(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 669 878 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.09.2015 Bulletin 2015/40

(21) Application number: **12739361.9**

(22) Date of filing: **20.01.2012**

(51) Int Cl.:
G09C 1/00 *(2006.01)* ***H04L 9/08*** *(2006.01)*
G06F 7/544 *(2006.01)*

(86) International application number:
PCT/JP2012/051199

(87) International publication number:
WO 2012/102203 (02.08.2012 Gazette 2012/31)

(54) **CONFIDENTIAL PRODUCT-SUM COMPUTATION METHOD, CONFIDENTIAL PRODUCT-SUM COMPUTATION SYSTEM, COMPUTATION APPARATUS, AND PROGRAM FOR SAME**

ZUVERLÄSSIGES PRODUKTSUMMEN-BERECHNUNGSVERFAHREN, ZUVERLÄSSIGES PRODUKTSUMMEN-BERECHNUNGSSYSTEM, BERECHNUNGSVORRICHTUNG UND PROGRAMM DAFÜR

PROCÉDÉ DE CALCUL DE PRODUIT-SOMME CONFIDENTIEL, SYSTÈME DE CALCUL DE PRODUIT-SOMME CONFIDENTIEL, APPAREIL DE CALCUL, ET PROGRAMME POUR CE PROCÉDÉ

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **24.01.2011 JP 2011012126**
14.03.2011 JP 2011054965
17.05.2011 JP 2011110635

(43) Date of publication of application:
04.12.2013 Bulletin 2013/49

(73) Proprietor: **Nippon Telegraph And Telephone Corporation**
Tokyo 100-8116 (JP)

(72) Inventors:
- **IKARASHI, Dai**
  Musashino-shi
  Tokyo 180-8585 (JP)
- **HAMADA, Koki**
  Musashino-shi
  Tokyo 180-8585 (JP)
- **CHIDA, Koji**
  Musashino-shi
  Tokyo 180-8585 (JP)

(74) Representative: **MERH-IP**
Matias Erny Reichl Hoffmann
Paul-Heyse-Strasse 29
80336 München (DE)

(56) References cited:
- **Ran Canetti ET AL: "Cryptography & Game Theory Lecture 4 -General secure two party and multi party computation", , 11 November 2009 (2009-11-11), XP055136476, Retrieved from the Internet: URL:http://www.cs.tau.ac.il/~canetti/f09-m aterials/f09-scribe4.pdf [retrieved on 2014-08-26]**
- **DAN BOGDANOV ET AL: "Sharemind: a framework for fast privacy-preserving computations", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20080703: 190107, 27 June 2008 (2008-06-27), pages 1-23, XP061002901, [retrieved on 2008-06-27]**
- **KOJI CHIDA ET AL.: 'Efficient 3-Party Secure Function Evaluation and Its Application' IPSJ SIG NOTES DVD-ROM vol. 2010, no. 1, 15 April 2010, pages 1 - 7, XP008170896**
- **KOJI CHIDA ET AL.: 'Keiryo Kensho Kano 3-Party Hitoku Kansu Keisan no Saiko' COMPUTER SECURITY SYMPOSIUM 2010 RONBUNSHU vol. 2, no. 9, 12 October 2010, pages 555 - 560, XP008171075**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- KOKI HAMADA ET AL.: '3-Party Hitoku Kansu Keisanjo no Random Chikan Protocol' COMPUTER SECURITY SYMPOSIUM 2010 RONBUNSHU vol. 2, no. 9, 12 October 2010, pages 561 - 566, XP008170364
- YEHUDA LINDELL: 'General Composition and Universal Composability in Secure Multiparty Computation' JOURNAL OF CRYPTOLOGY vol. 22, no. 3, July 2009, pages 395 - 428, XP019699797
- ROSARIO GENNARO ET AL.: 'On 2-Round Secure Multiparty Computation' LNCS, ADVANCES IN CRYPTOLOGY vol. 2442, August 2002, pages 178 - 193, XP055123962

Description

[TECHNICAL FIELD]

[0001] The present invention relates to a secure sum-of-product computation method, a secure sum-of-product computation system, a computation apparatus and programs therefor for performing data processings, particularly, a multiplication computation and a sum-of-product computation, while concealing data by secret sharing.

[BACKGROUND ART]

[0002] In the field of management and operation of so-called sensitive information, such as customer information and management information, the information to be managed is increasing in variety, and the information processing technology such as cloud computing is changing, so that measures to ensure security and privacy are becoming more important. Recently, the secret sharing art has become popular to prevent leakage of information by distributing the information among plural sites. Besides, a secure functional computation (a multi-party protocol) for deriving a specified computation result without reconstructing the distributed information is also being developed for commercialization. The secret sharing art is effective as a measure to ensure security when storing information but has a risk of leakage of information when using the information, because the information generally needs to be reconstructed for use. In view of the presence of such a risk of leakage of information, the secure functional computation can uses distributed information as operands for computation instead of the original input values and does not need to reconstruct the original input values at all in the computation process. Therefore, the secure functional computation can be said to be an advanced security art that maintains the functionality of the secret sharing art even when the information is used.

[0003] A prior art for performing a multiplication while concealing information is a multiplication protocol described in Non-Patent literature 1. A prior art for performing a sum-of-product computation while concealing information is a combination of a multiplication protocol and an addition protocol. These protocols are 3-party secure functional computation protocols that derive a result of an arithmetic/logical operation by cooperative computation by three parties (three computing entities) without reconstructing a shared input value. In the 3-party secure functional computation protocol, data is treated as a natural number smaller than a predetermined prime number p. To conceal data, which will be denoted as "a", the data a is divided into three fragments in such a manner that the fragments satisfy the following condition.

$$a=a_0+a_1+a_2 \bmod p$$

In practice, random numbers a_0 and a_1 are generated, and a relation holds: $a_2=a-a_0-a_1$. Then, a random number sequence (a_0, a_1) is transmitted to a party X of the three parties, a random number sequence (a_1, a_2) is transmitted to a party Y of the three parties, and a random number sequence (a_2, a_0) is transmitted to a party Z of the three parties. Since a_1 and a_2 are random numbers, any of the parties X, Y and Z does not have information about the data a. However, any two of the parties can cooperate to reconstruct the data a.

[0004] Since the concealment is an additive distribution, the shared value can be equally reconstructed before or after addition of its fragments because of the interchangeability. That is, the addition and the constant multiplication of the distributed fragments can be achieved without communications. If a multiplication can additionally be performed, a logical circuit can be formed, and any computation can be performed. The multiplication needs communications and random number generation and therefore is a bottleneck of the 3-party secure functional computation.

[PRIOR ART LITERATURE]

[NON-PATENT LITERATURE]

[0005] Non-patent literature 1: Koji Chida, Koki Hamada, Dai Ikarashi, Katsumi Takahashi, "A Three-Party Secure Function Evaluation with Lightweight Verifiability Revisited", CSS2010, 2010.

[SUMMARY OF THE INVENTION]

[PROBLEMS TO BE SOLVED BY THE INVENTION]

[0006] In the 3-party secure functional computation, the multiplication and the sum-of-product computation requires communications and random number generation and therefore are a bottleneck in the computation processing.

[0007] More specifically, the conventional multiplication protocol requires two rounds of communications. In addition, the computation amounts and the communication amounts of the three parties are not symmetrical to each other, so that a different program needs to be implemented in each party. As a result, the implementation cost increases. In addition, the part where the computation amount and the communication amount are at the maximum constitutes a bottleneck. In addition, the sum-of-product computation generally requires a large amount of communications.

[0008] An object of the present invention is to provide a secure sum-of-product computation method, a secure sum-of-product computation system, a computation apparatus and a program therefor that can quickly perform a multiplication and a sum-of-product computation and can be readily implemented.

[MEANS TO SOLVE THE PROBLEMS]

[0009] A secure sum-of-product computation method according to the present invention is a secure sum-of-product computation method used for performing a sum-of-product computation of data strings $A_0 = (a0_0, ..., a0_{na0-1})$, $A_1 = (a1_0, ..., a1_{na1-1})$ and $A_2 = (a2_0, ..., a2_{na2-1})$ and data strings $B_0 = (b0_0, ..., b0_{nb0-1})$, $B_1 = (b1_0, ..., b1_{nb1-1})$ and $B_2 = (b2_0, ..., b2_{nb2-1})$ by cooperative computation by three computation apparatuses, which are a party X, a party Y and a party Z, the sum-of-product computation being expressed as

[FORMULA 1]

$$\sum_{i0,j0}(e00_{i0,j0}\cdot a0_{i0}\cdot b0_{j0})+\sum_{i0,j1}(e01_{i0,j0}\cdot a0_{i0}\cdot b1_{j1})+\sum_{i1,j0}(e10_{i1,j0}\cdot a1_{i1}\cdot b0_{j0})$$
$$+\sum_{i1,j1}(e11_{i1,j1}\cdot a1_{i1}\cdot b1_{j1})+\sum_{i1,j2}(e12_{i1,j2}\cdot a1_{i1}\cdot b2_{j2})+\sum_{i2,j1}(e21_{i2,j1}\cdot a2_{i2}\cdot b1_{j1})$$
$$+\sum_{i2,j2}(e22_{i2,j2}\cdot a2_{i2}\cdot b2_{j2})+\sum_{i2,j0}(e20_{i2,j0}\cdot a2_{i2}\cdot b0_{j0})+\sum_{i0,j2}(e02_{i0,j2}\cdot a0_{i0}\cdot b2_{j2})$$

$$(i0 = 0, ..., na0\text{-}1,\ i1 = 0, ..., na1\text{-}1,\ i2 = 0, ..., na2\text{-}1,\ j0 = 0, ..., nb0\text{-}1,\ j1 =$$

0, ..., nb1-1, and j 2 = 0, ..., nb2-1, na0, na1, na2, nb0, nb1 and nb2 represent natural numbers), and comprises a party-X random number generation step, a party-X first computation step, a party-X second computation step, a party-Y random number generation step, a party-Y first computation step, a party-Y second computation step, a party-Z random number generation step, a party-Z first computation step and a party-Z second computation step.

[0010] In the processing, the data strings A_0, A_1, B_0 and B_1 are input to the party X, the data strings A_1, A_2, B_1 and B_2 are input to the party Y, and the data strings A_2, A_0, B_2 and B_0 are input to the party Z.

[0011] In the party-X random number generation step, the party X generates a number r_X and transmits the number to the party Y.

[0012] In the party-X first computation step, the party X computes a value c_X according to

[FORMULA 2]

$$c_X = \sum_{i0,j1}(e01_{i0,j1}\cdot a0_{i0}\cdot b1_{j1})+\sum_{i1,j0}(e10_{i1,j0}\cdot a1_{i1}\cdot b0_{j0})+r_X$$

($e01_{i0,j1}$ and $e10_{i1,j0}$ represent any numbers) and transmits the value to the party Z.

[0013] In the party-X second computation step, the party X receives a number r_Z from the party Z and a value c_Y from the party Y, computes values c_0 and c_1 according to

[FORMULA 3]

$$c_0 = \sum_{i0,j0} (e00_{i0,j0} \cdot a0_{i0} \cdot b0_{j0}) + c_X - r_Z$$

$$c_1 = \sum_{i1,j1} (e11_{i1,j1} \cdot a1_{i1} \cdot b1_{j1}) + c_Y - r_X$$

($e00_{i0,j0}$ and $e11_{i1,j1}$ represent any numbers) and outputs the values.

[0014] In the party-Y random number generation step, the party Y generates a number r_Y and transmits the number to the party Z.

[0015] In the party-Y first computation step, the party Y computes the value c_Y according to

[FORMULA 4]

$$c_Y = \sum_{i1,j2} (e12_{i1,j2} \cdot a1_{i1} \cdot b2_{j2}) + \sum_{i2,j1} (e21_{i2,j1} \cdot a2_{i2} \cdot b1_{j1}) + r_Y$$

($e12_{i1,j2}$ and $e21_{i2,j1}$ represent any numbers) and transmits the value to the party X.

