

(51) International Patent Classification:
G09C 1/00 (2006.01)(21) International Application Number:
PCT/JP2017/018745(22) International Filing Date:
18 May 2017 (18.05.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants: NEC CORPORATION [JP/JP]; 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). BAR-ILAN UNIVERSITY [IL/IL]; Ramat Gan, 5290002 (IL).

(72) Inventors: ARAKI, Toshinori; c/o NEC CORPORATION, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). OHARA, Kazuma; c/o NEC CORPORATION, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). FURUKAWA, Jun; c/o Israel Research Center, NEC Corporation of America, 2 Maskit Street, Building D, 2nd Floor, Herzliya, 4673302 (IL). YEHUDA, Lindell; c/o Bar-Ilan University, Ramat Gan, 5290002 (IL). ARIEL, Nof; c/o Bar-Ilan University, Ramat Gan, 5290002 (IL).

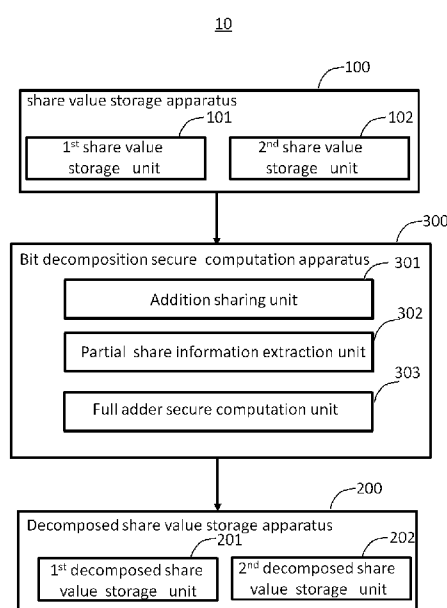
(74) Agent: KATO, Asamichi; c/o A. Kato & Associates, 20-12, Shin-Yokohama 3-chome, Kohoku-ku, Yokohama-shi, Kanagawa, 2220033 (JP).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: BIT DECOMPOSITION SECURE COMPUTATION APPARATUS, BIT COMBINING SECURE COMPUTATION APPARATUS, METHOD AND PROGRAM

[Fig. 1]

(57) Abstract: The present invention provides a bit decomposition secure computation system comprising: a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic; a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic; and a bit decomposition secure computation apparatus that, with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, being used as share information by the (2, 3) type RSS stored in the share value storage apparatus, includes: an addition sharing unit that sums two values out of r_1 , r_2 and r_3 by modulo 2^n , generates and distributes a share value of the (2, 3) type RSS with respect to the sum; and a full adder secure computation unit that executes addition processing of the value generated by the addition sharing unit and a value not used by the addition sharing unit, for each digit, by using secure computation of a full adder, and stores the result in the decomposed share value storage apparatus.

Published:

— *with international search report (Art. 21(3))*

Description

Title of Invention: BIT DECOMPOSITION SECURE COMPUTATION APPARATUS, BIT COMBINING SECURE COMPUTATION APPARATUS, METHOD AND PROGRAM

Technical Field

[0001] The present invention relates to a bit decomposition secure computation apparatus, bit combining secure computation apparatus, method and program.

Background Art

[0002] A secure computation scheme is a technology that can allow a computer system to conceal computation process and result against related parties. By performing secret sharing of data to store shares in a plurality of servers managed by a third party such as a cloud, it is possible to execute any operation on the data. Since data, computation process, and computation result are not known to the third party, the secure computation can be used, as an example, for outsourcing of analysis processing or the like of sensitive information such as personal information, though not limited thereto.

[0003] The following describes secure computation using replication type secret shared (hereinafter referred to as (2, 3) type RSS) having (2, 3) threshold access structure, as a premise of the present invention that relates to a secure computation using (2, 3) type RSS.

[0004] (2, 3) threshold type RSS is one of implementation methods of (2, 3) secret sharing schemes. The (2, 3) secret sharing scheme is a scheme such that three items of share information are generated from input values, and from one or less items of share information, an original information is not known, while the original value can be reconstructed from two or more items of share information.

[0005] In (2, 3) type RSS, in secret sharing of a value x of from 0 to $p-1$ or less, a set of three values r_1 , r_2 , and r_3 each from 0 to $p-1$ or less such that $x = r_1 + r_2 + r_3 \bmod p$, is generated, and, as three items of sharing information, three tuples are used, wherein the three tuples each have two values selected from (r_1, r_2, r_3) , different to each other, thereby implementing (2, 3) secret sharing. It is noted that p is called a modulus.

[0006] A method for executing computation on shares distributed by secret sharing without reconstruction is called secure computation. The following describes a secure computation method for a value shared (distributed) with the (2, 3) RSS scheme that relates to the present invention.

[0007] First, a sharing method of a value will be described, and then addition, subtraction, and multiplication will be described. Here, a procedure will be described in which a plurality of values each are shared by three apparatuses and secure computation is

performed on the shares (share values). Here, three apparatuses are distinguished by calling them apparatus 1, apparatus 2, and apparatus 3.

[0008] <Value-Sharing Scheme>

In secret-sharing of a value w of 0 or more and less than p , where p is an integer of 2 or more, r_1 , r_2 , and r_3 that are randomly selected so as to satisfy $w = r_1 + r_2 + r_3 \bmod p$ are generated and stored as follows.

The apparatus 1 stores (r_1, r_2) in a storage thereof as a share value of w .

The apparatus 2 stores (r_2, r_3) in a storage thereof as a share value of w .

The apparatus 3 stores (r_3, r_1) in a storage thereof as a share value of w .

[0009] It can be confirmed that w cannot be obtained in any one of the parties (apparatuses 1 to 3) because each of the parties lacks one of r_1 , r_2 , and r_3 , but w can be reconstructed from share values stored in two or more parties.

[0010] <Addition processing>

The following describes an addition processing executed with respect to sharing of a value w and a value w' stored in a distributed manner in the apparatus 1, the apparatus 2, and the apparatus 3, by the above-described method. Here, it is assumed that r_1 , r_2 , and r_3 are randomly selected to satisfy $w = r_1 + r_2 + r_3 \bmod p$, and r_1' , r_2' , and r_3' are randomly selected to satisfy $w' = r_1' + r_2' + r_3' \bmod p$.

[0011] The apparatus 1 stores $(s_1, t_1) = (r_1, r_2)$ as a share value of w and $(s_1', t_1') = (r_1', r_2')$ as a share value of w' , in a storage thereof.

The apparatus 2 stores $(s_2, t_2) = (r_2, r_3)$ as a share value of w and $(s_2', t_2') = (r_2', r_3')$ as a share value of w' , in a storage thereof.

The apparatus 3 stores $(s_3, t_3) = (r_3, r_1)$ as a share value of w and $(s_3', t_3') = (r_3', r_1')$ as a share value of w' , in a storage thereof.

[0012] The apparatus 1 to 3 respectively perform processing according to the following procedure.

[0013] The apparatus 1 calculates (s_1'', t_1'') by
 $(s_1'', t_1'') = (r_1'' = s_1 + s_1' \bmod p, r_2'' = t_1 + t_1' \bmod p)$
 and stores (s_1'', t_1'') in a storage thereof, as a share value of $w + w'$.

The apparatus 2 calculates (s_2'', t_2'') by
 $(s_2'', t_2'') = (r_2'' = s_2 + s_2' \bmod p, r_3'' = t_2 + t_2' \bmod p)$
 and stores (s_2'', t_2'') in a storage thereof, as a share value of $w + w'$.

The apparatus 3 calculates (s_3'', t_3'') by
 $(s_3'', t_3'') = (r_3'' = s_3 + s_3' \bmod p, r_1'' = t_3 + t_3' \bmod p)$
 and stores (s_3'', t_3'') in a storage thereof, as a share value of $w + w'$.

[0014] Each computation result of the apparatuses 1 to 3 is a share value of $w + w'$ that is shared using r_1'' , r_2'' and r_3'' which satisfy: $w + w' = r_1'' + r_2'' + r_3'' \bmod p$.

This can be confirmed by $r_1'' + r_2'' + r_3'' = (r_1 + r_2 + r_3) + (r_1' + r_2' + r_3') = w + w'$

mod p.

[0015] <Subtraction processing>

The following describes a subtraction processing executed with respect to sharing of a value w and a value w' stored in a distributed manner in the apparatus 1, the apparatus2, and the apparatus3 by the above described method. It is assumed that $w = r1 + r2 + r3 \bmod p$, and $w' = r1' + r2' + r3' \bmod p$.

[0016] The apparatus 1 stores $(s1, t1) = (r1, r2)$ as a share value of w and $(s1', t1') = (r1', r2')$ as a share value of w', in a storage thereof.

The apparatus 2 stores $(s2, t2) = (r2, r3)$ as a share value of w and $(s2', t2') = (r2', r3')$ as a share value of w', in a storage thereof.

The apparatus 3 stores $(s3, t3) = (r3, r1)$ as a share value of w and $(s3', t3') = (r3', r1')$ as a share value of w', in a storage thereof.

[0017] The apparatuses 1 to 3 respectively perform processing according to the following procedure.

[0018] The apparatus 1 calculates $(s1'', t1'')$ by

$(s1'', t1'') = (r1'' = s1 - s1' \bmod p, r2'' = t1 - t1' \bmod p)$ and stores $(s1'', t1'')$, in a storage thereof, as a share value of $w - w'$.

[0019] The apparatus 2 calculates $(s2'', t2'')$ by $(s2'', t2'') = (r2'' = s2 - s2' \bmod p, r3'' = t2 - t2' \bmod p)$ and stores $(s2'', t2'')$, in a storage thereof, as a share value of $w - w'$.

[0020] The apparatus 3 calculates $(s3'', t3'')$ by $(s3'', t3'') = (r3'' = s3 - s3' \bmod p, r1'' = t3 - t3' \bmod p)$ and stores $(s3'', t3'')$, in a storage thereof, as a share value of $w - w'$.

[0021] Each computation result of the apparatuses 1 to 3 is a share value of $w - w'$ that is shared using $r1'', r2''$ and $r3''$ which satisfy: $w - w' = r1'' + r2'' + r3'' \bmod p$.

This can be confirmed by $r1'' + r2'' + r3'' = (r1 + r2 + r3) - (r1' + r2' + r3') = w - w' \bmod p$.

