

Provably Secure and Not Relying on Any Unproved
Hypotheses. CRYPTO 1989:461-480

SUMMARY OF THE INVENTION

5 PROBLEMS TO BE SOLVED BY THE INVENTION

[0010]

This disclosure is being made in view of the above
described circumstances, for example, and embodiments of
the present invention ~~an object thereof is to~~ provide a
10 cryptographic processing device that has a high level of
security with improved diffusion properties, a
cryptographic processing method, and a program.

SOLUTIONS TO PROBLEMS

15 [0011]

According to a first aspect, there is provided a
cryptographic processing device comprising
a cryptographic processing unit configured to
divide and input constituent bits of data to be subjected
20 to data processing into a plurality of lines, and
repeatedly perform a data converting operation on the
data in the respective lines by using a round function,
wherein
the cryptographic processing unit has a structure
25 designed to input n/d -bit data formed by dividing n -bit
data as input data by a division number d to the
respective lines, and repeatedly perform a calculation as
a round calculation including the data converting
operation using the round function,
30 the cryptographic processing unit performs an
operation in which the n/d -bit data of each line having

output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round calculation of the next stage,

the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function with data of another line, and

the cryptographic processing unit sets a result of the round calculation of the previous stage as the input to the round calculation of the next stage by performing an operation that satisfies the following distribution conditions (1) through (3):

(1) F-function input-side data series are distributed to XOR-side data series of the next round function,

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

(3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round function without overlaps.

~~A first aspect of this disclosure resides in a cryptographic processing device that includes~~

~~a cryptographic processing unit that divides and inputs constituent bits of data to be subjected to data processing, into lines, and repeatedly performs a data converting operation on the data in the respective lines by using a round function,~~

~~wherein the cryptographic processing unit has a~~

5

~~structure designed to input n/d bit data formed by
dividing n bit data as input data by a division number d
to the respective lines, and repeatedly perform a
calculation as a round calculation including the data
converting operation using the round function, and
the cryptographic processing unit performs an
operation in which the n/d bit data of each line having
output data of the round calculation is redivided into~~

~~d/2 sets of data, the redivided data is recombined to
restructure d sets of n/d bit data different from output
data of the round calculation of the previous stage, and
the restructured data is set as input data for the round
5 calculation of the next stage.~~

[0012]

Further, in an embodiment of the cryptographic
processing device of this disclosure, the round function
includes an F-function that includes a calculation using
10 a round key, nonlinear transformation, and linear
transformation, and an exclusive OR operation between an
output or an input of the F-function and the data of
another line.

[0013]

15 Further, in an embodiment of the cryptographic
processing device of this disclosure, the cryptographic
processing unit sets the result of the round calculation
of the previous stage as the input to the round
calculation of the next stage by performing an operation
20 that satisfies the following distribution conditions (1)
through (3):

(1) F-function input-side data series are
invariably distributed to XOR-side data series of the
next round function,

25 (2) XOR-side data series are invariably distributed
to F-function input-side data series of the next round
function, and

(3) each one of data series divided into d/2 sets
is distributed to d/2 data series of the next round
30 function without overlaps.

[0014]

predetermined rule; and distributing the redivided data of the XOR-side series of the previous stage to the round-function input-side series of the next stage in accordance with a predetermined rule.

5 [0021]

Further, in an embodiment of the cryptographic processing device of this disclosure, the cryptographic processing unit performs an encrypting operation to transform a plain text as input data into a cipher text, or a decrypting operation to transform a cipher text as input data into a plain text.

[0022]

According to a second aspect, there is provided a cryptographic processing method implemented in a cryptographic processing device,
15 the cryptographic processing method comprising a cryptographic processing step of dividing and inputting constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly performing a data converting operation on the data in the respective lines by using a round function,

wherein

the cryptographic processing step includes inputting n/d -bit data formed by dividing n -bit data as input data by a division number d to the respective lines; and repeatedly performing a calculation as a round calculation including the data converting operation using the round function,

the cryptographic processing step includes an operation in which the n/d -bit data of each line having output data of the round calculation is redivided into

d/2 sets of data, the redivided data is recombined to restructure d sets of n/d-bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round calculation of the next stage,

the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function with data of another line, and

the cryptographic processing step includes setting a result of the round calculation of the previous stage as the input to the round calculation of the next stage by performing an operation that satisfies the following distribution conditions (1) through (3):

(1) F-function input-side data series are distributed to XOR-side data series of the next round function,

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

(3) each one of data series divided into d/2 sets is distributed to d/2 data series of the next round function without overlaps.