[0016] In the party-Y second computation step, the party Y receives the number r_X from the party X and a value c_Z from the party Z, computes values c_1 and c_2 according to

[FORMULA 5]

$$c_1 = \sum_{i1,j1} (e11_{i1,j1} \cdot a1_{i1} \cdot b1_{j1}) + c_Y - r_X$$

$$c_2 = \sum_{i2,j2} (e22_{i2,j2} \cdot a2_{i2} \cdot b2_{j2}) + c_Z - r_Y$$

($e22_{i2,j2}$ represents any number) and outputs the values.

[0017] In the party-Z random number generation step, the party Z generates the number r_Z and transmits the number to the party X.

[0018] In the party-Z first computation step, the party Z computes the value c_Z according to

[FORMULA 6]

$$c_Z = \sum_{i2,j0} (e20_{i2,j0} \cdot a2_{i2} \cdot b0_{j0}) + \sum_{i0,j2} (e02_{i0,j2} \cdot a0_{i0} \cdot b2_{j2}) + r_Z$$

($e20_{i2,j0}$ and $e02_{i0,j2}$ represent any numbers) and transmits the value to the party Y.

[0019] In the party-Z second computation step, the party Z receives the number r_Y from the party Y and the value c_X from the party X, computes the values c_0 and c_2 according to

[FORMULA 7]

$$c_0 = \sum_{i0,j0} (e00_{i0,j0} \cdot a0_{i0} \cdot b0_{j0}) + c_X - r_Z$$

$$c_2 = \sum_{i2,j2} (e22_{i2,j2} \cdot a2_{i2} \cdot b2_{j2}) + c_Z - r_Y$$

and outputs the values.

[EFFECTS OF THE INVENTION]

[0020] The secure sum-of-product computation methods, the secure sum-of-product computation systems, the computation apparatuses and the programs therefor according to the present invention can quickly perform a multiplication and a sum-of-product computation, and the programs can be readily implemented because the processings performed by the parties are symmetrical to each other.

[BRIEF DESCRIPTION OF THE DRAWINGS]

[0021]

Fig. 1 is a diagram showing an example of a configuration of a secure sum-of-product computation system 100;
Fig. 2 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation system 100;
Fig. 3 is a diagram showing an example of an internal configuration of each party of the secure sum-of-product computation systems 100 and 200;
Fig. 4 is a diagram showing an example of a configuration of a secure sum-of-product computation system 200;
Fig. 5 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation system 200;
Fig. 6 is a diagram showing an example of a configuration of a secure sum-of-product computation system 300;
Fig. 7 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation system 300;
Fig. 8 is a diagram showing an example of an internal configuration of each party of the secure sum-of-product computation systems 300, 400 and 500;
Fig. 9 is a diagram showing an example of a configuration of secure sum-of-product computation systems 400 and 500;
Fig. 10 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation systems 400 and 500;
Fig. 11 is a diagram showing an example of a configuration of a secure sum-of-product computation system 600;
Fig. 12 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation system 600;
Fig. 13 is a diagram showing an example of an internal configuration of each party of the secure sum-of-product computation systems 600, 700 and 800;
Fig. 14 is a diagram showing an example of a configuration of secure sum-of-product computation systems 700 and 800;
Fig. 15 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation systems 700 and 800;
Fig. 16 is a diagram showing an example of a configuration of secure sum-of-product computation system 900, 910 and 920; and
Fig. 17 is a diagram showing an example of a flow of a processing performed by the secure sum-of-product computation system 900, 910 and 920.

[DETAILED DESCRIPTION OF THE EMBODIMENTS]

[0022] In the following, embodiments of the present invention will be described in detail.

[FIRST EMBODIMENT]

[0023] Fig. 1 shows an example of a configuration of a secure sum-of-product computation system 100, and Fig. 2 shows an example of a flow of a processing performed by the secure sum-of-product computation system 100. The secure sum-of-product computation system 100 comprises a party X, a party Y and a party Z, which are computation apparatuses that perform symmetric computation processings.

[0024] A secure sum-of-product computation according to the present invention is achieved by the three computation apparatuses, the parties X, Y and Z, cooperating to perform sum-of-product computations of data strings $A_0 = (a0_0, ..., a0_{na0-1})$, $A_1 = (a1_0, ..., a1_{na1-1})$ and $A_2 = (a2_0, ..., a2_{na2-1})$ and data strings $B_0 = (b0_0, ..., b0_{nb0-1})$, $B_1 = (b1_0, ..., b1_{nb1-1})$ and $B_2 = (b2_0, ..., b2_{nb2-1})$. Note that na0, na1, na2, nb0, nb1 and nb2 represent natural numbers.

[0025] As shown in Fig. 3, each party has random number generation means 101, first computation means 102 and second computation means 103. In Fig. 3, a subject party is denoted as P, and other parties are denoted as P_- and P_+. Specifically, when the subject party is the party X, another party P_- is the party Z, and the remaining party P_+ is the party Y. When the subject party is the party Y, another party P_- is the party X, and the remaining party P_+ is the party Z. When the subject party is the party Z, another party P_- is the party Y, and the remaining party P_+ is the party X. In this specification, the relationship between the subject party P and the other parties P_- and P_+ that does not change depending on which of the parties serves as the subject party P is expressed as "symmetric (symmetrical)". And a processing performed by the parties in such a relationship is referred to as a "symmetric processing" or expressed as "symmetric (symmetrical)".

[0026] In the following, details of a cooperative computation processing performed by each party will be specifically described. First, data strings A_0, A_1, B_0 and B_1 are input to the party X, data strings A_1, A_2, B_1 and B_2 are input to the party Y, and data strings A_2, A_0, B_2 and B_0 are input to the party Z (S1).

[0027] Then, the party X performs the following processing. The random number generation means 101 first generates a random number r_X and transmits the random number to the party Y (S2-1). Then, the first computation means 102 computes a value c_X according to

[FORMULA 8]

$$c_X = \sum_{i0,j1} (e01_{i0,j1} \cdot a0_{i0} \cdot b1_{j1}) + \sum_{i1,j0} (e10_{i1,j0} \cdot a1_{i1} \cdot b0_{j0}) + r_X$$

and transmits the value c_X to the party Z (S2-2). Note that i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, j1 = 0, ..., nb1-1, and $e01_{i0,j1}$ and $e10_{i1,j0}$ each represent any number. The second computation means 103 receives a random number r_z from the party Z and a value c_Y from the party Y and computes values c_0 and c_1 according to

[FORMULA 9]

$$c_0 = \sum_{i0,j0} (e00_{i0,j0} \cdot a0_{i0} \cdot b0_{j0}) + c_X - r_Z$$

$$c_1 = \sum_{i1,j1} (e11_{i1,j1} \cdot a1_{i1} \cdot b1_{j1}) + c_Y - r_X$$

and outputs the values c_0 and c_1 (S3). Note that $e00_{i0,j0}$ and $e11_{i1,j1}$ each represent any number.

[0028] The party Y performs the following processing. The random number generation means 101 first generates a random number r_Y and transmits the random number to the party Z (S4-1). Then, the first computation means 102 computes the value c_Y according to

[FORMULA 10]

$$c_Y = \sum_{i1,j2} (e12_{i1,j2} \cdot a1_{i1} \cdot b2_{j2}) + \sum_{i2,j1} (e21_{i2,j1} \cdot a2_{i2} \cdot b1_{j1}) + r_Y$$

and transmits the value c_Y to the party X (S4-2). Note that i2 = 0, ..., na2-1, j2 = 0, ..., nb2-1, and $e12_{i1,j2}$ and $e21_{i2,j1}$ each represent any number. The second computation means 103 receives the random number r_X from the party X and a value c_Z from the party Z and computes values c_1 and c_2 according to

[FORMULA 11]

$$c_1 = \sum_{i1,j1} (e11_{i1,j1} \cdot a1_{i1} \cdot b1_{j1}) + c_Y - r_X$$

$$c_2 = \sum_{i2,j2} (e22_{i2,j2} \cdot a2_{i2} \cdot b2_{j2}) + c_Z - r_Y$$

and outputs the values c_1 and c_2 (S5). Note that $e22_{i2,j2}$ represents any number.

[0029] The party Z performs the following processing. The random number generation means 101 first generates the random number r_Z and transmits the random number to the party X (S6-1). Then, the first computation means 102 computes the value c_Z according to

[FORMULA 12]

$$c_Z = \sum_{i2,j0} (e20_{i2,j0} \cdot a2_{i2} \cdot b0_{j0}) + \sum_{i0,j2} (e02_{i0,j2} \cdot a0_{i0} \cdot b2_{j2}) + r_Z$$

and transmits the value c_Z to the party Y (S6-2). Note that $e20_{i2,j0}$ and $e02_{i0,j2}$ represent any numbers. The second computation means 103 receives the random number r_Y from the party Y and the value c_X from the party X and computes values c_0 and c_2 according to

[FORMULA 13]

$$c_0 = \sum_{i0,j0} (e00_{i0,j0} \cdot a0_{i0} \cdot b0_{j0}) + c_X - r_Z$$

$$c_2 = \sum_{i2,j2} (e22_{i2,j2} \cdot a2_{i2} \cdot b2_{j2}) + c_Z - r_Y$$

and outputs the values c_0 and c_2 (S7). Note that the series of steps S2-1 and S2-2, the series of steps S4-1 and S4-2 and the series of steps S6-1 and S6-2 can be performed in parallel, and the steps S3, S5 and S7 can also be performed in parallel.

[0030] Then, the total sum of the values c_0, c_1, and c_2 output from the parties X, Y and Z can be computed to obtain a sum-of-product computation result as expressed by the following formula.

[FORMULA 14]

$$c_o + c_1 + c_2 =$$
$$\sum_{i0,j0}(e00_{i0,j0} \cdot a0_{i0} \cdot b0_{j0}) + \sum_{i0,j1}(e01_{i0,j0} \cdot a0_{i0} \cdot b1_{j1}) + \sum_{i1,j0}(e10_{i1,j0} \cdot a1_{i1} \cdot b0_{j0})$$
$$+ \sum_{i1,j1}(e11_{i1,j1} \cdot a1_{i1} \cdot b1_{j1}) + \sum_{i1,j2}(e12_{i1,j2} \cdot a1_{i1} \cdot b2_{j2}) + \sum_{i2,j1}(e21_{i2,j1} \cdot a2_{i2} \cdot b1_{j1})$$
$$+ \sum_{i2,j2}(e22_{i2,j2} \cdot a2_{i2} \cdot b2_{j2}) + \sum_{i2,j0}(e20_{i2,j0} \cdot a2_{i2} \cdot b0_{j0}) + \sum_{i0,j2}(e02_{i0,j2} \cdot a0_{i0} \cdot b2_{j2})$$

In the processing described above, hash values or other values can be substituted for the random numbers.

[0031] The effect of the method according to the present invention will be compared with that of the method described in Non-Patent literature 1. Most of the computations in Non-Patent literature 1 are involved with random number generation and encryption and decryption for communications in the case where no physical secure channels are available. The amount of computations for encryption and decryption agrees with the amount of communications, so that the efficiency can be evaluated by observing the number of random numbers generated and the amount of communications.

[0032] In the case where an addition is performed after repeatedly performing multiplications as described in Non-Patent literature 1, the number of random numbers generated and the amount of communications are proportional to the number of elements of the input data strings. In the method according to the present invention, the parties X, Y and Z each generate only one random number and transmit only two pieces of data to the other parties. In addition, the processings performed by the parties X, Y and Z are symmetrical to each other, so that common programs can be implemented in all the parties, and the implementation cost can be reduced.

[SECOND EMBODIMENT]

[0033] A second embodiment is a specific example of the first embodiment, in which na0 = na1 = na2 = nb0 = nb1 = nb2 = n (n represents an integer equal to or greater than 1), and e00 = e01 = e10 = e11 = e12 = e21 = e22 = e20 = e02 = 1. Fig. 4 shows an example of a configuration of a secure sum-of-product computation system 200 according to this embodiment, and Fig. 5 shows an example of a flow of a processing performed by the secure sum-of-product computation system 200. The secure sum-of-product computation system 200 comprises a party X, a party Y, a party Z, a data string decomposition and supply part 210 and an output part 220. Each party has random number generation means 101, first computation means 102 and second computation means 103 as in the first embodiment as shown in Fig. 3.