[0022] <Multiplication Processing>

The following describes a multiplication processing executed with respect to values w and w' stored in the apparatuses 1, 2, and 3 by the above described method.

[0023] First describes what value each apparatus stores. It is assumed that $r1, r2$ and $r3$ are randomly selected values that satisfy $r1 + r2 + r3 = w \bmod p$, and $r1', r2', r3'$ are randomly selected values that satisfy $r1' + r2' + r3' = w' \bmod 2^n$.

[0024] The apparatus 1 stores $(s1, t1) = (r1, r2)$ as a share value of w and $(s1', t1') = (r1', r2')$ as a share value of w', in a storage thereof.'

The apparatus 2 stores $(s2, t2) = (r2, r3)$ as a share value of w and $(s2', t2') = (r2', r3')$ as a share value of w', in a storage thereof.

The apparatus 3 stores $(s3, t3) = (r3, r1)$ as a share value of w and $(s3', t3') = (r3', r1')$ as a share value of w', in a storage thereof.

[0025] The apparatuses 1 to 3 respectively perform processing according to the following

procedures.

[0026] The apparatus 1, apparatus 2 and apparatus 3 are assumed to store respectively $r1''$, $r2''$, and $r3''$ as randomly selected values that satisfy $r1'' + r2'' + r3'' = 0 \bmod 2^n$. $r1''$, $r2''$, $r3''$ that satisfy such a property are required by disposal, each time multiplication is executed. A method for efficiently generating such three values by three apparatuses will be described later.

[0027] The apparatus 1 calculates $u2 = s1 \cdot s1' + s1 \cdot t1' + t1 \cdot s1' + r1'' \bmod p$ and sends $u2$ to the apparatus 2.

The apparatus 2 calculates $u3 = s2 \cdot s2' + s2 \cdot t2' + t2 \cdot s2' + r2'' \bmod p$ and sends $u3$ to the apparatus 3.

The apparatus 3 calculates $u1 = s3 \cdot s3' + s3 \cdot t3' + t3 \cdot s3' + r3'' \bmod p$ and sends $u1$ to the apparatus 1.

[0028] The apparatus 1 stores $(u1, u2)$, in a storage thereof, as a share value of ww' .

The apparatus 2 stores $(u2, u3)$, in a storage thereof, as a share value of ww' .

The apparatus 3 stores $(u3, u1)$, in a storage thereof, as a share value of ww' .

[0029] The following can be confirmed.

$$u1 + u2 + u3 = r1r1' + r1r2' + r2r1' + r2r2' + r2r3' + r3r2' + r3r3' + r3r1' + r1r3' + r1'' + r2'' + r3'' = (r1 + r2 + r3)(r1' + r2' + r3') + r1'' + r2'' + r3'' = ww' \bmod p.$$

[0030] From the values stored in apparatus 1 and apparatus 2 by using the same computation method, $ww' \bmod p$ can be calculated. The same applies to combinations of other apparatuses. According to such a method, the multiplication on w and w' both shared by using (2, 3) type RSS is executed without reconstructing each value, and a value obtained by sharing of ww' by applying (2, 3) type RSS can be shared.

[0031] <Generation of Random Numbers>

The following describes a method for generating three values, addition of which become 0, without communication among the apparatus 1, the apparatus 2 and the apparatus 3, in large quantities, in such a manner in which a value that the apparatus possess is not known to other apparatuses. Here, a method for generating $r[i, 1]$, $r[i, 2]$, $r[i, 3]$, which satisfy

$$r[i, 1] + r[i, 2] + r[i, 3] = 0 \bmod 2^n, \text{ for } i = 1, \dots, N, \text{ where } N \text{ is a relatively large number, will be described.}$$

[0032] Suppose a pseudo random number generator (PRG) outputting an n -bit numeric string with key and index as input is provided. The index may be a counter or the like. This method is described in NPL 3 and the like.

[0033] First of all, as a setup process of the apparatus, $L1$, $L2$, and $L3$ which are keys of PRG are generated. Let $L1$ and $L3$ be stored in the apparatus 1, $L2$ and $L1$ in the apparatus 2 and $L3$ and $L2$ in the apparatus 3.

[0034] It is assumed that each of the apparatuses 1 to 3 shares an index idx synchronized

with a counter or the like.

[0035] The apparatus 1 supplies the key L1 and the index idx to the PRG, and generates, as an output of the RPG, a value of n bits numeric value $r'[1]$. The apparatus 1 also supplies the key L3 and index idx to the PRG, and generates, as an output of the RPG, a value of n bits numeric value $r'[3]$. Then, the apparatus 1 obtains:

$$r[1] = r'[1] - r'[3] \bmod p.$$

[0036] The apparatus 2 supplies the key L2 and the index idx to the PRG, and generates, as an output of the RPG, the value of n bits numeric value $r'[2]$. The apparatus 2 also supplies the key L1 and index idx into PRG, and generates, as an output of the RPG, a value of n bits numeric value $r'[1]$. Then, the apparatus 2 obtains:

$$r[2] = r'[2] - r'[1] \bmod p.$$

[0037] The apparatus 3 supplies the key L3 and the index idx to the PRG, and generates, as an output of the RPG, n bits numeric value $r'[3]$. The apparatus 2 also supplies the key L2 and index idx into PRG, and generates, as an output of the RPG, a value of n bits numeric value $r'[2]$. Then, the apparatus 3 obtains:

$$r[3] = r'[3] - r'[2] \bmod p.$$

[0038] The following holds:

$$r[1] + r[2] + r[3] = r'[1] - r'[3] + r'[2] - r'[1] + r[3] - r[2] = 0 \bmod p.$$

[0039] All N sets satisfy the above condition.

[0040] Focusing attention on the value: $r[1] = r'[1] - r'[3] \bmod p$ that is generated by the apparatus 1, the apparatus 3 cannot obtain $r'[1]$, and the apparatus 2 cannot obtain $r'[3]$.

[0041] From this, it can be seen that the apparatus 2 and the apparatus 3 cannot calculate $r[1]$. The same may be said to $r[2]$ and $r[3]$.

[0042] As long as the setup process has been completed, the above process can be executed, even before the computation is performed, for example.

[0043] In the above described secure computation using the (2, 3) type RSS, if $p = 2$, multiplication can be regarded as AND (logical product) processing and addition / subtraction can be regarded as exclusive OR processing. Thus, when $p = 2$, it may be said that the above computation is secure computation suited to logic operation. Also, assuming that all items of share information of the apparatuses 1 to 3 are (1, 1), (1, 1), and (1, 1), these becomes share information of a value 1, with $r1 = 1$, $r2 = 1$, and $r3 = 1$, thereby forming a complete system with a logical product, an exclusive OR, and a constant 1 to allow arbitrary operation to be executed.

[0044] The above method is described in NPL 1 and the like. Various variations can be adopted as such a method. For example, regarding $r1+r2+r3= w \bmod p$, $(r1 - r2 \bmod p, r2)$, $(r2 - r3 \bmod p, r3)$, and $(r3 - r1 \bmod p, r1)$, may be used as share information. A scheme in which 3 apparatuses each hold information corresponding to two different sets out of $r1, r2$, and $r3$ may be called as (2, 3) type RSS.

- [0045] Regarding RSS, an arbitrary operation can be processed by using (2, 3) type RSS with $p = 2$. However, since it is inefficient to execute all processing with logical operation, such an operation that can be configured by multiplication and addition had better to be performed by secure computation using (2, 3) type RSS with p set to a larger value.
- [0046] In addition, there are cases where it is desirable to combine numerical operation and logical operation. As an example, in a case of receiving a , b and c as inputs and processing $a * b \bmod 2^4 < c$, with a , b , and c being smaller than 2^4 (where $\wedge$ is a power operator), it is desirable to process $a * b$ as a numerical operation, and to process comparison operation as a logical operation. Although it is desirable to compute $a * b$ as a numerical operation, it is difficult to express the process of comparing $a * b$ with c as a numerical operation.
- [0047] In order to solve such a problem, a process called bit decomposition described in NPL 2 is known. Bit decomposition is a process for converting share information for numerical computation into share information for logical operation.
- [0048] It is assumed that sharing of a value $w = 5$ is performed by (2, 3) type RSS using $p = 8$, and the apparatus 1 stores (1, 2), the apparatus 2 stores (2, 2) and the apparatus 3 stores (2, 1).
- [0049] By using bit decomposition, from these items of information, it is possible to obtain share information for each bit of 1, 0, and 1, of a binary representation of 5 (=101).
- [0050] More specifically, after bit decomposition is performed, the apparatus 1 possesses (1, 1) for the first bit, (0, 1) for the second bit, (1, 0) for the third bit, and (0, 0) for the fourth bit.
- The apparatus 2 possesses (1, 1) for the first bit, (1, 1) for the second bit, (0, 0) for the third bit, and (0, 0) for the fourth bit.
- The apparatus 3 possesses (1, 1) for the first bit, (1, 0) for the second bit, (0, 0) for the third bit, and (0, 0) for the fourth bit.
- [0051] The following describes the outline of the method described in NPL 2, as a related technique regarding bit decomposition. This method performs bit decomposition in the following procedure.
- [0052] It is assumed that a value to be decomposed is shared by using r_1 , r_2 , and r_3 which satisfy $r = r_1 + r_2 + r_3 \bmod p$. NPL 2 uses a Mersenne prime number represented by $p = 2^n - 1$. Properties of a Mersenne prime number contribute to efficient computation of s in step 2.
- [0053] <Procedure 1>
Execute sharing of $r_{12} = r_1 + r_2 \bmod p$, and r_3 .
- [0054] <Procedure 2>
Determine whether or not $r_{12} + r_3$ is greater than p , and execute secure computation,

such that $s = 1$, if $12 + r3$ is greater than p , and $s = 0$ otherwise.

[0055] <Procedure 3>

Execute secret computation of $r12 + r3 + s \bmod 2^n$ by a full adder for each bit from a lower digit.

[0056] According to the method of NPL 2, there is description that bit decomposition can be performed by communication amount of $10n + 4$ bits, assuming that p is a number of n bits.