~~Further, a second aspect of this disclosure resides in a cryptographic processing method implemented in a cryptographic processing device,~~

~~the cryptographic processing method including a cryptographic processing step of dividing and inputting the constituent bits of data to be subjected to data processing into lines, and repeatedly performing a data converting operation on the data in the respective lines by using a round function,~~

~~wherein the cryptographic processing step includes:~~
~~inputting n/d bit data formed by dividing n bit data as~~
~~input data by a division number d to the respective~~
~~lines; and repeatedly performing a calculation as a round~~
5 ~~calculation including the data converting operation using~~
~~the round function, and~~

~~the cryptographic processing step includes an~~
~~operation in which the n/d bit data of each line having~~
~~the output data of the round calculation is redivided~~
10 ~~into $d/2$ sets of data, the redivided data is recombined~~

~~to restructure d sets of n/d -bit data different from the output data of the round calculation of the previous stage, and the restructured data is set as input data for the round calculation of the next stage.~~

5 [0023]

According to a third aspect, there is provided a program for causing a cryptographic processing device to perform cryptographic processing,

10 the program causing a cryptographic processing unit to carry out

a cryptographic processing step of dividing and inputting constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly performing a data converting operation on the data in the

15 respective lines by using a round function,

wherein

the cryptographic processing step includes:

20 inputting n/d -bit data formed by dividing n -bit data as input data by a division number d to the respective lines; and repeatedly performing a calculation as a round calculation including the data converting operation using the round function,

the cryptographic processing step includes an operation in which the n/d -bit data of each line having

25 output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round

30 calculation of the next stage,

the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function with data of another line, and

the cryptographic processing step includes setting
5 a result of the round calculation of the previous stage as the input to the round calculation of the next stage by performing an operation that satisfies the following distribution conditions (1) through (3):

(1) F-function input-side data series are
10 distributed to XOR-side data series of the next round function,

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

15 (3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round function without overlaps.

According to a fourth aspect, there is provided a cryptographic processing device comprising

20 a cryptographic processing unit configured to divide and input constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly perform a data converting operation on the data in the respective lines by using a round function,

25 wherein

the cryptographic processing unit has a structure designed to input n/d -bit data formed by dividing n -bit data as input data by a division number d to the respective lines, and repeatedly perform a calculation as
30 a round calculation including the data converting operation using the round function,

the cryptographic processing unit performs an operation in which the n/d -bit data of each line having output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round calculation of the next stage, and

the cryptographic processing unit performs an operation in which $d \times (d/2)$ sets of redivided data are generated by redividing n/d -bit data of each of d lines having the output data of the round calculation into $d/2$ sets of data, $d/2$ sets of redivided data selected from different lines among the d lines corresponding to the division number d are recombined to restructure d sets of n/d -bit data different from the output data of the round calculation of the previous stage, and the restructured data is set as the input data for the round calculation of the next stage.

According to a fifth aspect, there is provided an information processing device comprising:

a processor configured to execute a program;

a memory storing the program; and

a cryptographic processing unit configured to divide and input constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly perform a data converting operation on the data in the respective lines by using a round function,

wherein

the cryptographic processing unit has a structure designed to input n/d -bit data formed by dividing n -bit data as input data by a division number d to the respective lines, and repeatedly perform a calculation as a round calculation including the data converting operation using the round function,

the cryptographic processing unit performs an operation in which the n/d -bit data of each line having output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round calculation of the next stage,

the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function with data of another line, and

the cryptographic processing unit sets a result of the round calculation of the previous stage as the input to the round calculation of the next stage by performing an operation that satisfies the following distribution conditions (1) through (3):

(1) F-function input-side data series are distributed to XOR-side data series of the next round function,

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

(3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round function without overlaps.