[0034] The secure sum-of-product computation system 200 performs a sum-of-product computation

[FORMULA 15]

$$\sum_{i=0}^{n-1} a_i \cdot b_i$$

for two data strings $A = (a_0, ..., a_{n-1})$ and $B = (b_0, ..., b_{n-1})$ comprising elements a_i and b_i (i = 0, ..., n-1), which are natural numbers smaller than a prime number p while concealing the contents of the data strings through cooperative computation by the three computation apparatuses, the parties X, Y and Z (the sum-of-product computation is a multiplication of a and b in the case where n = 1).

[0035] Specifically, the data string decomposition and supply part 210 decomposes the input data strings A and B in such a manner that each element a_i and b_i satisfy conditional formulas $a_i = a0_i + a1_i + a2_i \bmod p$ and $b_i = b0_i + b1_i + b2_i \bmod p$ ($a0_i$, $a1_i$, $b0_i$ and $b1_i$ represent random numbers, and p represents a prime number) and supplies data strings $A_0 = (a0_0, ..., a0_{n-1})$, $A_1 = (a1_0, ..., a1_{n-1})$, $B_0 = (b0_0, ..., b0_{n-1})$ and $B_1 = (b1_0, ..., b1_{n-1})$ to the party X, the data strings A_1, $A_2 = (a2_0, ..., a2_{n-1})$, B_1 and $B_2 = (b2_0, ..., b2_{n-1})$ to the party Y, and data strings A_2, A_0, B_2 and B_0 to the party Z (S11).

[0036] Then, the party X performs the following processing. The random number generation means 101 first generates a random number r_X and transmits the random number to the party Y (S12-1). Then, the first computation means 102 computes a value c_X according to

[FORMULA 16]

$$c_X = \sum_i (a0_i \cdot b1_i + a1_i \cdot b0_i) + r_X$$

and transmits the value c_X to the party Z (S12-2). Then, the second computation means 103 receives a random number r_Z from the party Z and a value c_Y from the party Y and computes values c_0 and c_1 according to

[FORMULA 17]

$$c_0 = \sum_i (a0_i \cdot b0_i) + c_X - r_Z$$

$$c_1 = \sum_i (a1_i \cdot b1_i) + c_Y - r_X$$

and outputs the values c_0 and c_1 (S13).

[0037] The party Y performs the following processing. The random number generation means 101 first generates a random number r_Y and transmits the random number to the party Z (S14-1). Then, the first computation means 102 computes the value c_Y according to

[FORMULA 18]

$$c_Y = \sum_i (a1_i \cdot b2_i + a2_i \cdot b1_i) + r_Y$$

and transmits the value c_Y to the party X (S 14-2). Then, the second computation means 103 receives the random number r_X from the party X and a value c_Z from the party Z and computes values c_1 and c_2 according to

[FORMULA 19]

$$c_1 = \sum_i (a1_i \cdot b1_i) + c_Y - r_X$$

$$c_2 = \sum_i (a2_i \cdot b2_i) + c_Z - r_Y$$

and outputs the values c_1 and c_2 (S15).

[0038] The party Z performs the following processing. The random number generation means 101 first generates the random number r_Z and transmits the random number to the party X (S16-1). Then, the first computation means 102 computes the value c_Z according to

[FORMULA 20]

$$c_Z = \sum_i (a2_i \cdot b0_i + a0_i \cdot b2_i) + r_Z$$

and transmits the value c_Z to the party Y (S16-2). Then, the second computation means 103 receives the random number r_Y from the party Y and the value c_X from the party X and computes values c_0 and c_2 according to

[FORMULA 21]

$$c_0 = \sum_i (a0_i \cdot b0_i) + c_X - r_Z$$

$$c_2 = \sum_i (a2_i \cdot b2_i) + c_Z - r_Y$$

and outputs the values c_0 and c_2 (S17). Note that the series of steps S12-1 and S12-2, the series of steps S14-1 and S14-2 and the series of steps S16-1 and S16-2 can be performed in parallel, and the steps S 13, S15 and S17 can also be performed in parallel.

[0039] Then, the output part 220 computes the total sum (c_0+c_1+c_2) of the values c_0, c_1 and c_2 output from the parties X, Y and Z and outputs the total sum.

[0040] The following relation holds.

[FORMULA 22]

$$\begin{aligned} c_0 + c_1 + c_2 &= \sum_i (a0_i \cdot b0_i + a0_i \cdot b1_i + a1_i \cdot b0_i) \\ &\quad + \sum_i (a1_i \cdot b1_i + a1_i \cdot b2_i + a2_i \cdot b1_i) \\ &\quad + \sum_i (a2_i \cdot b2_i + a2_i \cdot b0_i + a0_i \cdot b2_i) \\ &= \sum_i (a0_i + a1_i + a2_i)(b0_i + b1_i + b2_i) \\ &= \sum_i a_i \cdot b_i \end{aligned}$$

From the relation above, it can be seen that the sum-of-product computation (a multiplication of a and b in the case where i = 1) has been correctly done.

[0041] In the processing described above, hash values or other values can be substituted for the random numbers. The data string decomposition and supply part 210 and the output part 220 can be provided in an apparatus other than the parties or provided in any one or more of the apparatuses serving as the parties.

[0042] The effect of the method according to the present invention will be compared with that of the method described in Non-Patent literature 1. Concerning the multiplications, in the method described in Non-Patent literature 1, two rounds of communications are required (the term "round" means the number of times that each of the parties X, Y and Z performing parallel processing needs to wait for the other parties to complete their respective processings), and the party X generates one random number and transmits four pieces of data, and the parties Y and Z generate no random number and transmit one piece of data. On the other hand, according to the present invention, one round of communications is required, and all the parties X, Y and Z generate one random number and transmit two pieces of data. That

is, the number of rounds is reduced to a half. In addition, the number of random numbers generated and the number of pieces of data transmitted are the same as those in the method described in Non-Patent literature 1, it can be said that the bottleneck is reduced because the processings performed by the parties X, Y and Z are symmetrical to each other.

[0043] Concerning the sum-of-product computation, in the case of the method of performing an addition after repeatedly performing multiplications described in Non-Patent literature 1, the number of random numbers generated and the amount of communications are proportional to the number of elements of the input data strings. However, in the case of the method according to the present invention, the parties X, Y and Z each generate only one random number and transmit only two pieces of data to the other parties. Since the processings for any computations performed by the parties X, Y and Z are symmetrical to each other, the implementation cost can be reduced.

[THIRD EMBODIMENT]

[0044] According to a third embodiment, a misuse detection function is added to the configurations for performing a sum-of-product computation according to the first and second embodiments. Fig. 6 shows an example of a configuration of a secure sum-of-product computation system 300, and Fig. 7 shows an example of a flow of a processing performed by the secure sum-of-product computation system 300. The secure sum-of-product computation system 300 comprises a party X, a party Y and a party Z, which are computation apparatuses that perform symmetric computation processings.

[0045] A secure sum-of-product computation according to the present invention is achieved by the three computation apparatuses, the parties X, Y and Z, cooperating to perform a total of m sets of sum-of-product computations of data strings $Aq\_0 = (a0_{q\_0}, ..., a0_{q\_na0-1})$, $A_{q-1} = (a1_{q\_0}, ..., a1_{q\text{-}na1-1})$ and $A_{q\_2} = (a2_{q\_0}, ..., a2_{q\_na2-1})$ and $B_{q\_0} = (b0_{q\_0}, ..., b0_{q-nb0-1})$, $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ and $B_{q\_2} = (b2_{q\_0}, ..., b2_{q\_nb2-1})$ (q = 0, ..., m-1, and m represents an integer equal to or greater than 1) (the sum-of-product computations are performed in parallel in the case where m is equal to or greater than 2). Note that na0, na1, na2, nb0, nb1 and nb2 represent natural numbers.

[0046] As shown in Fig. 8, each party has first random number generation means 301, first computation means 302, second computation means 303, second random number generation means 304, third computation means 305, fourth computation means 306 and misuse detection means 307. In Fig. 8, provided that any of the apparatuses described above is a party P, when the party P is the party X, a party P_- is the party Z, and a party P_+ is the party Y, and subscripts 0p, 1p and 2p correspond to numerals 0, 1 and 2, respectively. When the party P is the party Y, the party P_- is the party X, and the party P_+ is the party Z, and the subscripts 0p, 1p and 2p correspond to numerals 1, 2 and 0, respectively. When the party P is the party Z, the party P_- is the party Y, and the party P_+ is the party X, and the subscripts 0p, 1p and 2p correspond to numerals 2, 0 and 1, respectively.

[0047] In the following, details of a cooperative computation processing performed by each party will be specifically described. Steps S21 to S27 correspond to the sum-of-product computation processing according to the first embodiment, and steps S28 to S39 are involved in a misuse detection processing. It is assumed that the parties X and Y previously share a random number s_{q_Z}, the parties Y and Z previously share a random number s_{q_X}, and the parties Z and X previously share a random number s_{q_Y}. First, data strings A_{q_0}, A_{q-1}, B_{q-0} and B_{q-1} are input to the party X, data strings A_{q_1}, A_{q_2}, B_{q_1} and B_{q_2} are input to the party Y, and data strings A_{q_2}, A_{q_0}, B_{q_2} and B_{q_0} are input to the party Z (S21).

[0048] Then, the party X performs the following processing. The first random number generation means 301 first generates a random number r_{q_X} and transmits the random number to the party Y (S22-1). Then, the first computation means 302 computes a value c_{q_X} according to

[FORMULA 23]

$$c_{q\_X} = \sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) + r_{q\_X}$$

and transmits the value c_{q_X} to the party Z (S22-2). Note that i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, and j1 = 0, ..., nb1-1, and $e01_{q\_i0,q\_j1}$ and $e10_{q\_i1,q\_j0}$ each represent any number. The second computation means 303 receives a random number r_{q_Z} from the party Z and a value c_{q_Y} from the party Y and computes values c_{q_0} and c_{q_1} according to

[FORMULA 24]

$$c_{q\_0} = \sum_{q\_i0,q\_j0} (e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z}$$

$$c_{q\_1} = \sum_{q\_i1,q\_j1} (e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X}$$

and outputs the values c_{q_0} and c_{q_0} (S23). Note that $e00_{q\_i0,q\_j0}$ and $e11_{q\_i1}$, $q_{\_j1}$ represent any numbers.

[0049] The party Y performs the following processing. The random number generation means 301 first generates a random number r_{q_Y} and transmits the random number to the party Z (S24-1). Then, the first computation means 302 computes the value c_{q_Y} according to

[FORMULA 25]

$$c_{q\_Y} = \sum_{q\_i1,q\_j2} (e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j1} (e21_{q\_i2,q\_j1} \cdot a2_{q\_i2} \cdot b1_{q\_j1}) + r_{q\_Y}$$

and transmits the value c_{q_Y} to the party X (S24-2). Note that i2 = 0, ..., na2-1 and j2 = 0, ..., nb2-1, and $e12_{q\_i1,q\_j2}$ and $e21_{q\_i2,q\_j1}$ represent any numbers. The second computation means 303 receives the random number r_{q_X} from the party X and a value c_{q_Z} from the party Z and computes values c_{q_1} and c_{q_2} according to the following formula (S25).

[FORMULA 26]

$$c_{q\_1} = \sum_{q\_i1,q\_j1} (e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X}$$

$$c_{q\_2} = \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y}$$

Note that $e22_{q\_i2,q\_j2}$ represents any number.

[0050] The party Z performs the following processing. The random number generation means 301 first generates the random number r_{q_Z} and transmits the random number to the party X (S26-1). Then, the first computation means 302 computes the value c_{q_Z} according to

[FORMULA 27]

$$c_{q\_Z} = \sum_{q\_i2,q\_j0} (e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j2} (e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0}) + r_{q\_Z}$$

and transmits the value c_{q_Z} to the party Y (S26-2). Note that $e20_{q\_i2,q\_j0}$ and $e02_{q\_i0,q\_j2}$ represent any multipliers. The second computation means 303 receives the random number r_{q_Y} from the party Y and the value c_{q_X} from the party X and computes values c_{q_0} and c_{q_2} according to the following formula (S27).

[FORMULA 28]

$$c_{q\_0} = \sum_{q\_i0,q\_j0} (e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z}$$

$$c_{q\_2} = \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y}$$

Note that the series of steps S22-1 and S22-2, the series of steps S24-1 and S24-2 and the series of steps S26-1 and S26-2 can be performed in parallel, and the steps S23, S25 and S27 can also be performed in parallel.