Citation List

Non Patent Literature

[0057] NPL 1: Koji CHIDA, Dai IKARASHI, Koki HAMADA and Katsumi TAKAHASHI, "A Lightweight Three-party Secure Function Evaluation with Error Detection and Its Experimental Result", Vol. 52, No.9, 2674-2685, Sep. 2011

NPL 2: Dai IKARASHI, Koki HAMADA, Ryo KIKUCHI and Koji CHIDA, "O(1) Bits Communication Bit Decomposition and O($\log l$) Bits Communication Modulus Conversion for Small k secret-sharing-based Secure Computation", Computer Security Symposium 2013, 21-23 October 2013

NPL 3: Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof and Kazuma Ohara, "High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority", CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Pages 805-817

Summary of Invention

Technical Problem

[0058] The disclosures of Non Patent Literatures 1 to 3 given above are hereby incorporated in their entirety by reference into this specification. The following analysis is made by the inventors of the present invention.

[0059] As described above, according to NPL 2, bit decomposition can be performed by communication amount of $10n + 4$ bits, assuming that p is a number of n bits.

[0060] It is desirable to implement such a scheme whereby bit decomposition can be executed efficiently with a reduced communication amount, or, less than that of NPL 2, for example.

[0061] Accordingly, it is an object of the present invention to provide an apparatus, method, and program, each enabling bit decomposition and/or bit combining with less communication amount to realize efficient execution of secure computation.

Solution to Problem

[0062] According to an aspect of the present invention, there is provided a bit decomposition secure computing system comprising:

a share value storage apparatus to store share values obtained (distributed) by (2, 3)

type RSS (Replication type Secret Sharing) using modulo of power of 2 arithmetic, a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic; and a bit decomposition secure computation apparatus, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 randomly selected and satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, being used as share information by the (2, 3) type RSS stored in the share value storage apparatus, the bit decomposition secure computation apparatus includes: an addition sharing unit that sums two values out of r_1 , r_2 and r_3 by modulo 2^n arithmetic, generates and distributes a share value with respect to the sum by the (2, 3) type RSS; and a full adder secure computation unit that executes addition processing of the value generated by the addition sharing unit and a value not used by the addition sharing unit, for each digit, by using secure computation of a full adder, and stores the result in the decomposed share value storage apparatus.

[0063] According to another aspect of the present invention, there is provided a bit decomposition secure computation system comprising: a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS (Replication type Secret Sharing) using modulo of power of 2 arithmetic;

a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by applying (2, 3) type RSS using modulo 2 arithmetic; and

a bit decomposition secure computation apparatus, wherein

with respect to sharing of a value w , r_1 , r_2 , and r_3 randomly selected and satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, being used as share information by the (2, 3) type RSS stored in the share value storage apparatus, the bit decomposition secure computation apparatus includes

a full adder secure computation unit that performs secure computation of $r_{12} = r_1 + r_2 \bmod 2^n$ and secure computation of $r_{123} = r_{12} + r_3 \bmod 2^n$, for each digit, by using secure computation of a full adder, and stores the computation result in the decomposed share value storage apparatus.

[0064] According to a further aspect of the present invention, there is provided a bit combining secure computing system comprising:

a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS (Replication type Secret Sharing) using modulo of power of 2 arithmetic;

a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic; and

a bit combining secure computation apparatus, wherein

with respect to sharing of a value w_i , $r_{\{1, i\}}$, $r_{\{2, i\}}$, $r_{\{3, i\}}$ randomly selected

and satisfying $w_i = r_{\{1, i\}} + r_{\{2, i\}} + r_{\{3, i\}} \bmod 2$, for $i=1$ to n , being used as a sequence of n items of share information by the (2, 3) type RSS stored in the decomposed share value storage apparatus, the bit combining secure computation apparatus includes

a full adder secure computation unit that performs secure computation of $r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n$, where a symbol $\parallel$ is a concatenation operator, ^{n} is a power operator and n is a preset positive integer, and performs secure computation of $r_{123} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n$, for each digit, by using secure computation of a full adder, and stores the computation result in the share value storage apparatus.

[0065] According to an aspect of the present invention, there is provided a method in a computer system for providing bit decomposition secure computing, the method comprising:

an addition sharing step that sums two values out of r_1 , r_2 and r_3 by modulo 2^n , generates and distributes a share value by the (2, 3) type RSS (Replication type Secret Sharing) scheme with respect to the sum, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 randomly selected and satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS stored in a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS using modulo of power of 2 arithmetic; and

a full adder secure computation step that executes addition processing of the value generated by the addition sharing step and a value not used by the addition sharing step, for each digit, by using secure computation of a full adder, and stores the result in a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic.

[0066] According to another aspect of the present invention, there is provided a method in a computer system for providing bit decomposition secure computing, the method comprising

a full adder secure computation step that performs secure computation of $r_{12} = r_1 + r_2 \bmod 2^n$ and secure computation of $r_{123} = r_{12} + r_3 \bmod 2^n$, for each digit, by using secure computation of a full adder, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 randomly selected and satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS (Replication type Secret Sharing) scheme stored in a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS using modulo of power of 2 arithmetic; and

stores the computation result in a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2

arithmetic.

[0067] According to a further aspect of the present invention, there is provided a method in a computer system for providing bit combining secure computing, the method comprising

a full adder secure computation step that performs secure computation of $r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n$, where a symbol $\parallel$ is a concatenation operator, ^{n} is a power operator and n is a preset positive integer, and performs secure computation of $r_{123} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n$, for each digit by secure computation of a full adder, wherein with respect to sharing of a value w_i , $r_{\{1, i\}}$, $r_{\{2, i\}}$, $r_{\{3, i\}}$ randomly selected and satisfying $w_i = r_{\{1, i\}} + r_{\{2, i\}} + r_{\{3, i\}} \bmod 2$, for $i=1$ to n , are used as a sequence of n items of share information by the (2, 3) type RSS stored in a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic; and

stores the computation results in a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS using modulo of power of 2 arithmetic.

[0068] According to an aspect of the present invention, there is provided a program causing a computer to execute bit decomposition secure computing processing comprising:

an addition sharing process that sums two values out of r_1 , r_2 and r_3 by modulo 2^n , generates and distributes a share value by the (2, 3) type RSS (Replication type Secret Sharing) scheme with respect to the sum, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 randomly selected and satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS stored in a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS using modulo of power of 2 arithmetic; and

a full adder secure computation process that executes addition processing of the value generated by the addition sharing process and a value not used by the addition sharing process, for each digit, by using secure computation of a full adder, and stores the result in a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic.

[0069] According to another aspect of the present invention, there is provided a program causing a computer to execute bit decomposition secure computing processing comprising:

a full adder secure computation process that performs secure computation of $r_{12} = r_1 + r_2 \bmod 2^n$ and secure computation of $r_{123} = r_{12} + r_3 \bmod 2^n$, for each digit, by using secure computation of a full adder, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 randomly selected and satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a

power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS (Replication type Secret Sharing) scheme stored in a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS using modulo of power of 2 arithmetic; and stores the computation result in a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic.

[0070] According to a further aspect of the present invention, there is provided a program causing a computer to execute bit combining secure computing processing comprising: a full adder secure computation process that performs secure computation of $r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n$, where a symbol $\parallel$ is a concatenation operator, ^{n} is a power operator and n is a preset positive integer, and performs secure computation of $r_{123} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n$, for each digit by secure computation of a full adder, wherein with respect to sharing of a value w_i , $r_{\{1, i\}}$, $r_{\{2, i\}}$, $r_{\{3, i\}}$ randomly selected and satisfying $w_i = r_{\{1, i\}} + r_{\{2, i\}} + r_{\{3, i\}} \bmod 2$, for $i=1$ to n , are used as a sequence of n items of share information by the (2, 3) type RSS stored in a decomposed share value storage apparatus to store a sequence of share values obtained (distributed) by (2, 3) type RSS using modulo 2 arithmetic;

stores the computation results in a share value storage apparatus to store share values obtained (distributed) by (2, 3) type RSS using modulo of power of 2 arithmetic.

[0071] According to yet another aspect of the present invention, there is provided a non-transitory computer-readable recording medium storing therein the above program, such as a semiconductor memory such as random access memory (RAM), a read only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a universal serial bus (USB) device, and solid state drive (SSD), or a storage device such as a Hard Disk Drive (HDD), a Compact Disc (CD), or Digital Versatile Disc (DVD) and so forth.

Advantageous Effects of Invention

[0072] According to the present invention, bit decomposition and/or bit combining can be executed with less communication amount to make secure computation more efficient.

Still other features and advantages of the present invention will become readily apparent to those skilled in this art from the following detailed description in conjunction with the accompanying drawings wherein only example embodiments of the invention are shown and described, simply by way of illustration of the best mode contemplated of carrying out this invention. As will be realized, the invention is capable of other and different embodiments, and its several details are capable of modifications in

various obvious respects, all without departing from the invention. Accordingly, the drawing and description are to be regarded as illustrative in nature, and not as restrictive.

Brief Description of Drawings

- [0073] [fig.1]FIG. 1 is a diagram illustrating an arrangement of a first example embodiment.
- [fig.2]FIG. 2 is a flowchart illustrating an operation of the first example embodiment of the present invention.
- [fig.3]FIG. 3 is a diagram illustrating an arrangement of a second example embodiment.
- [fig.4]FIG. 4 is a flowchart illustrating an operation of the second example embodiment of the present invention.
- [fig.5]FIG. 5 is a diagram illustrating an arrangement of a third example embodiment.
- [fig.6]FIG. 6 is a flowchart illustrating an operation of the third example embodiment of the present invention.
- [fig.7]FIG. 7 is a diagram illustrating an arrangement of a fourth example embodiment of the present invention.