~~Further, a third aspect of this disclosure resides in a program for causing a cryptographic processing device to perform cryptographic processing,~~

~~the program causing a cryptographic processing unit to carry out~~

~~a cryptographic processing step of dividing and inputting the constituent bits of data to be subjected to data processing into lines, and repeatedly performing a data converting operation on the data in the respective lines by using a round function,~~

~~wherein the cryptographic processing step includes: inputting n/d bit data formed by dividing n bit data as input data by a division number d to the respective lines; and repeatedly performing a calculation as a round calculation including the data converting operation using the round function; and~~

~~the cryptographic processing step includes an operation in which the n/d bit data of each line having output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d bit data different from output data of the round calculation of the previous stage, and the restructured data is set as input data for the round calculation of the next stage.~~

[0024]

It should be noted that the program of this

disclosure is a program that is recorded on a storage medium and is then provided to an information processing device or a computer system that can execute various program codes, for example. As a program executing unit
5 in an information processing device or a computer system executes such a program, operations according to the program are performed.

[0025]

Other aspect~~subjects~~, features, and advantages of
10 this disclosure will become apparent from the detailed description below in conjunction with the later described embodiments of the present invention and the accompanying drawings. In this specification, a system is a logical integration of devices, and each of the component devices
15 is not necessarily located in the same housing.

EFFECTS OF THE INVENTION

[0026]

According to an embodiment of this disclosure,
20 cryptographic processing with improved diffusion properties and a high level of security is realized.

Specifically, a cryptographic processing unit divides and inputs the constituent bits of the data to be subjected to data processing to lines, and repeatedly
25 performs a data converting operation using round functions on the data of the respective lines. The cryptographic processing unit inputs n/d -bit data obtained by dividing n -bit data as input data by a division number d to each line, and repeatedly performs a
30 round calculation that is a calculation including a data converting operation using round functions. The n/d -bit

CLAIMS

1. ~~(amended)~~—A cryptographic processing device comprising

5 a cryptographic processing unit configured to divide and input constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly perform a data converting operation on the data in the respective lines by using a round function,

10 wherein

the cryptographic processing unit has a structure designed to input n/d -bit data formed by dividing n -bit data as input data by a division number d to the respective lines, and repeatedly perform a calculation as
15 a round calculation including the data converting operation using the round function,

the cryptographic processing unit performs an operation in which the n/d -bit data of each line having output data of the round calculation is redivided into
20 $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round calculation of the next stage,

25 the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function with data of another line, and

the cryptographic processing unit sets a result of the round calculation of the previous stage as the input
30 to the round calculation of the next stage by performing an operation that satisfies the following distribution

conditions (1) through (3):

(1) F-function input-side data series are distributed to XOR-side data series of the next round function,

5 (2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

(3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round
10 function without overlaps.

2. The cryptographic processing device according to claim 1, wherein the round function includes an F-function that includes a calculation using a round key,
15 nonlinear transformation, and linear transformation, and an exclusive OR operation between an output or an input of the F-function and data of another line.

20 ~~3. (deleted)~~

34. The cryptographic processing device according to claim 1, wherein the cryptographic processing unit has a generalized Feistel structure having equal to or greater than 4 as the division number d of input data.

25

45. ~~(amended)~~ The cryptographic processing device according to claim 1, wherein the cryptographic processing unit performs an operation in which $d \times (d/2)$ sets of redivided data are generated by redividing n/d -
30 bit data of each of d lines having the output data of the round calculation into $d/2$ sets of data, $d/2$ sets of

redivided data selected from different lines among the d lines corresponding to the division number d are recombined to restructure d sets of n/d -bit data different from the output data of the round calculation of the previous stage, and the restructured data is set as the input data for the round calculation of the next stage.

56. The cryptographic processing device according to claim 1, wherein, when all output bits are in a diffusion state that satisfies the following two conditions, or when the output bits are expressed in a relational expression with input bits, the cryptographic processing unit has a structure that realizes a full diffusion state satisfying the following two conditions:

(Condition 1) all input bits are included in the relational expression, and

(Condition 2) all the input bits have passed through the round function at least once.

67. The cryptographic processing device according to claim 56, wherein the cryptographic processing unit realizes the full diffusion state through four rounds of round calculations.

~~78.~~ ~~(amended)~~ The cryptographic processing device according to claim 1, wherein the connection structure that determines an input-output relationship between the output data of the round calculation of the previous stage and the redivided data of the round calculation of the next stage is a connection structure selected from

connection structures that have $(d/2)$ sets of $2n/d$ -bit data as units that are data generated by combining $d \times (d/2)$ sets of redivided data generated through a redividing operation performed on the n/d -bit data in the lines having the output data of the round calculation.