[0051] Following the steps S21 to S27, each party performs a misuse detection processing as described below.

[0052] A processing performed by the party X will be described. First, the second random number generation means 304 generates a random number sequence ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) and a random number ρ_X and transmits the random number sequence and the random number to the party Y, and generates a random number sequence ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) and transmits the random number sequence to the party Z (S28). Then, the third computation means 305 computes a random number sequence ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$), transmits the random number sequence to the party Y, receives a random number sequence ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) from the party Y and a random number sequence ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) from the party Z, computes a random number sequence ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q-0}$, ..., $\alpha Y1_{q\_na1-1}$-s_{q_Y}·$a1_{q\_na1-1}$) and a value γ_X according to

[FORMULA 29]

$$\gamma_X = \sum_{i0,j1,q} (e01_{q\_i0,q\_j1} \cdot \alpha X0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{i1,j0,q} (e10_{q\_i1,q\_j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \rho_X$$

and transmits the random number sequence and the value to the party Z (S29). Then, the fourth computation means 306 receives a random number sequence ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-s_{q_Z}·$a2_{q\_na2-1}$) from the party Y and a value ρ_Z from the party Z, computes a value

[FORMULA 30]

$$\gamma'_Z = \sum_{i2,j0,q} \{e20_{q\_i2,q\_j0} \cdot (\alpha Z2_{q\_i2} - s_{q\_Z} \cdot a2_{q\_i2}) \cdot b0_{q\_j0} - s_{q\_Z} \cdot r_{q\_Z}\} + \rho_Z$$

and transmits the value to the party Y (S30). Then, the misuse detection means 307 receives a value γ_Y from the party Y, a value γ'_Y and a random number sequence ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$) from the party Z, computes

[FORMULA 31]

$$\sum_{i2,j1,q} \{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y ,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs valuesc_{q_0} and c_{q_1} if the computation result is 0 (S31).

[0053] Next, a processing performed by the party Y will be described. First, the second random number generation means 304 generates a random number sequence ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) and a random number ρ_Y and transmits the random number sequence and the random number to the party Z, and generates a random number sequence ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) and transmits the random number sequence to the party X (S32). Then, the third computation means 305 computes a random number sequence ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$), transmits the random number

sequence to the party Z, receives a random number sequence ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) from the party X and a random number sequence ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) from the party Z, computes a random number sequence ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-s_{q_Z}·$a2_{q\_na2-1}$) and a value

[FORMULA 32]

$$\gamma_Y = \sum_{i1,j2,q} (e12_{q\_i1,q\_j2} \cdot \alpha Y1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{i2,j1,q} (e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \rho_Y$$

and transmits the random number sequence and the value to the party X (S33). Then, the fourth computation means 306 receives the random number ρ_X from the party X and a random number sequence ($\alpha X0_{q\_0}$-s_{q_X}·$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-s_{q_X}·$a0_{q\_na0-1}$) from the party Z, computes a value

[FORMULA 33]

$$\gamma'_X = \sum_{i0,j1,q} \{e01_{q\_i0,q\_j1} \cdot (\alpha X0_{q\_i0} - s_{q\_x} \cdot a0_{q\_i0}) \cdot b1_{q\_j1} - s_{q\_x} \cdot r_{q\_x}\} + \rho_X$$

and transmits the value to the party Z (S34). Then, the misuse detection means 307 receives a value γ'_Z and a random number sequence ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) from the party X and a value γ_Z from the party Z, computes

[FORMULA 34]

$$\sum_{i0,j2,q} \{e02_{q\_i0,q\_j2} \cdot (\alpha Z0_{q\_i0} - s_{q\_z} \cdot a0_{q\_i0}) \cdot b2_{q\_j2} + s_{q\_z} \cdot c_{q\_z}\} - \gamma_Z + \gamma'_Z,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_1} and c_{q_2} if the computation result is 0 (S35).

[0054] Next, a processing performed by the party Z will be described. First, the second random number generation means 304 generates a random number sequence ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) and a random number ρ_Z and transmits the random number sequence and the random number to the party X, and generates a random number sequence ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) and transmits the random number sequence to the party Y (S36). Then, the third computation means 305 computes a random number sequence ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$), transmits the random number sequence to the party X, receives a random number sequence ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) from the party X and a random number sequence ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) from the party Y, computes a random number sequence ($\alpha X0_{q\_0}$-s_{q_X}·$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-s_{q_X}·$a0_{q\_na0-1}$) and a value γ_Z according to

[FORMULA 35]

$$\gamma_Z = \sum_{i2,j0,q} (e20_{q\_i2,q\_j0} \cdot \alpha Z2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{i0,j2,q} (e02_{q\_i0,q\_j2} \cdot \alpha Z0_{q\_i0} \cdot b2_{q\_j2}) + \rho_Z$$

and transmits the random number sequence and the value to the party Y (S37). Then, the fourth computation means 306 receives a random number sequence ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-s_{q_Y}·$a1_{q\_na1-1}$) from the party X and a value ρ_Y from the party Y, computes a value γ'_Y according to

[FORMULA 36]

$$\gamma'_Y = \sum_{i1,j2,q} \left\{ e12_{q\_i1,q\_j2} \cdot (\alpha Y1_{q\_i1} - s_{q\_Y} \cdot a1_{q\_i1}) \cdot b2_{q\_j2} - s_{q\_Y} \cdot r_{q\_Y} \right\} + \rho_Y$$

and transmits the value to the party X (S38). Then, the misuse detection means 307 receives the value γ_X from the party X and the value γ'_X and a random number sequence ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) from the party Y, computes

[FORMULA 37]

$$\sum_{i1,j0,q} \left\{ e10_{q\_i1,q\_j0} \cdot (\alpha X1_{q\_i1} - s_{q\_X} \cdot a1_{q\_i1}) \cdot b0_{q\_j0} + s_{q\_X} \cdot c_{q\_X} \right\} - \gamma_X + \gamma'_X ,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_2} and c_{q_0} if the computation result is 0 (S39).

[0055] If no misuse detection occurs, the total sum of the values c_{q_0}, c_{q_1} and c_{q_2} output from the parties X, Y and Z can be computed to obtain a sum-of-product computation result as expressed by the following formula.

[FORMULA 38]

$$\begin{aligned} & c_{q\_0} + c_{q\_1} + c_{q\_2} = \\ & \sum_{q\_i0,q\_j0} (e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) \\ & + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) + \sum_{q\_i1,q\_j1} (e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) \\ & + \sum_{q\_i1,q\_j2} (e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j1} (e21_{q\_i2,q\_j1} \cdot a2_{q\_i2} \cdot b1_{q\_j1}) \\ & + \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j0} (e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0}) \\ & + \sum_{q\_i0,q\_j2} (e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0}) \end{aligned}$$

In the processing described above, hash values or other values can be substituted for the random numbers.

[0056] The misuse detection according to the present invention is performed once for one multiplication, one sum-of-product computation or a set of multiplications or sum-of-product computations performed in parallel. The values $\alpha P{+}0_{q\_i0}$, $\alpha P{+}1_{q\_i1}$ and $\alpha P{+}2_{q\_i2}$ (q = 0, ..., m-1) included in the value γ_{P+} transmitted by the party P_+ involved with the misuse detection function are fragments of the respective values a_{q_i} multiplied by different random numbers. Thus, if any of the values is not correct, the party P_+ cannot predict the random numbers. Therefore, if the modulo is a prime number p, the probability that any misuse can be made agree with the misuse in the sum-of-product computation processing is only 1/(p-1).

[FOURTH EMBODIMENT]

[0057] A fourth embodiment is a specific example of the third embodiment, in which na0 = na1 = na2 = nb0 = nb1 = nb2 = n (n represents an integer equal to or greater than 1), and e00 = e01 = e10 = e11 = e12 = e21 = e22 = e20 = e02 = 1. Fig. 9 shows an example of a configuration of a secure sum-of-product computation system 400 according to this

embodiment, and Fig. 10 shows an example of a flow of a processing performed by the secure sum-of-product computation system 400. The secure sum-of-product computation system 400 comprises a party X, a party Y, a party Z, a data string decomposition and supply part 410 and an output part 420. As in the third embodiment, each party has first random number generation means 301, first computation means 302, second computation means 303, second random number generation means 304, third computation means 305, fourth computation means 306 and misuse detection means 307.

[0058] The secure sum-of-product computation system 400 performs a sum-of-product computation

[FORMULA 39]

$$\sum_{i=0}^{n-1} a_{q\_i} \cdot b_{q\_i}$$

for m sets of data strings Aq = (a_{q_0}, ..., a_{q_n-1}) and Bq = (b_{q_0}, ..., b_{q_n-1}) (m represents an integer equal to or greater than 1, and q = 0, ..., m-1) comprising elements a_{q_i} and b_{q_i} (i = 0, ..., n-1 (n represents an integer equal to or greater than 1)), which are natural numbers smaller than a prime number p, through cooperative computation by the three computation apparatuses, the parties X, Y and Z (the sum-of-product computation is a multiplication of a and b in the case where n = 1). As in the third embodiment, it is assumed that the parties X and Y previously share a random number s_{q_Z}, the parties Y and Z previously share a random number s_{q_X}, and the parties Z and X previously share a random number s_{q_Y}.

[0059] Specifically, the data string decomposition and supply part 410 first decomposes the m sets of input data strings Aq and Bq in such a manner that each element a_{q_i} and b_{q_i} satisfy conditional formulas $a_{q\_i} = a0_{q\_i}+a1_{q\_i}+a2_{q\_i} \bmod p$ and $b_{q\_i} = b0_{q\_i}+b1_{q\_i}+b2_{q\_i} \bmod p$ ($a0_{q\_i}$, $a1_{q\_i}$, $b0_{q\_i}$ and $b1_{q\_i}$ represent random numbers, and p represents a prime number) and supplies data strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_n-1})$, $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_n-1})$, $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_n-1})$ and $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_n-1})$ to the party X, the data strings A_{q_1}, $A_{q\_2} = (a2_{q\_0}, ..., a2_{q\_n-1})$, B_{q_1} and $B_{q\_2} = (b2_{q\_0}, ..., b2_{q\_n-1})$ to the party Y, and data strings A_{q_2}, A_{q_0}, B_{q_2} and B_{q_0} to the party Z (S41).

[0060] Then, the party X performs the following processing. The first random number generation means 301 first generates a random number r_{q_X} and transmits the random number to the party Y (S42-1). Then, the first computation means 302 computes a value c_{q_X} according to

[FORMULA 40]

$$c_{q\_x} = \sum_{i} (a0_{q\_i} \cdot b1_{q\_i} + a1_{q\_i} \cdot b0_{q\_i}) + r_{q\_x}$$

and transmits the value c_{q_X} to the party Z (S42-2). Then, the second computation means 303 receives a random number r_{q_Z} from the party Z and a value c_{q_Y} from the party Y and computes values c_{q_0} and c_{q_1} according to the following formula (S43).

[FORMULA 41]

$$c_{q\_0} = \sum_{i} (a0_{q\_i} \cdot b0_{q\_i}) + c_{q\_x} - r_{q\_z}$$

$$c_{q\_1} = \sum_{i} (a1_{q\_i} \cdot b1_{q\_i}) + c_{q\_Y} - r_{q\_x}$$

[0061] The party Y performs the following processing. The first random number generation means 301 first generates a random number r_{q_Y} and transmits the random number to the party Z (S44-1). Then, the first computation means 302 computes the value c_{q_Y} according to

[FORMULA 42]

$$c_{q\_Y} = \sum_i (a1_{q\_i} \cdot b2_{q\_i} + a2_{q\_i} \cdot b1_{q\_i}) + r_{q\_Y}$$

and transmits the value c_{q_Y} to the party X (S44-2). Then, the second computation means 306 receives the random number r_{q_X} from the party X and a value c_{q_Z} from the party Z and computes values c_{q_1} and c_{q_2} according to the following formula (S45).