Description of Embodiments

- [0074] Example embodiments will be described with reference to drawings. According to the method of the above described NPL 2, sharing of r_3 is performed in the above described Procedure 1. A method for executing this processing without communication will be described.
- [0075] Suppose that sharing of a value is performed by using r_1 , r_2 , and r_3 satisfying $r = r_1 + r_2 + r_3 \bmod p$ as shares.
- [0076] When generating shares related to r_i ($i = 1, 2, 3$) satisfying $r = r_1 + r_2 + r_3 \bmod p$, the value obtained by setting all the values to zero other than a portion relating r_i of share information of $r = r_1 + r_2 + r_3 \bmod p$ is the share information of r_i .
- [0077] Suppose that the apparatus 1 retains (r_2 , r_3), the apparatus 2 retains (r_3 , r_1), and the apparatus 3 retains (r_1 , r_2).
- For example, if all other than a portion relating to r_1 are set to zero, the apparatus 1 will possess (0, 0), the apparatus 2 will possess (0, r_1), and the apparatus 3 will possess (r_1 , 0), which can be made share information of r_1 .
- [0078] The fact that the apparatuses 2 and 3 retain r_1 itself has no influence on confidentiality. This is because they are values that can be grasped originally. Similarly, for r_2 and r_3 , the share information can be obtained without communicating among apparatuses.
- [0079] The reason that s is added in the above described Procedure 3, i.e., $r_1^2 + r_3 + s \bmod 2^n$, according to the method according to NPL 2, is to obtain $r_1^2 + r_3 \bmod p$, by the

secret computation of $\text{mod } 2^n$.

[0080] In the case of $s = 1$, if $r_{12} + r_3 = r' + p$, then the following holds:

$$r' + p \bmod p = r' + p + 1 = r' + 2^n \bmod 2^n.$$

[0081] In the case of $s = 0$, if $r_{12} + r_3 = r'$, then $r' \bmod p = r' \bmod 2^n$.

[0082] From above, irrespective of the value of s , the computation result of the above described Procedure 3 is $r_{12} + r_3 \bmod p$.

[0083] However, if 2^n is used as p , the processing that is executed when $r_{12} + r_3$ exceeds 2^n is unnecessary.

[0084] <Modes>

The following describes the bit decomposition method with the above described modification added as one of modes of the present invention.

[0085] <Procedure 1>

Execute sharing of $r_{12} = r_1 + r_2 \bmod 2^n$.

[0086] <Procedure 2>

Generate share of r_3 on each apparatus.

[0087] <Procedure 3>

Execute secret computation of a full adder for each bit from a lower digit to compute $r_{12} + r_3 + s \bmod 2^n$.

[0088] The following evaluates a communication amount of the above processing.

Let r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$ be randomly selected and be stored as follows.

(r_1 , r_2) is stored as a share value of w in the apparatus 1.

(r_2 , r_3) is stored as a share value of w in the apparatus 2.

(r_3 , r_1) is stored as a share value of w in the apparatus 3.

[0089] <Communication amount of Procedure 1>

Distribution of $r_1 + r_2$ is performed by the apparatus 1. First, the apparatus 1 computes $r_{12} = r_1 + r_2 \bmod 2^n$ and randomly selects r_{12A} and r_{12B} satisfying $r_{12A} + r_{12B} = r_{12} \bmod 2^n$.

[0090] Next, the apparatus 1 sends r_{12A} and r_{12B} to the apparatus 2 and the apparatus 3, respectively.

[0091] At this time, the apparatus 1 obtains (r_{12B} , r_{12A}) as a share value of r_{12} , the apparatus 2 obtains (r_{12A} , 0) as a share value of r_{12} , and the apparatus 3 obtains (0, r_{12B}) as a share value of r_{12} .

In this process, $2n$ bit communication is performed.

[0092] <Communication amount of Procedure 2>

As described above, share information of r_3 can be generated without communication.

[0093] <Communication amount of Procedure 3>

The secure computation of an full adder requires one AND operation to calculate carry of each digit. Therefore, in the case of addition of n digits, communication of $3 * (n - 1)$ bits is required.

[0094] As a result, it can be seen that the bit decomposition can be calculated with the communication amount of $5n-3$ bits. The following describes an example for explaining how to divide the computation result into bit units by processing of an adder.

[0095] The computation process of decomposition will be described for $p = 8$, $r = 6$ (110 in binary representation), $r_1 = 3$ (011 in binary representation), $r_2 = 2$ (010 in binary representation), $r_3 = 1$ (001 in binary representation).

[0096] Let j-th digit of r_i from a lowest digit be r_{i_j} , j-th digit of $r_1 r_2 \bmod 8$ be r_{12_j} , and j-th digit of $r_1 + r_2 + r_3 \bmod 8$ be r_{123_j} .

[0097] Next, a procedure for computing
 $r_{12} + r_3 \bmod 8 = 5 + 1 \bmod 8 = 6$
 from the lowest digit will be described.

[0098] <First Digit>

Computation of the first digit is as follows:

$$r_{123_1} = r_{12_1} \text{ XOR } r_{3_1} = 0 \text{ XOR } 1 \text{ XOR } 1 = 0,$$

where XOR is a bitwise exclusive OR.

Carry with respect to the computation of the first digit is as follows:

$$c_1 = r_{12_1} \text{ AND } r_{3_1} = 1 \text{ AND } 1 = 1$$

(In the first digit, there is no carry (carry) from a lower digit.)

[0099] <Second Digit>

Computation of the second digit is as follows:

$$r_{123_2} = r_{12_2} \text{ XOR } r_{3_2} \text{ XOR } c_1 = 0 \text{ XOR } 0 \text{ XOR } 1 = 1$$

Carry with respect to the computation of the second digit is as follows:

$$c_2 = c_1 \text{ XOR } (1 \text{ XOR } r_{12_2} \text{ XOR } r_{3_2}) \text{ AND } (r_{3_2} \text{ XOR } c_1) = 1 \text{ XOR } (1 \text{ XOR } 0 \text{ XOR } 0) \text{ AND } (0 \text{ XOR } 1) = 0$$

[0100] <Third Digit>

Computation of the third digit is as follows:

$$r_{123_3} = r_{12_3} \text{ XOR } r_{3_3} \text{ XOR } c_2 = 1 \text{ XOR } 0 \text{ XOR } 0 = 1$$

[0101] As described above, it is possible to compute the value obtained by decomposing each digit bit by bit, with one AND processing, as with $r_{123_1} = 0$, $r_{123_2} = 1$, and $r_{123_3} = 1$. This process can be executed by secure computation. The result of the secure computation is a share value of the value obtained by decomposition for each bit.

[0102] In the above case, as (2, 3) threshold type RSS,
 the apparatus 1 holds (r_1 , r_2),
 the apparatus 2 holds (r_2 , r_3), and

the apparatus 3 holds (r_3, r_1) , with the value w given as follows:

$$w = r_1 + r_2 + r_3 \bmod p.$$

- [0103] However, the present invention is applicable as long as it is a (2, 3) threshold type RSS that holds information corresponding to two different values among three values of r_1 , r_2 , and r_3 . For example, the apparatus 2 may hold $(r_2 + r_3, r_3)$ instead of (r_2, r_3) , or even a method can be also implemented in which the apparatus 2 holds $(r_2 - r_3, r_2 + r_3)$, and so forth, as long as a secure computation is equipped with addition, multiplication and constant.
- [0104] Alternatively, at first, $r_{12} = r_1 + r_2 \bmod 2^n$ is calculated by secure computation, and then operation on $r_{12} + r_3$ may be executed by secure computation a full adder. When using this method, the communication amount for calculating r_{12} is $3n$ bits, which is rather inefficient as compared with a case where the apparatus 1 distributes, but the total communication amount is $6n - 3$ bits.
- [0105] When computation of $r_1 + r_2$ is performed by secure computation of a full adder, there is no need to perform computation for a carry generated from the most significant digit, so computation on r_{12} can be executed by a communication amount of $3n - 3$ bit. In this case, it is possible to execute bit decomposition with the communication amount of $6n - 6$ bits.
- [0106] These variations are also more efficient than the method according to NPL 2.
- [0107] Also, if both processing ($r_{12} = r_1 + r_2 \bmod 2^n$ and $r_{12} + r_3 \bmod 2^n$) are to be executed using secure computation of a full adder, it is possible to use a mechanism for giving tolerance against fraud on the secure computation method using (2, 3) type RSS as described in NPL 3.
- [0108] Furthermore, it is also possible to create share information for a combined value from bit decomposed share information. Carry computation for each carry from a low order digit to a high order digit is executed by secure computation and when carry computation for the entire digits is finished, the secure computation result of each digit are combined.
- [0109] In this method, since there is no subject (party) holding information equivalent to $r_1 + r_2 \bmod 2^n$, both $r_{12} = r_1 + r_2 \bmod 2^n$, and $r_{12} + r_3 \bmod 2^n$ are computed by secure computation of a full adder.
- [0110] When computation of the full adder is executed sequentially from a lower digit, $n-1$ AND operations are generated. As a result, the number of times of communication is $n-1$. In order to reduce this number, a carry save adder may be used, in which the number of AND operations increases but a depth of the circuit can be made shallow.
- [0111] <Example Embodiments>
- Configuration and operation of a first embodiment of the present invention will be described with reference to the drawings.

[0112] <Example Embodiment 1>

In the first embodiment, when sharing of w is performed by a (2, 3) type RSS scheme using r_1 , r_2 , and r_3 which are randomly selected to satisfy $w = r_1 + r_2 + r_3 \bmod 2^n$, one apparatus distributes r_1 and r_2 and executes $r_1 + r_2 \bmod 2^n$ and $r_1 + r_2 + r_3 \bmod 2^n$ by using secure computation of a full adder, thereby generating bit decomposed share information.

[0113] Fig. 1 is a block diagram illustrating an arrangement of the first example embodiment of the present invention. Referring to Fig. 1, a bit decomposition secure computing system 10 according to the first embodiment of the present invention includes a share value storage apparatus 100 that stores share values obtained by applying (2, 3) type RSS using 2^n as p , a decomposed share value storage apparatus 200 that stores bit decomposed share information, and a bit decomposition secure computation apparatus 300 that reads share values stored in the share value storage apparatus 100 and stores bit decomposed values in the decomposed share value storage apparatus 200.

[0114] In the first example embodiment, there are provided three sets of apparatuses, wherein the apparatuses 100, 200, and 300 in Fig. 1 constitute one set. That is, there are provided three sets of the systems 10. The apparatuses 100, 200, and 300 or any two apparatuses selected from the apparatuses 100, 200, and 300 may be arranged in one unit, or may be arranged in a distributed manner wherein, for example, at least between the apparatuses 100 and 200 and between the apparatuses 200 and 300, there may be provided one or more communication paths such as local area network (LAN) and/or wide area network (WAN). Note that in Fig. 1, arrowed lines between the apparatuses 100 and 300 and between the apparatuses 300 and 200 each only indicate an example of data flow. The communications between the apparatuses 100 and 300 and between the apparatuses 300 and 200 are as a matter of course not limited to the direction of the arrowed line. The same can be said in later-described other embodiments.

