~~108.~~ The apparatus of claim ~~9~~ 5, wherein the round function is further configured to:

divide the first random bit string into d (where d is the number of times of referencing a key table) bit strings each having a length of L bits (where L is a length of an input bit string for the one or more key tables) on the basis of the number of times of referencing a key table,

convert the d bit strings, each having a length of L bits, into d bit strings, each having m bits (where m is a length of an output bit string for the one or more key tables), by referencing the one or more key tables as many times as the number of times of referencing a key table, and

generate the second random bit string by concatenating the d bit strings, each having a length of m bits.

~~119.~~ A method of encryption, comprising:

generating a round tweak bit string;

converting, by using a first transformation function, the round tweak bit string and a first input bit string, which is input to one of input branches of a Feistel structure which includes a round function to which one or more key tables, the first transformation function, and a second transformation function are applied, into a first random bit string having a length that extends beyond a length of the first input bit string;

converting the first random bit string into a second random bit string by referencing the one or more key tables;

converting, by using the second transformation function, the second random bit string into a third random bit string having the same length as the length of the first input bit string;

and

performing an exclusive OR operation between the third random bit string and a second input bit string that is input to another input branch among the input branches of the Feistel structure;

wherein the length of the first input bit string is varied according to a length of a unit input required in an environment to which the cryptographic algorithm is applied.

1210. The method of claim 119, wherein the length of the first random bit string is determined on the basis of a predetermined number of times of referencing a key table and ~~the~~a length of ~~the~~an input bit string for the one or more key tables.

1311. The method of claim 119, wherein the converting into the second random bit string comprises converting the first random bit string into the second random bit string by referencing the one or more key tables according to a predetermined number of times of referencing a key table.

1412. The method of claim 1311, wherein the converting into the second random bit string comprises:

dividing the first random bit string into d (where d is the number of times of referencing a key table) bit strings each having a length of L bits (where L is a length of an input bit string for the one or more key tables) on the basis of the number of times of referencing a key table,

converting the d bit strings, each having a length of L bits, into d bit strings, each having m bits (where m is a length of an output bit string for the one or more key tables), by referencing the one or more key tables as many times as the number of times of referencing a key table;

and

generating the second random bit string by concatenating the d bit strings, each having a length of m bits.

~~45~~13. An apparatus for encryption, comprising:

one or more processors;

a memory; and

one or more programs,

wherein the one or more programs are stored in the memory and are configured to be executed by the one or more processors and

the one or more programs include commands for

generating a round tweak bit string,

converting, by using a first transformation function, the round tweak bit string and a first input bit string, which is input to one of input branches of a Feistel structure which includes a round function to which one or more key tables, the first transformation function, and a second transformation function are applied, into a first random bit string having a length that extends beyond a length of the first input bit string,

converting the first random bit string into a second random bit string by referencing the one or more key tables,

converting, by using athe second transformation function, the second random bit string into a third random bit string having the same length as the length of the first input bit string, and

performing an exclusive OR operation between the third random bit string and a second input bit string that is input to another input branch among the input branches of the Feistel

structure.

wherein the length of the first input bit string is varied according to a length of a unit input required in an environment to which the cryptographic algorithm is applied.

~~16~~14. The apparatus of claim ~~15~~13, wherein the length of the first random bit string is determined on the basis of a predetermined number of times of referencing a key table and ~~the~~a length of ~~the~~an input bit string for the one or more key tables.

~~17~~15. The apparatus of claim ~~15~~13, wherein the converting into the second random bit string comprises converting the first random bit string into the second random bit string by referencing the one or more key tables according to a predetermined number of times of referencing a key table.

~~18~~16. The apparatus of claim ~~17~~15, wherein the converting into the second random bit string comprises:

dividing the first random bit string into d (where d is the number of times of referencing a key table) bit strings each having a length of L bits (where L is a length of an input bit string for the one or more key tables) on the basis of the number of times of referencing a key table;

converting the d bit strings, each having a length of L bits, into d bit strings, each having m bits (where m is a length of an output bit string for the one or more key tables), by referencing the one or more key tables as many times as the number of times of referencing a key table; and

generating the second random bit string by concatenating the d bit strings, each having a length of m bits.