[FORMULA 43]

$$c_{q\_1} = \sum_i (a1_{q\_i} \cdot b1_{q\_i}) + c_{q\_Y} - r_{q\_X}$$

$$c_{q\_2} = \sum_i (a2_{q\_i} \cdot b2_{q\_i}) + c_Z - r_Y$$

[0062] The party Z performs the following processing. The first random number generation means 301 first generates the random number r_{q_Z} and transmits the random number to the party X (S46-1). Then, the first computation means 302 computes the value c_{q_Z} according to

[FORMULA 44]

$$c_{q\_Z} = \sum_i (a2_{q\_i} \cdot b0_{q\_i} + a0_{q\_i} \cdot b2_{q\_i}) + r_{q\_Z}$$

and transmits the value c_{q_Z} to the party Y (S46-2). Then, the second computation means 303 receives the random number r_{q_Y} from the party Y and the value c_{q_X} from the party X and computes values c_{q_0} and c_{q_2} according to the following formula (S47).

[FORMULA 45]

$$c_0 = \sum_i (a0_i \cdot b0_i) + c_X - r_Z$$

$$c_2 = \sum_i (a2_i \cdot b2_i) + c_Z - r_Y$$

Note that the series of steps S42-1 and S4-2, the series of steps S44-1 S44-2 and the series of steps S46-1 and S46-2 can be performed in parallel, and the steps S43, S45 and S47 can also be performed in parallel.

[0063] Following the steps S41 to S47, each party performs a misuse detection processing as described below. A processing performed by the party X will be described. First, the second random number generation means 3 04 generates a random number sequence ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_n-1}$) and a random number ρ_x and transmits the random number sequence and the random number to the party Y, and generates a random number sequence ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$) and transmits the random number sequence to the party Z (S48). Then, the third computation means 305 computes a random number sequence ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$-s_{q_Z}·$a0_{q\_n-1}$), transmits the random number sequence to the party Y, receives a random number sequence ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$) from the party Y and a random number sequence ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_n-1}$) from the party Z, computes a random number sequence ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_n-1}$-s_{q_Y}·$a1_{q\_n-1}$) and a value γ_X according to

[FORMULA 46]

$$\gamma_X = \sum_{i,q} (\alpha X0_{q\_i} \cdot b1_{q\_i} + \alpha X1_{q\_i} \cdot b0_{q\_i}) + \rho_X$$

and transmits the random number sequence and the value to the party Z (S49). Then, the fourth computation means 306 receives a random number sequence ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_n-1}$-s_{q_Z}·$a2_{q\_n-1}$) from the party Y and a value ρ_Z from the party Z, computes a value γ'_Z according to

[FORMULA 47]

$$\gamma'_Z = \sum_{i,q} \{(\alpha Z2_{q\_i} - s_{q\_Z} \cdot a2_{q\_i}) \cdot b0_{q\_i} - s_{q\_Z} \cdot r_{q\_Z}\} + \rho_Z$$

and transmits the value to the party Y (S50). Then, the misuse detection means 307 receives a value γ_Y from the party Y, a value γ'_Y and a random number sequence ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$-s_{q_Y}·$a2_{q\_n-1}$) from the party Z, computes

[FORMULA 48]

$$\sum_{i,q} \{(\alpha Y2_{q\_i} - s_{q\_Y} \cdot a2_{q\_i}) \cdot b1_{q\_i} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_0} and c_{q_1} if the computation result is 0 (S51).

Next, a processing performed by the party Y will be described.

[0064] First, the second random number generation means 304 generates a random number sequence ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_n-1}$) and a random number ρ_Y and transmits the random number sequence and the random number to the party Z, and generates a random number sequence ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$ and transmits the random number sequence to the party X (S52). Then, the third computation means 305 computes a random number sequence ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$-s_{q_X}·$a1_{q\_n-1}$), transmits the random number sequence to the party Z, receives a random number sequence ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_n-1}$) from the party X and a random number sequence ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$) from the party Z, computes a random number sequence ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_n-1}$-s_{q_Z}·$a2_{q\_n-1}$) and a value γ_Y according to

[FORMULA 49]

$$\gamma_Y = \sum_{i,q} (\alpha Y1_{q\_i} \cdot b2_{q\_i} + \alpha Y2_{q\_i} \cdot b1_{q\_i}) + \rho_Y$$

and transmits the random number sequence and the value to the party X (S53). Then, the fourth computation means 306 receives the random number ρ_X from the party X and a random number sequence ($\alpha X0_{q\_0}$-s_{q_X}·$a0_{q\_0}$, ..., $\alpha X0_{q\_n-1}$-s_{q_X}·$a0_{q\_n-1}$) from the party Z, computes a value γ'_X according to

[FORMULA 50]

$$\gamma'_X = \sum_{i,q} \{(\alpha X0_{q\_i} - s_{q\_X} \cdot a0_{q\_i}) \cdot b1_{q\_i} - s_{q\_X} \cdot r_{q\_X}\} + \rho_X$$

and transmits the value to the party Z (S54). Then, the misuse detection means 307 receives a value γ'_Z and a random number sequence ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$-s_{q_Z}·$a0_{q\_n-1}$) from the party X and a value γ_Z from the party Z, computes

[FORMULA 51]

$$\sum_{i,q}\{(\alpha Z0_{q\_i} - s_{q\_Z}\cdot a0_{q\_i})\cdot b2_{q\_i} + s_{q\_Z}\cdot c_{q\_Z}\} - \gamma_Z + \gamma'_Z,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_1} and c_{q_2} if the computation result is 0 (S55).

[0065] Next, a processing performed by the party Z will be described. First, the second random number generation means 304 generates a random number sequence ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_n-1}$) and a random number ρ_Z and transmits the random number sequence and the random number to the party X, and generates a random number sequence ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$) and transmits the random number sequence to the party Y (S56). Then, the third computation means 305 computes a random number sequence ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$-s_{q_Y}·$a2_{q\_n-1}$), transmits the random number sequence to the party X, receives a random number sequence ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$) from the party X and a random number sequence ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_n-1}$) from the party Y, computes a random number sequence ($\alpha X0_{q\_0}$-s_{q_X}·$a0_{q\_0}$, ..., $\alpha X0_{q\_n-1}$-s_{q_X}·$a0_{q\_n-1}$) and a value γ_Z according to

[FORMULA 52]

$$\gamma_Z = \sum_{i,q}(\alpha Z2_{q\_i}\cdot b0_{q\_i} + \alpha Z0_{q\_i}\cdot b2_{q\_i}) + \rho_Z$$

and transmits the random number sequence and the value to the party Y (S57). Then, the fourth computation means 306 receives a random number sequence ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_n-1}$-s_{q_Y}·$a1_{q\_n-1}$) from the party X and a value ρ_Y from the party Y, computes a value γ'_Y according to

[FORMULA 53]

$$\gamma'_Y = \sum_{i,q}\{(\alpha Y1_{q\_i} - s_{q\_Y}\cdot a1_{q\_i})\cdot b2_{q\_i} - s_{q\_Y}\cdot r_{q\_Y}\} + \rho_Y$$

and transmits the value to the party X (S58). Then, the misuse detection means 307 receives the value γ_X from the party X and the value γ'_X and a random number sequence ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$-s_{q_X}·$a1_{q\_n-1}$) from the party Y, computes

[FORMULA 54]

$$\sum_{i,q}\{(\alpha X1_{q\_i} - s_{q\_X}\cdot a1_{q\_i})\cdot b0_{q\_i} + s_{q\_X}\cdot c_{q\_X}\} - \gamma_X + \gamma'_X,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_2} and c_{q_0} if the computation result is 0 (S59).

[0066] Then, the output part 420 computes the total sum (c_{q_0}+c_{q_1}+c_{q_2}) of the values c_{q_0}, c_{q_1} and c_{q_2} output from the parties X, Y and Z and outputs the total sum (S60).

[0067] The following relation holds.

[FORMULA 55]

$$\begin{aligned} c_{q\_0} + c_{q\_1} + c_{q\_2} &= \sum_i (a0_{q\_i} \cdot b0_{q\_i} + a0_{q\_i} \cdot b1_{q\_i} + a1_{q\_i} \cdot b0_{q\_i}) \\ &+ \sum_i (a1_{q\_i} \cdot b1_{q\_i} + a1_{q\_i} \cdot b2q_{q\_i} + a2_{q\_i} \cdot b1_{q\_i}) \\ &+ \sum_i (a2_{q\_i} \cdot b2_{q\_i} + a2_{q\_i} \cdot b0_{q\_i} + a0_{q\_i} \cdot b2_{q\_i}) \\ &= \sum_i (a0_{q\_i} + a1_{q\_i} + a2_{q\_i})(b0_{q\_i} + b1_{q\_i} + b2_{q\_i}) \\ &= \sum_i a_{q\_i} \cdot b_{q\_i} \end{aligned}$$

From the relation above, it can be seen that the sum-of-product computation (a multiplication of a_q and bq in the case where i = 1 (in the case where n = 1)) has been correctly done. In the processing described above, hash values or other values can be substituted for the random numbers.

[0068] The data string decomposition and supply part 410 and the output part 420 can be provided in an apparatus other than the parties or provided in any one or more of the apparatuses serving as the parties.

[0069] The effect of the method according to the present invention will be compared with that of the method described in Non-Patent literature 1. Provided that m = 1, according to the present invention, the number of rounds is 2, the number of pieces of data transmitted by each party is 10, and the number of random numbers generated by each party is 5. In addition, since the value S_P can be repeatedly used once it is shared among the parties, the actual number of rounds is 2, the actual number of pieces of data transmitted is 9, and the number of random numbers generated is 4. On the other hand, according to the method described in Non-Patent literature 1, the number of rounds is 4, the number of pieces of data transmitted by the party X is 20, the number of random numbers generated by the party X is 12, the number of pieces of data transmitted by the parties Y and Z is 17, and the number of random numbers generated by the parties Y and Z is 9. Therefore, the method according to the present invention is about twice as efficient as the method described in Non-Patent literature 1.

[0070] In the case where $m \geq 2$, the efficiency is further improved. According to the present invention, the number of rounds is 2, the number of pieces of data transmitted by each party is 6m + 3, and the number of random numbers generated by each party is 3m + 1. On the other hand, according to the method described in Non-Patent literature 1, the number of rounds is 4, the number of pieces of data transmitted by the party X is 20m, the number of random numbers generated by the party X is 12m, the number of pieces of data transmitted by the parties Y and Z is 17m, and the number of random numbers generated by the parties Y and Z is 9m. Therefore, the method according to the present invention is about three times as efficient as the method described in Non-Patent literature 1.

[FIFTH EMBODIMENT]

[0071] While the secure sum-of-product computation system 400 according to the fourth embodiment is configured to perform a sum-of-product computation expressed as

[FORMULA 56]

$$\sum_{i=0}^{n-1} a_{q\_i} \cdot b_{q\_i},$$

a secure sum-of-product computation system 500 according to a fifth embodiment has a configuration in which one of the values involved in the multiplication is fixed, for example. More specifically, the secure sum-of-product computation system 500 performs the following m sum-of-product computations of a data string $Aq = (a_{q\_0}, ..., a_{q\_n-1})$ (m represents

an integer equal to or greater than 1, and q = 0, ..., m-1) comprising elements a_{q_i} (q = 0, ..., m-1 (m represents an integer equal to or greater than 1), and i = 0, ..., n-1 (n represents an integer equal to or greater than 1)), which are natural numbers smaller than a prime number p, and a value b, which is a natural number smaller than the prime number p, through cooperative computation by three computation apparatuses, the parties X, Y and Z.

[FORMULA 57]

$$\sum_{i=0}^{n-1} a_{q\_i} \cdot b$$

The functional configuration and the process flow are the same as those in the fourth embodiment and therefore will be described below with reference to them (that is, Fig. 9 (and Fig. 8) showing the configuration and Fig. 10 showing the process flow). As in the fourth embodiment, it is assumed that the parties X and Y previously share a random number s_{q_Z}, the parties Y and Z previously share a random number s_{q_X}, and the parties Z and X previously share a random number s_{q_Y}.