[0115] The share value storage apparatus 100 includes a first share value storage unit 101 and a second share value storage unit 102. The first share value storage unit 101 and the second share value storage unit 102 store respectively share values (first share and second share) in such a way that it can be understood which values out of the three values used for generating share information by the (2, 3) type RSS scheme are used and how the values are processed to obtain the stored share value.

[0116] The decomposed share value storage apparatus 200 includes a first decomposed share value storage unit 201 and a second decomposed share value storage unit 202. The first decomposed share value storage unit 201 and the second decomposed share value storage unit 202 store respectively the share information (first share value and second share value) in such a way that it can be understood which share values out of the three

values used for generating share information by the (2, 3) type RSS scheme are used and how the values are processed to obtain the stored share information.

- [0117] The bit decomposition secure computation apparatus 300 includes an addition sharing unit 301, a partial share information extraction unit 302, and a full adder secure computation unit 303. The bit decomposition secure computation apparatus 300 reads share values stored in the first share value storage unit 101 and the second share value storage unit 102 of the share value storage apparatus 100, communicates with another bit decomposition secure computation apparatus 300 (not shown), and stores information (bit decomposed share value) in the first decomposed share value storage unit 201 and the second decomposed share value storage unit 202 of the decomposed share value storage apparatus 200.
- [0118] The addition sharing unit 301, using two indices out of the three values constituting share information by (2, 3) type RSS, as inputs, reads share value(s) stored in the share value storage apparatus 100. If the share value storage apparatus 100 stores share values of both two indices, the addition sharing unit 301 generates share information by the (2, 3) type RSS with respect to a sum of the share values of the two indices and sends the generated share information to the addition sharing units 301 of other two apparatuses (not shown).
- [0119] The partial share information extraction unit 302, using one index out of the three values constituting share information by (2, 3) type RSS scheme, as input, reads the value stored in the share value storage apparatus 100, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by (2, 3) type RSS scheme.
- [0120] The full adder secure computation unit 303 performs addition processing using secure computation of a full adder on the share information by (2, 3) type RSS generated and distributed by the addition sharing unit 301 and the share information by (2, 3) type RSS scheme generated by the partial share information extraction unit 302, and stores the value obtained by combining the share information of the computation result for each bit obtained for each bit in the decomposed share value storage apparatus 200.
- [0121] Fig. 2 is a flowchart illustrating an operation of the first example embodiment of the present invention. It is assumed that in the share value storage apparatus 100, share values that are shared with the (2, 3) type RSS by using r_1 , r_2 , and r_3 satisfying $r = r_1 + r_2 + r_3 \bmod 2^n$ are stored.
- [0122] In the operation of the first example embodiment,
 $r_{ij} = r_i + r_j \bmod 2^n$ is shared, and
 addition of r_{ij} and r_k is executed by secure computation of a full adder.
 Any combination of i , j , and k may be used as long as i , j and k are values different to

each other and selected from a combination of values 1, 2 and 3.

[0123] The following processing is executed by 3 sets of share value storage apparatuses 100, decomposed share value storage apparatuses 200, and bit decomposition secure computation apparatuses 300.

[0124] First, each addition sharing unit 301 decides whether or not the share value storage apparatus 100 associated with the bit decomposition secure computation apparatus 300 stores information on r_i and r_j . When stored, each addition sharing unit 301 computes $r_{ij} = r_i + r_j \bmod 2^n$ and then sends the computed result to the addition sharing unit 301 of the other two bit decomposition secure computation apparatuses 300. After that, each addition sharing unit 301 outputs the share information of r_{ij} (Step A1).

[0125] Next, the partial share information extraction unit 302 produces partial share information in which values other than the portion related to r_k are set to 0 from the values stored in the share value storage apparatus 100 (Step A2).

[0126] Next, the full adder secure computation 303 executes addition processing using secure computation of a full adder with respect to the share information of r_{ij} and the share information of r_k , and then stores a sequence of the results in the decomposed share value storage apparatus 200 (Step A3).

[0127] <Example Embodiment 2>

The following describes configuration and operation of a second example embodiment of the present invention with reference to the drawings.

[0128] In the second example embodiment, when w is shared by (2, 3) type RSS scheme using r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$,

$r_{12} = r_1 + r_2 \bmod 2^n$ is computed by secure computation of a full adder, and

$r_{12} + r_3 \bmod 2^n$ is computed from lower order bits by secure computation of a full adder.

[0129] Fig. 3 is a block diagram illustrating an arrangement of a second example embodiment of the present invention. Referring to Fig. 3, a bit decomposition secure computing system 10A according to the second embodiment of the present invention includes a share value storage apparatus 100 that stores share values obtained by applying (2, 3) type RSS scheme using 2^n as p , a decomposed share value storage apparatus 200 that stores bit decomposed share information, a bit decomposition apparatus 300 that reads share values stored in the share value storage apparatus 100 and stores bit decomposed values in the decomposed share value storage apparatus 200.

[0130] There are provided three sets of apparatuses, where apparatuses 100, 200, and 300 in Fig. 1 constitute one set, as with the first example embodiment. That is, there are provided three sets of the systems 10A.

- [0131] The share value storage apparatus 100 includes a first share value storage unit 101 and a second share value storage unit 102. The first share value storage unit 101 and the second share value storage unit 102 store share values in such a way that it can be understood which values out of the three values used for generating share information by (2, 3) type RSS are used and how the values are processed to obtain the stored share value.
- [0132] The decomposed share value storage apparatus 200 includes a first decomposed share value storage unit 201 and a second decomposed share value storage unit 202. The first decomposed share value storage unit 201 and the second decomposed share value storage unit 202 store the values (bit decomposed share values) in such a way that it can be understood which values out of the three values used for generating share information by (2, 3) type RSS are used and how the values are processed to obtain the stored share value.
- [0133] The bit decomposition secure computation apparatus 300 includes a partial share information extraction unit 302 and a full adder secure computation unit 303.
- [0134] The bit decomposition secure computation apparatus 300A reads values stored in the share value storage apparatus 100, communicates with other two bit decomposition secure computation apparatuses 300A, and stores information in the decomposed share value storage apparatus 200.
- [0135] The partial share information extraction unit 302 reads, using the index of one of the three values constituting share information by (2, 3) type RSS scheme, as an input, values stored in the share value storage apparatus 100, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by (2, 3) type RSS.
- [0136] The full adder secure computation apparatus 303A, using 3 sets of share information by the (2, 3) type RSS generated by the partial share information extraction unit 302 as inputs, executes secure computation of a full adder from low order bit, for the three values, and stores the share information of the computation result for each bit in the decomposed share value storage apparatus 200.
- [0137] Fig. 4 is a flowchart illustrating an operation of the second example embodiment of the present invention.
- [0138] In the share value storage apparatus 100, there are stored share values of n bit value r to be shared that have been obtained by applying (2, 3) type RSS scheme using r_1 , r_2 , and r_3 , which satisfy $r = r_1 + r_2 + r_3 \bmod 2^n$.
- In the operation of the second example embodiment,
 $r_{ij} = r_i + r_j \bmod 2^n$ is executed by secure computation of a full adder, and
 $r_{ij} + r_k \bmod 2^n$ is executed by secure computation of a full adder, where i, j, and

k are values different to each other and selected from a combination of values 1, 2 and 3.

[0139] The following processing is executed by the three sets of share value storage apparatuses 100, decomposed share value storage apparatuses 200, and bit decomposition secure computation apparatuses 300A.

[0140] First, the partial share information extraction unit 302 outputs partial share information in which values other than the portion related to r_i are regarded as 0 from the values stored in the share value storage apparatus 100. (Step B1)

[0141] Next, the partial share information extraction unit 302 outputs partial share information in which values other than the portion related to r_j are regarded as 0 from the values stored in the share value storage apparatus 100. (Step B2)

[0142] Next, the partial share information extraction unit 302 outputs partial share information in which values other than the portion related to r_k are regarded as 0 from the values stored in the share value storage apparatus 100. (Step B3)

[0143] Next, the full adder secure computation 303 executes secure computation of a full adder in descending order of the least significant bit with respect to the share information of r_i and the share information of r_j , and outputs a sequence of the results as the share information of r_{ij} . (Step B4)

[0144] Next, the full adder secure computation 303 executes secure computation of a full adder with respect to the share information of r_{ij} and the share information of r_k , and stores a sequence of the results in the decomposed share value storage apparatus 200. (Step B5).

[0145] <Example Embodiment 3>

The following describes a configuration and operation of a third example embodiment of the present invention with reference to the drawings.

[0146] In the third example embodiment, with respect to $i = 1, \dots, N$, when a bit w_i is shared by (2, 3) type RSS using $r_{\{i, 1\}}$, $r_{\{i, 2\}}$, $r_{\{i, 3\}}$ satisfying $w = r_{\{i, 1\}} + r_{\{i, 2\}} + r_{\{i, 3\}} \bmod 2$, bit combining is performed by executing by secure computation of a full adder,

$$r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n; \text{ and}$$

$$r_{12} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n,$$

where a symbol $\parallel$ is a bit concatenation operator.

[0147] Fig. 5 is a block diagram illustrating an arrangement of the third embodiment of the present invention. Referring to Fig. 5, a bit combining secure computing system 20 according to the third embodiment of the present invention comprises a share value storage apparatus 100 that stores share values obtained by applying (2, 3) type RSS using 2^n as p , a bit decomposed share value storage apparatus 200 that stores the share information, and a bit combining secure computation apparatus 400 that reads

the values stored in the decomposed share value storage apparatus 200 and stores the values in the share value storage apparatus 100.

[0148] There are provided three sets of apparatuses, where apparatuses 100, 200, and 400 in Fig. 5 constitute one set. That is, there are provided three sets of the systems 20.

[0149] The share value storage apparatus 100 includes a first share value storage unit 101 and a second share value storage unit 102. The first share value storage unit 101 and the second share value storage unit 102 store share values in such a way that it can be understood which values out of the three values used for generating share information by (2, 3) type RSS scheme are used and how the values are processed to obtain the stored share value.

[0150] The decomposed share value storage apparatus 200 includes a first decomposed share value storage unit 201 and a second decomposed share value storage unit 202. The first decomposed share value storage unit 201 and the second decomposed share value storage unit 202 store share values in such a way that it can be understood which values out of the three values used for generating share information by (2, 3) type RSS are used and how the values are processed to obtain the stored share value.