89. ~~(amended)~~ The cryptographic processing device according to claim 1, wherein the cryptographic processing unit has involution properties.

10

910. The cryptographic processing device according to 89, wherein the operation to restructure redivided data of respective round calculations in the cryptographic processing unit includes: distributing redivided data of round-function input-side series of the previous stage to XOR-side series of the next stage in accordance with a predetermined rule; and distributing redivided data of XOR-side series of the previous stage to round-function input-side series of the next stage in accordance with a predetermined rule.

20

1011. The cryptographic processing device according to claim 1, wherein the cryptographic processing unit performs an encrypting operation to transform a plain text as input data into a cipher text, or a decrypting operation to transform a cipher text as input data into a plain text.

25

1112. ~~(amended)~~ A cryptographic processing method

30

implemented in a cryptographic processing device, the cryptographic processing method comprising

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

(3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round function without overlaps.

1213. ~~(amended)~~ A program for causing a cryptographic processing device to perform cryptographic processing,
 10 the program causing a cryptographic processing unit to carry out

a cryptographic processing step of dividing and inputting constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly
 15 performing a data converting operation on the data in the respective lines by using a round function,

wherein

the cryptographic processing step includes:
 inputting n/d -bit data formed by dividing n -bit data as
 20 input data by a division number d to the respective lines; and repeatedly performing a calculation as a round calculation including the data converting operation using the round function,

the cryptographic processing step includes an
 25 operation in which the n/d -bit data of each line having output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the
 30 restructured data is set as input data for a round calculation of the next stage,

the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function with data of another line, and

the cryptographic processing step includes setting
 5 a result of the round calculation of the previous stage as the input to the round calculation of the next stage by performing an operation that satisfies the following distribution conditions (1) through (3):

(1) F-function input-side data series are

10 distributed to XOR-side data series of the next round function,

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

15 (3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round function without overlaps.

1314. ~~(added)~~ A cryptographic processing device

20 comprising

a cryptographic processing unit configured to divide and input constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly perform a data converting operation on the
 25 data in the respective lines by using a round function, wherein

the cryptographic processing unit has a structure designed to input n/d -bit data formed by dividing n -bit data as input data by a division number d to the
 30 respective lines, and repeatedly perform a calculation as a round calculation including the data converting

operation using the round function,

the cryptographic processing unit performs an operation in which the n/d -bit data of each line having output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output data of a round calculation of a previous stage, and the restructured data is set as input data for a round calculation of the next stage, and

the cryptographic processing unit performs an operation in which $d \times (d/2)$ sets of redivided data are generated by redividing n/d -bit data of each of d lines having the output data of the round calculation into $d/2$ sets of data, $d/2$ sets of redivided data selected from different lines among the d lines corresponding to the division number d are recombined to restructure d sets of n/d -bit data different from the output data of the round calculation of the previous stage, and the restructured data is set as the input data for the round calculation of the next stage.

~~1415. (added)~~ The cryptographic processing device according to claim ~~1314~~, wherein

the round function includes an F-function and an exclusive OR operation to be performed on a output or an input of the F-function and data of another line, and

the cryptographic processing unit sets a result of the round calculation of the previous stage as the input to the round calculation of the next stage by performing an operation that satisfies the following distribution conditions (1) through (3):

(1) F-function input-side data series are distributed to XOR-side data series of the next round function,

(2) XOR-side data series are distributed to F-function input-side data series of the next round function, and

(3) each one of data series divided into $d/2$ sets is distributed to $d/2$ data series of the next round function without overlaps.

10

1516. ~~(added)~~—An information processing device comprising:

a processor configured to execute a program;

a memory storing the program; and

15

a cryptographic processing unit configured to divide and input constituent bits of data to be subjected to data processing into a plurality of lines, and repeatedly perform a data converting operation on the data in the respective lines by using a round function,

20

wherein

the cryptographic processing unit has a structure designed to input n/d -bit data formed by dividing n -bit data as input data by a division number d to the respective lines, and repeatedly perform a calculation as a round calculation including the data converting operation using the round function,

25

the cryptographic processing unit performs an operation in which the n/d -bit data of each line having output data of the round calculation is redivided into $d/2$ sets of data, the redivided data is recombined to restructure d sets of n/d -bit data different from output

30