[0072] Specifically, the data string decomposition and supply part 410 first decomposes the input data string Aq and the value b in such a manner that each element a_{q_i} of the data string satisfies a conditional formula $a_{q\_i} = a0_{q\_i}+a1_{q\_i}+a2_{q\_i}$ mod p and the value satisfies a conditional formula b = b0+b1+b2 mod p ($a0_{q\_i}$, $a1_{q\_i}$, b0 and b 1 represent random numbers, and p represents a prime number) and supplies data strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_n-1})$ and $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_n-1})$ and values b0 and b1 to the party X, data strings A_{q_1} and $A_{q\_2} = (a2_{q\_0}, ..., a2_{q\_n-1})$ and values b1 and b2 to the party Y, and data strings A_{q_2} and A_{q_0} and values b2 and b0 to the party Z (S41).

[0073] Then, the party X performs the following processing. The first random number generation means 301 first generates a random number r_{q_X} and transmits the random number to the party Y (S42-1). Then, the first computation means 302 computes a value c_{q_X} according to

[FORMULA 58]

$$c_{q\_X} = \sum_{i} (a0_{q\_i} \cdot b1 + a1_{q\_i} \cdot b0) + r_{q\_X}$$

and transmits the value c_{q_X} to the party Z (S42-2). Then, the second computation means 303 receives a random number r_{q_Z} from the party Z and a value c_{q_Y} from the party Y and computes values c_{q_0} and c_{q_1} according to the following formula (S43).

[FORMULA 59]

$$c_{q\_0} = \sum_{i} (a0_{q\_i} \cdot b0) + c_{q\_X} - r_{q\_Z}$$

$$c_{q\_1} = \sum_{i} (a1_{q\_i} \cdot b1) + c_{q\_Y} - r_{q\_X}$$

[0074] The party Y performs the following processing. The random number generation means 304 first generates a random number r_{q_Y} and transmits the random number to the party Z (S44-1). Then, the first computation means 305 computes the value c_{q_Y} according to

[FORMULA 60]

$$c_{q\_Y} = \sum_i (a1_{q\_i} \cdot b2 + a2_{q\_i} \cdot b1) + r_{q\_Y}$$

and transmits the value c_{q_Y} to the party X (S44-2). Then, the second computation means 306 receives the random number r_{q_X} from the party X and a value c_{q_Z} from the party Z and computes values c_{q_1} and c_{q_2} according to the following formula (S45).

[FORMULA 61]

$$c_{q\_1} = \sum_i (a1_{q\_i} \cdot b1) + c_{q\_Y} - r_{q\_X}$$

$$c_{q\_2} = \sum_i (a2_{q\_i} \cdot b2) + c_{q\_Z} - r_{q\_Y}$$

[0075] The party Z performs the following processing. The first random number generation means 301 first generates the random number r_{q_Z} and transmits the random number to the party X (S46-1). Then, the first computation means 302 computes the value c_{q_Z} according to

[FORMULA 62]

$$c_{q\_Z} = \sum_i (a2_{q\_i} \cdot b0 + a0_{q\_i} \cdot b2) + r_{q\_Z}$$

and transmits the value c_{q_Z} to the party Y (S46-2). Then, the second computation means 303 receives the random number r_{q_Y} from the party Y and the value c_{q_X} from the party X and computes values c_{q_0} and c_{q_2} according to the following formula (S47).

[FORMULA 63]

$$c_{q\_0} = \sum_i (a0_{q\_i} \cdot b0) + c_{q\_X} - r_{q\_Z}$$

$$c_{q\_2} = \sum_i (a2_{q\_i} \cdot b2) + c_{q\_Z} - r_{q\_Y}$$

Note that the series of steps S42-1 and S42-2, the series of steps S44-1 and S44-2 and the series of steps S46-1 and S46-2 can be performed in parallel, and the steps S43, S45 and S47 can also be performed in parallel.

[0076] Following the steps S41 to S47, each party performs a misuse detection processing as described below. A processing performed by the party X will be described. First, the second random number generation means 304 generates random numbers $\alpha Y1$ and ρ_x and transmits the random numbers to the party Y, and generates a random number $\alpha Z0$ and transmits the random number to the party Z (S48). Then, the third computation means 305 computes a value

[FORMULA 64]

$$\alpha Z0 - \sum_{i,q} (s_{q\_Z} \cdot a0_{q\_i}),$$

transmits the value to the party Y, receives a random number $\alpha X1$ from the party Y and a random number $\alpha X0$ from the party Z, computes values

[FORMULA 65]

$$\alpha Y1 - \sum_{i,q} (s_{q\_Y} \cdot a1_{q\_i})$$

and

[FORMULA 66]

$$\gamma_X = \alpha X0 \cdot b1 + \alpha X1 \cdot b0 + \rho_X$$

and transmits the values to the party Z (S49). Then, the fourth computation means 306 receives a value

[FORMULA 67]

$$\alpha Z2 - \sum_{i,q} (s_{q\_Z} \cdot a2_{q\_i})$$

from the party Y and a value ρ_Z from the party Z, computes a value

[FORMULA 68]

$$\gamma'_Z = (\alpha Z2 - \sum_{i,q} (s_{q\_Z} \cdot a2_{q\_i})) \cdot b0 - \sum_{q} s_{q\_Z} \cdot r_{q\_Z} + \rho_Z$$

and outputs the value to the party Y (S50).

[0077] Then, the misuse detection means 307 receives a value γ_Y from the party Y, a value γ'_Y and a value

[FORMULA 69]

$$\alpha Y2 - \sum_{i,q} (s_{q\_Y} \cdot a2_{q\_i})$$

from the party Z, computes

[FORMULA 70]

$$(\alpha Y2 - \sum_{i,q}(s_{q\_Y} \cdot a2_{q\_i})) \cdot b1 + \sum_{q} s_{q\_Y} \cdot c_{q\_Y} - \gamma_Y + \gamma'_Y,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_0} and c_{q_1} if the computation result is 0 (S51).

[0078] Next, a processing performed by the party Y will be described. First, the second random number generation means 304 generates random numbers $\alpha Z2$ and ρ_Y and transmits the random numbers to the party Z, and generates a random number $\alpha X1$ and transmits the random number to the party X (S52). Then, the third computation means 305 computes a value

[FORMULA 71]

$$\alpha X1 - \sum_{i,q}(s_{q\_X} \cdot a1_{q\_i})$$

transmits the value to the party Z, receives a random number $\alpha Y1$ from the party X and a random number $\alpha Y2$ from the party Z, computes

[FORMULA 72]

$$\alpha Z2 - \sum_{i,q}(s_{q\_Z} \cdot a2_{q\_i})$$

and

[FORMULA 73]

$$\gamma_Y = \alpha Y1 \cdot b2 + \alpha Y2 \cdot b1 + \rho_Y$$

and transmits the values to the party X (S53). Then, the fourth computation means 306 receives the random number ρ_X from the party X and a value

[FORMULA 74]

$$\alpha X0 - \sum_{i,q}(s_{q\_X} \cdot a0_{q\_i})$$

from the party Z, computes a value γ'_X according to

[FORMULA 75]

$$\gamma'_X = (\alpha X0 - \sum_{i,q}(s_{q\_X} \cdot a0_{q\_i})) \cdot b1 - \sum_{q} s_{q\_X} \cdot r_{q\_X} + \rho_X$$

and transmits the value to the party Z (S54). Then, the misuse detection means 307 receives a value γ'_Z and a value

[FORMULA 76]

$$\alpha Z0 - \sum_{i,q} (s_{q\_Z} \cdot a0_{q\_i})$$

from the party X and a value γ_Z from the party Z, computes

[FORMULA 77]

$$(\alpha Z0 - \sum_{i,q} (s_{q\_Z} \cdot a0_{q\_i})) \cdot b2 + \sum_{q} s_{q\_Z} \cdot c_{q\_Z} - \gamma_Z + \gamma'_Z,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_1} and c_{q_2} if the computation result is 0 (S55).

[0079] Next, a processing performed by the party Z will be described. First, the second random number generation means 304 generates random numbers $\alpha X0$ and ρ_Z and transmits the random numbers to the party X, and generates a random number $\alpha Y2$ and transmits the random number to the party Y (S56). Then, the third computation means 305 computes a value

[FORMULA 78]

$$\alpha Y2 - \sum_{i,q} (s_{q\_Y} \cdot a2_{q\_i}),$$

transmits the value to the party X, receives a random number $\alpha Z0$ from the party X and a random number $\alpha Z2$ from the party Y, computes values

[FORMULA 79]

$$\alpha X0 - \sum_{i,q} (s_{q\_X} \cdot a0_{q\_i})$$

and

[FORMULA 80]

$$\gamma_Z = \alpha Z2 \cdot b0 + \alpha Z0 \cdot b2 + \rho_Z$$

and transmits the values to the party Y (S57). Then, the fourth computation means 306 receives a value

[FORMULA 81]

$$\alpha Y1 - \sum_{i,q} (s_{q\_Y} \cdot a1_{q\_i})$$

from the party X and a value ρ_Y from the party Y, computes a value γ'_Y according to

[FORMULA 82]

$$\gamma'_Y = (\alpha Y1 - \sum_{i,q}(s_{q\_Y} \cdot a1_{q\_i})) \cdot b2 - \sum_{q} s_{q\_Y} \cdot r_{q\_Y} + \rho_Y$$

and transmits the value to the party X (S58). Then, the misuse detection means 307 receives the value γ_X from the party X and the value γ'_X and a value

[FORMULA 83]

$$\alpha X1 - \sum_{i,q}(s_{q\_X} \cdot a1_{q\_i})$$

from the party Y, computes

[FORMULA 84]

$$(\alpha X1 - \sum_{i,q}(s_{q\_X} \cdot a1_{q\_i})) \cdot b0 + \sum_{q} s_{q\_X} \cdot c_{q\_X} - \gamma_X + \gamma'_X,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_2} and c_{q_0} if the computation result is 0 (S59).

[0080] Then, the output part 420 computes the total sum ($c_{q\_0}+c_{q\_1}+c_{q\_2}$) of the values c_{q_0}, c_{q_1} and c_{q_2} output from the parties X, Y and Z and outputs the total sum (S60).

[FORMULA 85]

$$\begin{aligned} c_{q\_0} + c_{q\_1} + c_{q\_2} &= \sum_{i}(a0_{q\_i} \cdot b0 + a0_{q\_i} \cdot b1 + a1_{q\_i} \cdot b0) \\ &\quad + \sum_{i}(a1_{q\_i} \cdot b1 + a1_{q\_i} \cdot b2 + a2_{q\_i} \cdot b1) \\ &\quad + \sum_{i}(a2_{q\_i} \cdot b2 + a2_{q\_i} \cdot b0 + a0_{q\_i} \cdot b2) \\ &= \sum_{i}(a0_{q\_i} + a1_{q\_i} + a2_{q\_i})(b0 + b1 + b2) \\ &= \sum_{i} a_{q\_i} \cdot b \end{aligned}$$

From the relation above, it can be seen that the sum-of-product computation has been correctly done. In the processing described above, hash values or other values can be substituted for the random numbers. The data string decomposition and supply part 410 and the output part 420 can be provided in an apparatus other than the parties or provided in any one or more of the apparatuses serving as the parties.

[0081] The effect of the method according to the present invention will be compared with that of the method described in Non-Patent literature 1. According to the present invention, the number of rounds is 2, the number of pieces of data

transmitted by each party is 2m, and the number of random numbers generated by each party is 3. Therefore, the method according to the present invention is about nine times as efficient as the method described in Non-Patent literature 1. An improvement is that the number of random numbers generated is constant and therefore does not depend on the value m, rather than increasing with the value m.