[0151] The bit combining secure computation apparatus 400 includes a partial share information extraction unit 302, and a full adder secure computation unit 303.

[0152] The bit combining secure computation apparatus 400 reads values stored in the decomposed share value storage apparatus 200, communicates with other binding secure computation apparatuses 400 and stores information in the share value storage apparatus 100.

[0153] The partial share information extraction unit 302 extracts, using an index of one of three values constituting share information by (2, 3) type RSS, as an input, reads the value stored in the decomposed share value storage apparatus 200 and generates share information obtained by setting values to zero except for one of the three values constituting the share information by (2, 3) type RSS.

[0154] The full adder secure computation unit 303 receives, as inputs, 3 sets of share information by the (2, 3) type RSS generated by the partial share information extraction unit 302, executes secure computation of a full adder, from low order bit of respective three values, and then stores share information of the computation result for each bit in the share value storage apparatus 100.

[0155] Fig. 6 is a flowchart illustrating an operation of the third embodiment of the present invention. It is assumed that the decomposed share value storage apparatus 200 stores share values shared with (2,3) type RSS using $r_{\{i, 1\}}$, $r_{\{i, 2\}}$, $r_{\{i, 3\}}$ satisfying $r_i = r_{\{i, 1\}} + r_{\{i, 2\}} + r_{\{i, 3\}} \bmod 2$.

[0156] In the operation of the third example embodiment,

$$r_{ij} = r_{\{i, n\}} \parallel \dots \parallel r_{\{i, 1\}} + r_{\{j, n\}} \parallel \dots \parallel r_{\{j, 1\}} \bmod 2^n$$

is executed by secure computation of a full adder, and

$$r_{ij} + r_{\{k, n\}} \parallel \dots r_{\{k, 1\}} \bmod 2^n$$

is executed by secure computation of a full adder, where indices i, j, and k are values different to each other and selected from a combination of values 1, 2, and 3.

[0157] The following processing is executed by the three sets of share value storage apparatuses 100, decomposed share value storage apparatuses 200, and bit combining secure computation apparatuses 400.

[0158] First, the partial share information extraction unit 302 outputs partially decomposed share information in which values other than a portion related to $r_{\{i, n\}} \parallel \dots \parallel r_{\{i, 1\}}$ are regarded as 0 from the values stored in the decomposed share storage apparatus 200 (Step C1).

[0159] Next, the partial share information extraction unit 302 extracts partially decomposed share information in which values other than a portion relating to $r_{\{j, n\}} \parallel \dots \parallel r_{\{j, 1\}}$ are regarded as 0 from the values stored in the decomposed share value storage apparatus 200 (Step C2).

[0160] Next, the partial share information extraction unit 302 extracts partially decomposed share information in which values other than a portion relating to $r_{\{k, n\}} \parallel \dots \parallel r_{\{k, 1\}}$ are regarded as 0 from the values stored in the decomposed share value storage apparatus 200 (Step C3).

[0161] Next, the full adder secure computation unit 303 performs secure computation of a full adder for partially decomposed share information of $r_{\{i, n\}} \parallel \dots \parallel r_{\{i, 1\}}$ and partially decomposed share information of $r_{\{j, n\}} \parallel \dots \parallel r_{\{j, 1\}}$ and outputs a sequence of the results, as share information of r_{ij} (Step C4).

[0162] Next, the full adder secure computation unit 303 performs secure computation of a full adder for the share information of r_{ij} and the partially decomposed share information of $r_{\{k, n\}} \parallel \dots \parallel r_{\{k, 1\}}$, and stores the result in the share value storage apparatus 100 (Step C5).

[0163] The bit decomposition secure computing systems 10 and 10A in respectively described in the first and second embodiments may be implemented on a computer system as illustrated in Fig. 7, for example. Referring to FIG. 7, a computer system 500, such as a server system, includes a processor (Central Processing Unit) 502, a memory 504 including, for example, a semiconductor memory (for example, Random Access Memory (RAM), Read Only Memory (ROM), Electrically Erasable and Programmable ROM (EEPROM), and/or a storage device including at least one of Hard Disk Drive (HDD), Compact Disc (CD), Digital Versatile Disc (DVD) and so forth, a display device 506, and a communication interface 508. The communication interface 508 (such as a network interface controller (NIC)) may well be configured to communicate with other computer systems (parties) via LAN and/or WAN, for example. A

program for executing the process of the bit decomposition secure computation apparatus in Fig.1 or Fig. 3 is stored in a memory 504 and the processor 112 reads the program from the memory to execute the program to realize the bit decomposition secure computation. The memory 504 may includes the share value storage apparatus 100 and the decomposed Share value storage apparatus 200. The bit coupling secure computing system 20 in the third example embodiment may well be implemented on a computer system as illustrated in Fig. 7.

- [0164] According to the first and second example embodiments, it is possible to convert share value shared by (2, 3) type RSS into a value in which each bit is shared by (2, 3) type RSS.
- [0165] According to the third example embodiment, it is also possible to execute the reverse processing efficiently.
- [0166] With the processing, it becomes possible to efficiently execute such complex processing that combines secure computation of values and secure computation of bits.
- [0167] The disclosure of the aforementioned NPLs 1-3 is incorporated by reference herein. The particular exemplary embodiments or examples may be modified or adjusted within the scope of the entire disclosure of the present invention, inclusive of claims, based on the fundamental technical concept of the invention. In addition, a variety of combinations or selections of elements disclosed herein may be used within the concept of the claims. That is, the present invention may encompass a wide variety of modifications or corrections that may occur to those skilled in the art in accordance with the entire disclosure of the present invention, inclusive of claims and the technical concept of the present invention.

Reference Signs List

- [0168] 10, 10A bit decomposition secure computing system
- 20 bit coupling secure computing system
- 100 share value storage apparatus
- 101 first share value storage unit
- 102 2nd share value storage unit
- 200 decomposed Share value storage apparatus
- 201 first decomposed share value storage unit
- 202 second decomposed share value storage unit
- 300, 300A bit decomposition secure computation apparatus
- 301 addition sharing unit
- 302 partial share information extraction unit
- 303 full adder secure computation unit
- 400 bit combining secure computation apparatus

500 computer system

502 processor

504 memory

506 display

508 communication interface

Claims

- [Claim 1] A bit decomposition secure computing system comprising:
 a share value storage apparatus to store share values obtained by applying (2, 3) type RSS (Replication type Secret Sharing) using modulo of power of 2 arithmetic,
 a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic; and
 a bit decomposition secure computation apparatus, wherein
 with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where $^{\wedge}$ is a power operator and n is a preset positive integer, being used as share information by the (2, 3) type RSS stored in the share value storage apparatus,
 the bit decomposition secure computation apparatus includes:
 an addition sharing unit that sums two values out of r_1 , r_2 and r_3 by modulo 2^n arithmetic, generates and distributes a share value with respect to the sum by the (2, 3) type RSS; and
 a full adder secure computation unit that executes addition processing of the value generated by the addition sharing unit and a value not used by the addition sharing unit, for each digit, by using secure computation of a full adder, and stores the result in the decomposed share value storage apparatus.
- [Claim 2] A bit decomposition secure computation system comprising:
 a share value storage apparatus to store share values obtained by applying (2, 3) type RSS (Replication type Secret Sharing) using modulo of power of 2 arithmetic;
 a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic; and
 a bit decomposition secure computation apparatus, wherein
 with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where $^{\wedge}$ is a power operator and n is a preset positive integer, being used as share information by the (2, 3) type RSS stored in the share value storage apparatus, the bit decomposition secure computation apparatus includes
 a full adder secure computation unit that performs secure computation of $r_{12} = r_1 + r_2 \bmod 2^n$ and secure computation of $r_{123} = r_{12} + r_3$

mod 2^n , for each digit, by using secure computation of a full adder, and stores the computation result in the decomposed share value storage apparatus.

[Claim 3]

A bit combining secure computing system comprising:

a share value storage apparatus to store share values obtained by applying (2, 3) type RSS (Replication type Secret Sharing) using modulo of power of 2 arithmetic;

a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic; and

a bit combining secure computation apparatus, wherein

with respect to sharing of a value w_i , $r_{\{1, i\}}$, $r_{\{2, i\}}$, $r_{\{3, i\}}$

satisfying $w_i = r_{\{1, i\}} + r_{\{2, i\}} + r_{\{3, i\}} \bmod 2$, for $i=1$ to n , being used as a sequence of n items of share information by the (2, 3) type RSS stored in the decomposed share value storage apparatus, the bit combining secure computation apparatus includes

a full adder secure computation unit that performs secure computation of $r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n$, where a symbol $\parallel$ is a concatenation operator, ^{n} is a power operator and n is a preset positive integer, and performs secure computation of $r_{123} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n$, for each digit, by using secure computation of a full adder, and stores the computation result in the share value storage apparatus.

[Claim 4]

The bit decomposition secure computing system according to claim 1, wherein the bit decomposition secure computation apparatus includes a partial share information extraction unit that, using one index out of three values constituting share information by the (2, 3) type RSS, as input, reads the value stored in the share value storage apparatus, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by the (2, 3) type RSS, wherein

the full adder secure computation unit performs addition processing using secure computation of a full adder on the share information by the (2, 3) type RSS generated and distributed by the addition sharing unit and the share information by the (2, 3) type RSS generated by the partial share information extraction unit, and

stores the value obtained by combining the share information of the computation result, for each bit, in the decomposed share value storage

apparatus.

[Claim 5]

The bit decomposition secure computing system according to claim 2, wherein the bit decomposition secure computation apparatus includes a partial share information extraction unit that, using one index out of three values constituting share information by the (2, 3) type RSS, as input, reads the value stored in the share value storage apparatus, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by the (2, 3) type RSS, wherein the full adder secure computation unit, using 3 sets of share information by the (2, 3) type RSS generated by the partial share information extraction unit, including r_i , r_j , r_k , where i , j and k being different to each other and selected from 1 to 3, performs secure computation of $r_{ij} = r_i + r_j \bmod 2^n$, and secure computation of $r_{ij} + r_k \bmod 2^n$, by secure computation of a full adder, from low order bit, and stores a sequence of the computation result, for each bit in the decomposed share value storage apparatus.

[Claim 6]

The bit combining secure computing system according to claim 3, wherein the bit combining secure computation apparatus includes a partial share information extraction unit that, using one index out of three values constituting share information by the (2, 3) type RSS, as input, reads the value stored in the share value storage apparatus, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by the (2, 3) type RSS.

[Claim 7]

A method in a computer system for providing bit decomposition secure computing, the method comprising:

an addition sharing step that sums two values out of r_1 , r_2 and r_3 by modulo 2^n , generates and distributes a share value by the (2, 3) type RSS (Replication type Secret Sharing) scheme with respect to the sum, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS stored in a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic; and

a full adder secure computation step that executes addition processing

of the value generated by the addition sharing step and a value not used by the addition sharing step, for each digit, by using secure computation of a full adder, and stores the result in a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic.

[Claim 8]

A method in a computer system for providing bit decomposition secure computing, the method comprising

a full adder secure computation step that performs secure computation of $r_{12} = r_1 + r_2 \bmod 2^n$ and secure computation of $r_{123} = r_{12} + r_3 \bmod 2^n$, for each digit, by using secure computation of a full adder, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS (Replication type Secret Sharing) scheme stored in a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic; and stores the computation result in a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic.

[Claim 9]

A method in a computer system for providing bit combining secure computing, the method comprising

a full adder secure computation step that performs secure computation of $r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n$, where a symbol $\parallel$ is a concatenation operator, ^{n} is a power operator and n is a preset positive integer, and performs secure computation of $r_{123} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n$, for each digit by secure computation of a full adder, wherein with respect to sharing of a value w_i , $r_{\{1, i\}}$, $r_{\{2, i\}}$, $r_{\{3, i\}}$ satisfying $w_i = r_{\{1, i\}} + r_{\{2, i\}} + r_{\{3, i\}} \bmod 2$, for $i=1$ to n , are used as a sequence of n items of share information by the (2, 3) type RSS stored in a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic; and stores the computation results in a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic.

[Claim 10]

The method according to claim 7, comprising

a partial share information extraction step that, using one index out of three values constituting share information by (2, 3) type RSS, as input,

reads the value stored in the share value storage apparatus, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by the (2, 3) type RSS, wherein the full adder secure computation step performs addition processing using secure computation of a full adder on the share information by (2, 3) type RSS generated and distributed by the addition sharing step and the share information by (2, 3) type RSS generated by the partial share information extraction step, and stores the value obtained by combining the share information of the computation result for each bit, in the decomposed share value storage apparatus.

[Claim 11]

The method according to claim 8, comprising a partial share information extraction step that, using one index out of three values constituting share information by the (2, 3) type RSS, as input, reads the value stored in the share value storage apparatus, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by the (2, 3) type RSS, wherein the full adder secure computation step, using 3 sets of share information by the (2, 3) type RSS generated by the partial share information extraction step, including r_i , r_j , r_k , where i , j and k being different to each other and selected from 1 to 3, performs secure computation of $r_{ij} = r_i + r_j \bmod 2^n$, and secure computation of $r_{ij} + r_k \bmod 2^n$, by secure computation of a full adder, from low order bit, and stores a sequence of the computation result, for each bit in the decomposed share value storage apparatus.

[Claim 12]

The method according to claim 9, comprising a partial share information extraction step that, using one index out of three values constituting share information by (2, 3) type RSS, as input, reads the value stored in the share value storage apparatus, and generates share information obtained by setting values to zero except for one of the three values constituting the share information by (2, 3) type RSS.

[Claim 13]

A program causing a computer to execute bit decomposition secure computing processing comprising:
an addition sharing process that sums two values out of r_1 , r_2 and r_3 by modulo 2^n , generates and distributes a share value by the (2, 3) type

RSS (Replication type Secret Sharing) scheme with respect to the sum, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS stored in a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic; and

a full adder secure computation process that executes addition processing of the value generated by the addition sharing process and a value not used by the addition sharing process, for each digit, by using secure computation of a full adder, and stores the result in a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic.

[Claim 14]

A program causing a computer to execute bit decomposition secure computing processing comprising:

a full adder secure computation process that performs secure computation of $r_{12} = r_1 + r_2 \bmod 2^n$ and secure computation of $r_{123} = r_{12} + r_3 \bmod 2^n$, for each digit, by using secure computation of a full adder, wherein with respect to sharing of a value w , r_1 , r_2 , and r_3 satisfying $w = r_1 + r_2 + r_3 \bmod 2^n$, where ^{n} is a power operator and n is a preset positive integer, are used as share information by the (2, 3) type RSS (Replication type Secret Sharing) scheme stored in a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic; and stores the computation result in a decomposed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic.

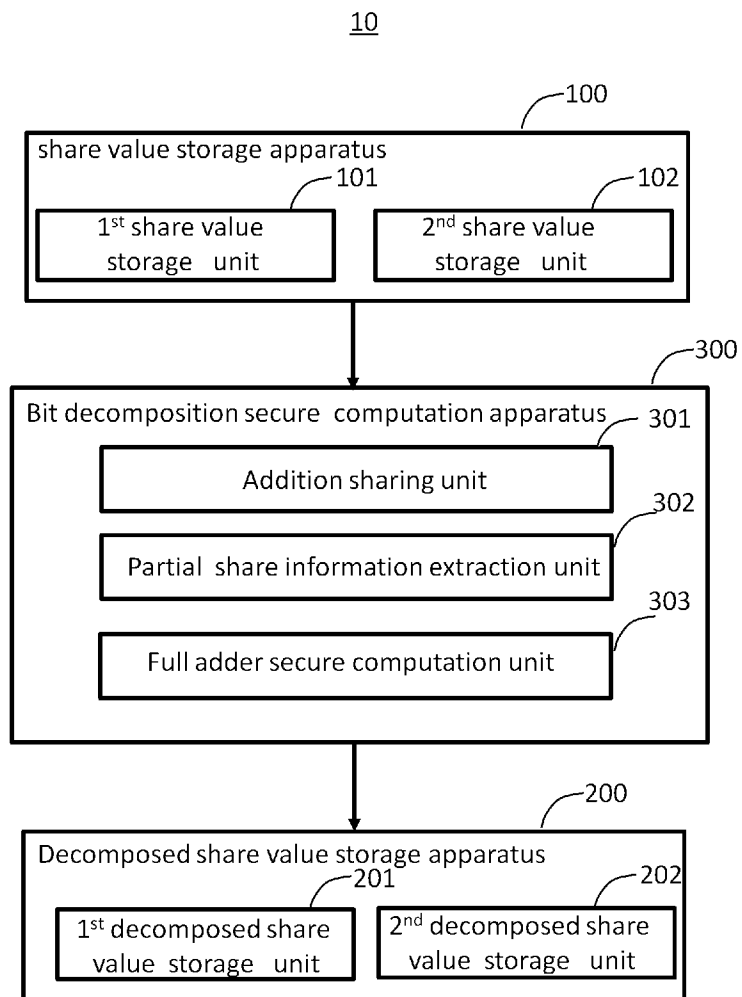
[Claim 15]

A program causing a computer to execute bit combining secure computing processing comprising:

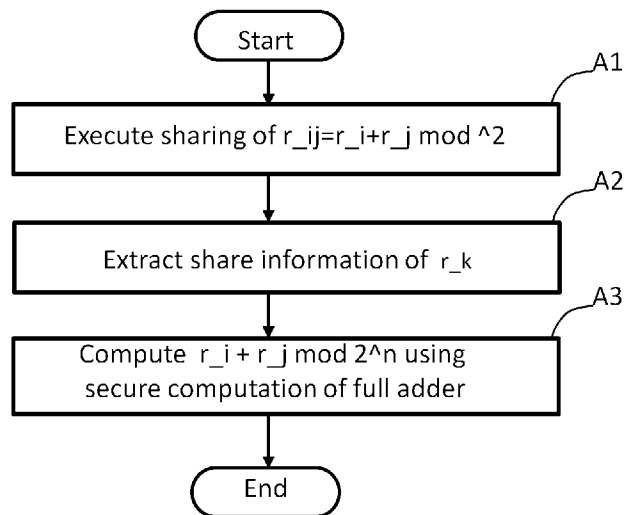
a full adder secure computation process that performs secure computation of $r_{12} = r_{\{1, n\}} \parallel \dots \parallel r_{\{1, 1\}} + r_{\{2, n\}} \parallel \dots \parallel r_{\{2, 1\}} \bmod 2^n$, where a symbol $\parallel$ is a concatenation operator, ^{n} is a power operator and n is a preset positive integer, and performs secure computation of $r_{123} = r_{12} + r_{\{3, n\}} \parallel \dots \parallel r_{\{3, 1\}} \bmod 2^n$, for each digit by secure computation of a full adder, wherein with respect to sharing of a value w_i , $r_{\{1, i\}}$, $r_{\{2, i\}}$, $r_{\{3, i\}}$ satisfying $w_i = r_{\{1, i\}} + r_{\{2, i\}} + r_{\{3, i\}} \bmod 2$, for $i=1$ to n , are used as a sequence of n items of share information by the (2, 3) type RSS stored in a de-

composed share value storage apparatus to store a sequence of share values obtained by applying (2, 3) type RSS using modulo 2 arithmetic; stores the computation results in a share value storage apparatus to store share values obtained by applying (2, 3) type RSS using modulo of power of 2 arithmetic.