[SIXTH EMBODIMENT]

[0082] In the multiplication protocol for a and b, the secure sum-of-product computation system 300 with a misuse detection function shown in the third embodiment uses values α_{P0p} and α_{PP-} indicating fragment values of a value $s_P \cdot a_{0p}$ to compare $(\alpha_{P0p}-\alpha_{PP-}) \cdot b_{1p}$ and $s_P \cdot a_{0p} \cdot b_{1p}$ and uses values α_{P1p} and α_{PP+} indicating fragment values of a value $s_P \cdot a_{1p}$ to compare $(\alpha_{P1p}-\alpha_{PP+}) \cdot b_{0p}$ and $s_P \cdot a_{1p} \cdot b_{0p}$ in order to check the validity of $a_{0p} \cdot b_{1p}+a_{1p} \cdot b_{0p}$. However, in the former comparison, the multiplication protocol of the secure sum-of-product computation system 300 involves a procedure of round-trip transmission of computed values between the parties. Specifically, the value $\alpha Z2_{q\_i2}-s_{q\_Z} \cdot a2_{q\_i2}$ needs to be transmitted from the party Y to the party X and then transmitted from the party X back to the party Y, the value $\alpha X0_{q\_i0}-s_{q\_X} \cdot a0_{q\_i0}$ needs to be transmitted from the party Z to the party Y and then transmitted from the party Y back to the party Z, and the value $\alpha Y1_{q\_i1}-s_{q\_Y} \cdot a1_{q\_i1}$ needs to be transmitted from the party X to the party Z and then transmitted from the party Z back to the party X. Therefore, a computed value may leak during the transmission, and a server may perform a misuse (acquisition of information concerning data to be concealed) without causing a change of the computation result. That is, the third embodiment can be said to provide a configuration capable of perfect concealment as far as the server perform no misuse.

[0083] A sixth embodiment provides a configuration capable of perfect concealment even if the server performs a misuse. More specifically, the sixth embodiment provides a configuration whose protocol does not involve a round-trip transmission of a computed value that can lead to a misuse. Fig. 11 shows an example of a configuration of a secure sum-of-product computation system 600, and Fig. 12 shows an example of a flow of a processing performed by the secure sum-of-product computation system 600. The secure sum-of-product computation system 600 comprises a party X, a party Y and a party Z. As shown in Fig. 13, each party has first random number generation means 301, first computation means 302 and second computation means 303, which are the same as those of the secure sum-of-product computation system 300, as well as second random number generation means 604, third computation means 605, fourth computation means 606 and misuse detection means 607.

[0084] In the following specific description, the functions of the first random number generation means 301, the first computation means 302 and the second computation means 303 and the secure sum-of-product computation processing (steps S21 to S27) implemented by these functions are the same as those of the secure sum-of-product computation system 300 and therefore will not be further described, and the misuse detection processing, which differs from that of the secure sum-of-product computation system 300, will be particularly described.

[0085] Following the steps S21 to S27, each party performs a misuse detection processing as described below. As in the third embodiment, it is assumed that the parties X and Y previously share a random number s_{q_Z}, the parties Y and Z previously share a random number s_{q_X}, and the parties Z and X previously share a random number s_{q_Y}.

[0086] A processing performed by the party X will be described. First, the second random number generation means 604 generates a random number ρ_x and transmits the random number to the party Y, and generates random number sequences $(\alpha Z0_{q\_0}, ..., \alpha Z0_{q\_na0-1})$ and $(\beta Z0_{q\_0}, ..., \beta Z0_{q\_nb0-1})$ and transmits the random number sequences to the party Z (S68). Then, the third computation means 605 computes random number sequences $(\alpha Z0_{q\_0}-S_{q\_Z} \cdot a0_{q\_0}, ..., \alpha Z0_{q\_na0-1}-s_{q\_Z} \cdot a0_{q\_na0-1})$ and $(\beta Z0_{q\_0}-s_{q\_Z} \cdot b0_{q\_0}, ..., \beta Z0_{q\_nb0-1}-s_{q\_Z} \cdot b0_{q\_nb0-1})$, transmits the random number sequences to the party Y, receives random number sequences $(\alpha X1_{q\_0}, ..., \alpha X1_{q\_na1-1})$ and $(\beta X1_{q\_0}, ..., \beta X1_{q\_nb1-1})$ from the party Y, computes a value γ_X according to

[FORMULA 86]

$$\gamma_X = \sum_{i1,j0,q} (e10_{q\_i1,q\_j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \sum_{i0,j1,q} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot \beta X1_{q\_j1}) + \rho_X$$

and transmits the value to the party Z (S69). Then, the fourth computation means 606 receives a random number ρ_Z from the party Z, computes a value γ'_Z according to

[FORMULA 87]

$$\gamma'_Z = \sum_q (-s_{q\_z} \cdot r_{q\_z}) + \rho_Z$$

and transmits the value to the party Y (S70). Then, the misuse detection means 607 receives a value γ_Y from the party Y, a value γ'_Y and random number sequences ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$) and ($\beta Y2_{q\_0}$-s_{q_Y}·$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2\_1}$-s_{q_Y}·$b2_{q\_nb2-1}$) from the party Z, computes

[FORMULA 88]

$$\sum_{i1,i2,j1,j2,q} \{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + e12_{q\_i1,q\_j2} \cdot (\beta Y2_{q\_j2} - s_{q\_Y} \cdot b2_{q\_j2}) \cdot a1_{q\_i1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y ,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_0} and c_{q_1} if the computation result is 0 (S71).

[0087] Next, a processing performed by the party Y will be described. First, the second random number generation means 604 generates a random number ρ_Y and transmits the random number to the party Z, and generates random number sequences ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) and ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$) and transmits the random number sequences to the party X (S72). Then, the third computation means 605 computes random number sequences ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) and ($\beta X1L_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-s_{q_X}·$b1_{q\_nb1-1}$), transmits the random number sequences to the party Z, receives random number sequences ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) and ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) from the party Z, computes a value γ_Y according to

[FORMULA 89]

$$\gamma_Y = \sum_{i2,j1,q} (e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \sum_{i1,j2,q} (e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot \beta Y2_{q\_j2}) + \rho_Y$$

and transmits the value to the party X (S73). Then, the fourth computation means 606 receives the random number ρ_X from the party X, computes a value γ'_X according to

[FORMULA 90]

$$\gamma'_X = \sum_q (-s_{q\_x} \cdot r_{q\_x}) + \rho_X$$

and transmits the value to the party Z (S74). Then, the misuse detection means 607 receives a value γ'_Z and random number sequences ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) and ($\beta Z0_{q\_0}$-s_{q_Z}·$b0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$-s_{q_Z}·$b0_{q\_nb0-1}$) from the party X and a value γ_Z from the party Z, computes

[FORMULA 91]

$$\sum_{i0,i2,j0,j2,q}\{e02_{q\_i0,q\_j2}\cdot(\alpha Z0_{q\_i0}-s_{q\_Z}\cdot a0_{q\_i0})\cdot b2_{q\_j2} + e20_{q\_i2,q\_j0}\cdot(\beta Z0_{q\_j0}-s_{q\_Z}\cdot b0_{q\_j0})\cdot a2_{q\_i2}+s_{q\_Z}\cdot c_{q\_Z}\}-\gamma_Z+\gamma'_Z$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_1} and c_{q_2} if the computation result is 0 (S75).

[0088] Next, a processing performed by the party Z will be described. First, the second random number generation means 604 generates a random number ρ_Z and transmits the random number to the party X, and generates random number sequences ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2\text{-}1}$) and ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2\text{-}1}$) and transmits the random number sequences to the party Y (S76). Then, the third computation means 605 computes random number sequences ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2\text{-}1}$-$s_{q\_Y}$·$a2_{q\_na2\text{-}1}$) and ($\beta Y2_{q\_0}$-$s_{q\_Y}$·$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2\text{-}1}$-$s_{q\_Y}$·$b2_{q\_nb2\text{-}1}$), transmits the random number sequences to the party X, receives random number sequences ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0\text{-}1}$) and ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0\text{-}1}$) from the party X, computes a value γ_Z according to

[FORMULA 92]

$$\gamma_Z=\sum_{i0,j2,q}(e02_{q\_i0,q\_j2}\cdot\alpha Z0_{q\_i0}\cdot b2_{q\_j0})+\sum_{i2,j0,q}(e20_{q\_i2,q\_j0}\cdot a2_{q\_i2}\cdot\beta Z0_{q\_j0})+\rho_Z$$

and transmits the value to the party Y (S77). Then, the fourth computation means 606 receives a random number ρ_Y from the party Y, computes a value γ'_Y according to

[FORMULA 93]

$$\gamma'_Y=\sum_{q}(-s_{q\_Y}\cdot r_{q\_Y})+\rho_Y$$

and transmits the value to the party X (S78). Then, the misuse detection means 607 receives the value γ_X from the party X and the value γ'_X and random number sequences ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1\text{-}1}$-$s_{q\_X}$·$a1_{q\_na1\text{-}1}$) and ($\beta X1_{q\_0}$-$s_{q\_X}$·$b1_{q\_0}$, ..., $\beta X1_{q\_nb1\text{-}1}$-$s_{q\_X}$·$b1_{q\_nb1\text{-}1}$) from the party Y, computes

[FORMULA 94]

$$\sum_{i0,i1,j0,j1,q}\{e10_{q\_i1,q\_j0}\cdot(\alpha X1_{q\_i1}-s_{q\_X}\cdot a1_{q\_i1})\cdot b0_{q\_j0} + e01_{q\_i0,q\_j1}\cdot(\beta X1_{q\_j1}-s_{q\_X}\cdot b1_{q\_j1})\cdot a0_{q\_i0}+s_{q\_X}\cdot c_{q\_X}\}-\gamma_X+\gamma'_X$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_2} and c_{q_0} if the computation result is 0 (S79). In the processing described above, hash values or other values can be substituted for the random numbers.

[0089] In the multiplication protocol for a and b, the secure sum-of-product computation system 600 described above uses values β_{P1p} and β_{PP+} indicating fragment values of a value s_P·b_{1p} to compare (β_{P1p}+a_{0p}·β_{PP+}) and s_P·a_{1p}·b_{0p} and uses values α_{P1p} and α_{PP+} indicating fragment values of a value s_P·a_{1p} to compare (α_{P1p}-α_{PP}+)·b_{0p} and s_P·a_{1p}·b_{0p} in order to check the validity of a_{0p}·b_{1p}+a_{1p}·b_{0p}. With such a configuration, the protocol involves no round-trip transmission of computed values among the parties. Therefore, leakage of a computed value can be prevented, and therefore, the server cannot perform a misuse. In addition, the number of processing steps is the same as that of the secure sum-of-

product computation system 300, the secure sum-of-product computation system 600 can maintain approximately the same level of efficiency.

[SEVENTH EMBODIMENT]

[0090] A seventh embodiment is a specific example of the sixth embodiment, in which na0 = na1 = na2 = nb0 = nb1 = nb2 = n, and e00 = e01 = e10 = e11 = e12 = e21 = e22 = e20 = e02 = 1. Fig. 14 shows an example of a configuration of a secure sum-of-product computation system 700 according to this embodiment, and Fig. 15 shows an example of a flow of a processing performed by the secure sum-of-product computation system 700. The secure sum-of-product computation system 700 comprises a party X, a party Y, a party Z, a data string decomposition and supply part 410 and an output part 420. The data string decomposition and supply part 410 and the output part 420 are the same as those of the secure sum-of-product computation system 400 according to the fourth embodiment. As shown in Fig. 13, each party has first random number generation means 301, first computation means 302 and second computation means 303, which are the same as those of the secure sum-of-product computation system 400, as well as second random number generation means 604, third computation means 605, fourth computation means 606 and misuse detection means 607.

[0091] As with the secure sum-of-product computation system 400 according to the fourth embodiment, the secure sum-of-product computation system 700 performs each set of sum-of-product computations

[FORMULA 95]

$$\sum_{i=0}^{n-1} a_{q\_i} \cdot b_{q\_i}$$

for m sets of data strings Aq = (a_{q_0}, ..., a_{q_n-1}) and Bq = (b_{q_0}, ..., b_{q_n-1}) comprising elements a_{q_i} and b_{q_i}, which are natural numbers smaller than a prime number p, through cooperative computation by the three computation apparatuses, the parties X, Y and Z (the sum-of-product computation is a multiplication of a_q and bq in the case where n = 1).

[0092] In the following specific description, the functions of the data string decomposition and supply part 410, the first random number generation means 301, the first computation means 302, the second computation means 303 and the output part 420 and the secure sum-of-product computation processing (steps S41 to S47 and S60) implemented by these functions are the same as those of the secure sum-of-product computation system 400 according to the fourth embodiment and therefore will not be further described, and the misuse detection processing, which differs from that of the secure sum-of-product computation system 400, will be particularly described.

[0093] Following the steps S41 to S47, each party performs a misuse detection processing as described below. As in the sixth embodiment, it is assumed that the parties X and Y previously share a random number s_{q_Z}, the parties Y and Z previously share a random number s_{q_X}, and the parties Z and X previously share a random number s_{q_Y}.