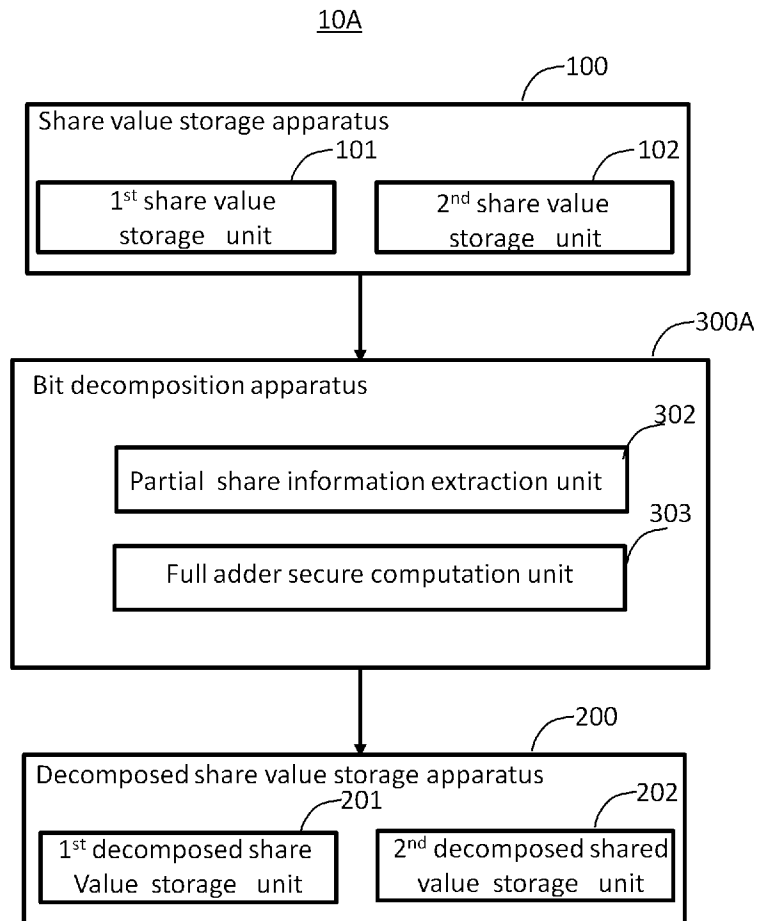
[Fig. 1]



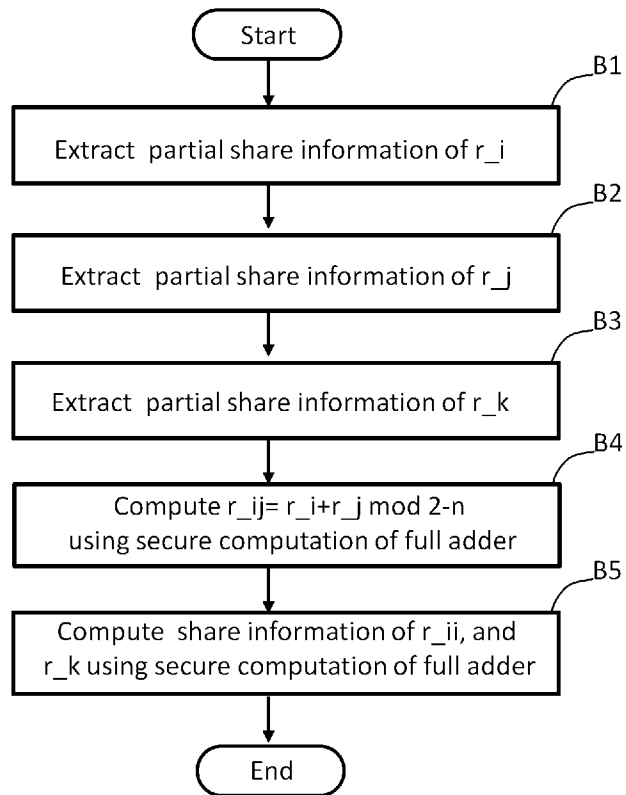
[Fig. 2]



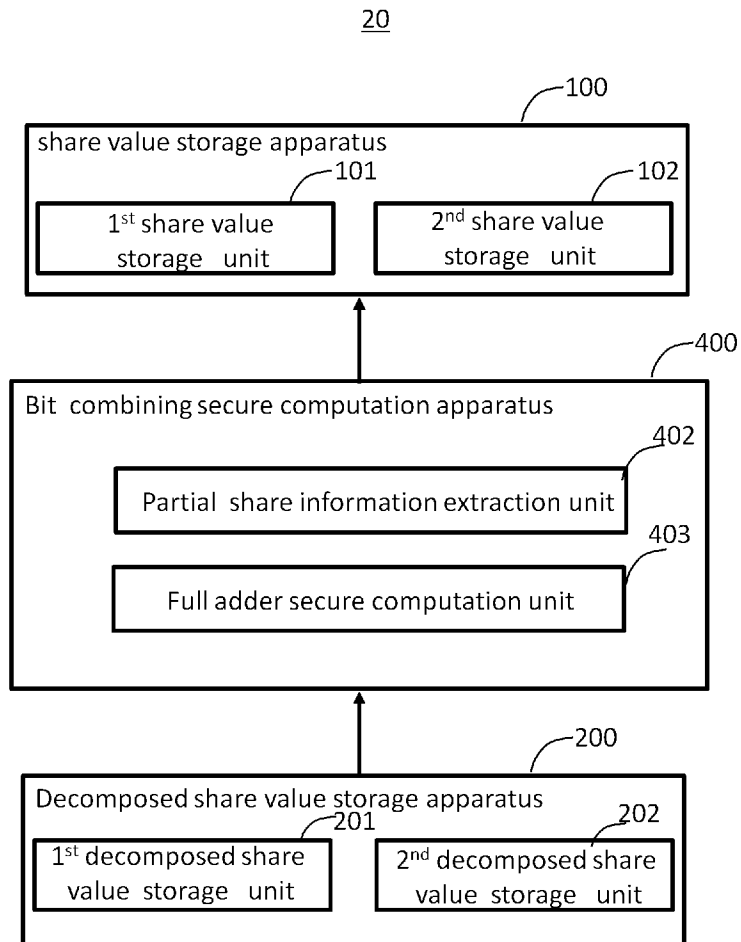
[Fig. 3]



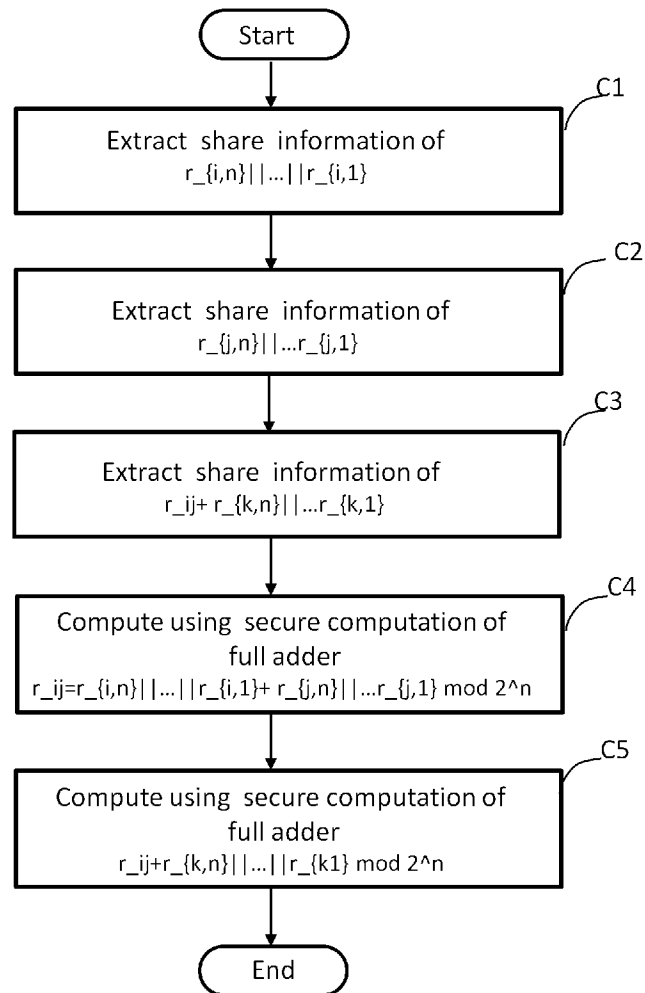
[Fig. 4]



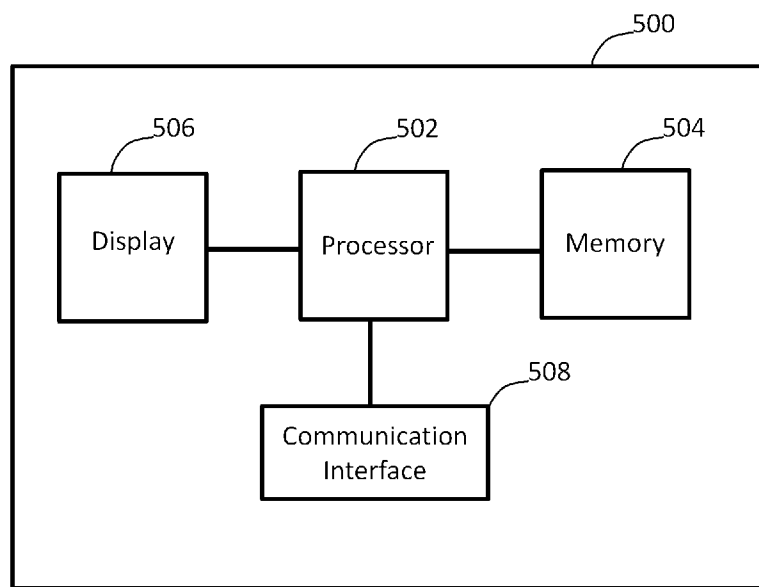
[Fig. 5]



[Fig. 6]



[Fig. 7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/018745

A. CLASSIFICATION OF SUBJECT MATTER		
Int.Cl. G09C1/00 (2006.01) i		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
Int.Cl. G09C1/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2017 Registered utility model specifications of Japan 1996-2017 Published registered utility model applications of Japan 1994-2017		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ARAKI, T, et al., Secure Three-Party Computation with Low Communication and Its Implementation via Bit-Slicing, Abstracts of 2017 Symposium on Cryptography and Information Security (SCIS 2017), 2017.01.24, 2D3-5	1-15
A	WO 2015/053185 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 2015.04.16, Whole document (Family: None)	1-15
☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
09.08.2017		22.08.2017
Name and mailing address of the ISA/JP		Authorized officer
Japan Patent Office		KANEKI, Yoichi
3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		5S 4876
		Telephone No. +81-3-3581-1101 Ext. 3546

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/018745

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE COCK, M., et al., Efficient and Private Scoring of Decision Trees, Support Vector Machines and Logistic Regression Models based on Pre-Computation, IEEE Transactions on Dependable and Secure Computing, Vol. PP, Issue 99, [online], 2017.03.07, [Retrieved on 2017-08-09.] Retrieved from the Internet <URL: http://doi.org/10.1109/TDSC.2017.2679189 >	1-15