[0094] A processing performed by the party X will be described. First, the second random number generation means 604 generates a random number ρ_X and transmits the random number to the party Y, and generates random number sequences ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$) and ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_n-1}$) and transmits the random number sequences to the party Z (S88). Then, the third computation means 605 computes random number sequences ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$-s_{q_Z}·$a0_{q\_n-1}$) and ($\beta Z0_{q\_0}$-s_{q_Z}·$b0_{q\_0}$, ..., $\beta Z0_{q\_n-1}$-s_{q_Z}·$b0_{q\_n-1}$), transmits the random number sequences to the party Y, receives random number sequences ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$) and ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_n-1}$) from the party Y, computes a value γ_X according to

[FORMULA 96]

$$\gamma_X = \sum_{i,q} (\alpha X1_{q\_i} \cdot b0_{q\_i} + a0_{q\_i} \cdot \beta X1_{q\_i}) + \rho_X$$

and transmits the value to the party Z (S89). Then, the fourth computation means 606 receives a random number ρ_Z from the party Z, computes a value γ'_Z according to

[FORMULA 97]

$$\gamma'_Z = \sum_q (-s_{q\_Z} \cdot r_{q\_Z}) + \rho_Z$$

and transmits the value to the party Y (S90). Then, the misuse detection means 607 receives a value γ_Y from the party Y, a value γ'_Y and random number sequences ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$-s_{q_Y}·$a2_{q\_n-1}$) and ($\beta Y2_{q\_0}$-s_{q_Y}·$b2_{q\_0}$, ..., $\beta Y2_{q\_n-1}$-s_{q_Y}·$b2_{q\_n-1}$) from the party Z, computes

[FORMULA 98]

$$\sum_{i,q} \{(\alpha Y2_{q\_i} - s_{q\_Y} \cdot a2_{q\_i}) \cdot b1_{q\_i} + (\beta Y2_{q\_i} - s_{q\_Y} \cdot b2_{q\_i}) \cdot a1_{q\_i} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y ,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_0} and c_{q_1} if the computation result is 0 (S91).

[0095] Next, a processing performed by the party Y will be described. First, the second random number generation means 604 generates a random number ρ_Y and transmits the random number to the party Z, and generates random number sequences ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$) and ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_n-1}$) and transmits the random number sequences to the party X (S92). Then, the third computation means 605 computes random number sequences ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$-s_{q_X}·$a1_{q\_n-1}$) and ($\beta X1_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1_{q\_n-1}$-s_{q_X}·$b1_{q\_n-1}$), transmits the random number sequences to the party Z, receives random number sequences ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$) and ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_n-1}$) from the party Z, computes a value γ_Y according to

[FORMULA 99]

$$\gamma_Y = \sum_{i,q} (\alpha Y2_{q\_i} \cdot b1_{q\_i} + a1_{q\_i} \cdot \beta Y2_{q\_i}) + \rho_Y$$

and transmits the value to the party X (S93). Then, the fourth computation means 606 receives the random number ρ_X from the party X, computes a value γ'_X according to

[FORMULA 100]

$$\gamma'_X = \sum_q (-s_{q\_X} \cdot r_{q\_X}) + \rho_X$$

and transmits the value to the party Z (S94). Then, the misuse detection means 607 receives a value γ'_Z and random number sequences ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$-s_{q_Z}·$a0_{q\_n-1}$) and ($\beta Z0_{q\_0}$-s_{q_Z}·$b0_{q\_0}$, ..., $\beta Z0_{q\_n-1}$-s_{q_Z}·$b0_{q\_n-1}$) from the party X and a value γ_Z from the party Z, computes

[FORMULA 101]

$$\sum_{i,q} \{(\alpha Z0_{q\_i} - s_{q\_Z} \cdot a0_{q\_i}) \cdot b2_{q\_i} + (\beta Z0_{q\_i} - s_{q\_Z} \cdot b0_{q\_i}) \cdot a2_{q\_i} + s_{q\_Z} \cdot c_{q\_Z}\} - \gamma_Z + \gamma'_Z ,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_1} and c_{q_2} if the computation result is 0 (S95).

[0096] Next, a processing performed by the party Z will be described.

[0097] First, the second random number generation means 604 generates a random number ρ_Z and transmits the random number to the party X, and generates random number sequences ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_n-1}$) and ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_n-1}$) and transmits the random number sequences to the party Y (S96). Then, the third computation means 605 computes random number sequences ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., ..., $\alpha Y2_{q\_n-1}$-s_{q_Y}·$a2_{q\_n-1}$) and ($\beta Y2_{q\_0}$-s_{q_Y}·$b2_{q\_0}$, ..., $\beta Y2_{q\_n-1}$-s_{q_Y}·$b2_{q\_n-1}$), transmits the random number sequences to the party X, receives random number sequences ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_n-1}$) and ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_n-1}$) from the party X, computes a value γ_Z according to

[FORMULA 102]

$$\gamma_Z = \sum_{i,q} (\alpha Z0_{q\_i} \cdot b2_{q\_i} + a2_{q\_i} \cdot \beta Z0_{q\_i}) + \rho_Z$$

and transmits the value to the party Y (S97). Then, the fourth computation means 606 receives a random number ρ_Y from the party Y, computes a value γ'_Y according to

[FORMULA 103]

$$\gamma'_Y = \sum_{q} (-s_{q\_Y} \cdot r_{q\_Y}) + \rho_Y$$

and transmits the value to the party X (S98). Then, the misuse detection means 607 receives the value γ_X from the party X and the value γ'_X and random number sequences ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_n-1}$-s_{q_X}·$a1_{q\_n-1}$) and ($\beta X1_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1q_{\_n-1}$-s_{q_X}·$b1_{q\_n-1}$) from the party Y, computes

[FORMULA 104]

$$\sum_{i,q} \{(\alpha X1_{q\_i} - s_{q\_X} \cdot a1_{q\_i}) \cdot b0_{q\_i} + (\beta X1_{q\_i} - s_{q\_X} \cdot b1_{q\_i}) \cdot a0_{q\_i} + s_{q\_X} \cdot c_{q\_X}\} - \gamma_X + \gamma'_X ,$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_2} and c_{q_0} if the computation result is 0 (S99). In the processing described above, hash values or other values can be substituted for the random numbers.

[EIGHTH EMBODIMENT]

[0098] While the secure sum-of-product computation system 700 according to the seventh embodiment is configured to perform a sum-of-product computation expressed as

[FORMULA 105]

$$\sum_{i=0}^{n-1} a_{q\_i} \cdot b_{q\_i}$$

as with the secure sum-of-product computation system 400 according to the fourth embodiment and apply the method

according to the embodiment 6 to the misuse detection processing for the sum-of-product computation, a secure sum-of-product computation system 800 according to an eighth embodiment has a configuration in which one of the values involved in the multiplication in the sum-of-product computation is fixed. More specifically, the secure sum-of-product computation system 800 is configured to perform the following m sum-of-product computations of a data string $A_q = (a_{q\_0}, ..., a_{q\_n-1})$ comprising elements a_{q_i}, which are natural numbers smaller than a prime number p, and a value b, which is a natural number smaller than the prime number p, through cooperative computation by three computation apparatuses, the parties X, Y and Z, as with the secure sum-of-product computation system 500 according to the fifth embodiment and apply the misuse detection method according to the sixth embodiment to the misuse detection processing for the sum-of-product computation.

[FORMULA 106]

$$\sum_{i=0}^{n-1} a_{q\_i} \cdot b$$

[0099] In the following specific description, the functions of the data string decomposition and supply part 410, the first random number generation means 301, the first computation means 302, the second computation means 303 and the output part 420 and the secure sum-of-product computation processing (steps S41 to S47 and S60) implemented by these functions are the same as those of the secure sum-of-product computation system 500 according to the fifth embodiment and therefore will not be further described, and the misuse detection processing, which differs from that of the secure sum-of-product computation system 500, will be particularly described. The functional configuration and the process flow are the same as those in the seventh embodiment and therefore will be described below with reference to them (that is, Fig. 14 (and Fig. 13) showing the configuration and Fig. 15 showing the process flow).

[0100] Following the steps S41 to S47, each party performs a misuse detection processing as described below. As in the seventh embodiment, it is assumed that the parties X and Y previously share a random number s_{q_Z}, the parties Y and Z previously share a random number s_{q_X}, and the parties Z and X previously share a random number s_{q_Y}.

[0101] A processing performed by the party X will be described. First, the second random number generation means 604 generates a random number ρ_x and transmits the random number to the party Y, and generates random numbers $\alpha Z0$ and $\beta Z0_q$ and transmits the random numbers to the party Z (S88). Then, the third computation means 605 computes random numbers

[FORMULA 107]

$$\alpha Z0 - \sum_{i,q} (s_{q\_Z} \cdot a0_{q\_i}),$$

$$\beta Z0_q - s_{q\_Z} \cdot b0$$

transmits the random numbers to the party Y, receives random numbers $\alpha X1$ and $\beta X1_q$ from the party Y, computes a value γ_X according to

[FORMULA 108]

$$\gamma_X = \alpha X1 \cdot b0 + \sum_{i,q} (a0_{q\_i} \cdot \beta X1_q) + \rho_X$$

and transmits the value to the party Z (S89). Then, the fourth computation means 606 receives a random number ρ_Z from the party Z, computes a value γ'_Z according to

[FORMULA 109]

$$\gamma'_Z = -\sum_q (s_{q\_z} \cdot r_{q\_z}) + \rho_Z$$

and transmits the value to the party Y (S90). Then, the misuse detection means 607 receives a value γ_Y from the party Y, a value γ'_Y and values

[FORMULA 110]

$$\alpha Y2 - \sum_{i,q} (s_{q\_Y} \cdot a2_{q\_i})$$

and

[FORMULA 111]

$$\beta Y2_q - s_{q\_Y} \cdot b2$$

from the party Z, computes

[FORMULA 112]

$$(\alpha Y2 - \sum_{i,q} (s_{q\_Y} \cdot a2_{q\_i})) \cdot b1$$

$$+ \sum_q \left\{ \sum_i (a1_{q\_i} (\beta Y2_q - s_{q\_Y} \cdot b2)) + s_{q\_Y} \cdot c_{q\_Y} \right\} - \gamma_Y + \gamma'_Y \text{,}$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_0} and c_{q_1} if the computation result is 0 (S91).

[0102] Next, a processing performed by the party Y will be described. First, the second random number generation means 604 generates a random number ρ_Y and transmits the random number to the party Z, and generates random numbers $\alpha X1$ and $\beta X1_q$ and transmits the random numbers to the party X (S92). Then, the third computation means 605 computes random numbers

[FORMULA 113]

$$\alpha X1 - \sum_{i,q} (s_{q\_X} \cdot a1_{q\_i}) \quad ,$$

$$\beta X1_q - s_{q\_X} \cdot b1$$

transmits the random numbers to the party Z, receives random numbers $\alpha Y2$ and $\beta Y2_q$ from the party Z, computes a value γ_Y according to

[FORMULA 114]

$$\gamma_Y = \alpha Y2 \cdot b1 + \sum_{i,q} (a1_{q\_i} \cdot \beta Y2_q) + \rho_Y$$

and transmits the value to the party X (S93). Then, the fourth computation means 606 receives the random number ρ_X from the party X, computes a value γ'_X according to

[FORMULA 115]

$$\gamma'_X = -\sum_q (s_{q\_X} \cdot r_{q\_X}) + \rho_X$$

and transmits the value to the party Z (S94). Then, the misuse detection means 607 receives a random number γ_Z from the party Z and random numbers γ'_Z,

[FORMULA 116]

$$\alpha Z0 - \sum_{i,q} (s_{q\_Z} \cdot a0_{q\_i})$$

and

[FORMULA 117]

$$\beta Z0_q - s_{q\_Z} \cdot b0$$

from the party X, computes

[FORMULA 118]

$$(\alpha Z0 - \sum_{i,q} (s_{q\_z} \cdot a0_{q\_i})) \cdot b2$$

$$+ \sum_q \left\{ \sum_i (a2_{q\_i} (\beta Z0_q - s_{q\_z} \cdot b0)) + s_{q\_z} \cdot c_{q\_z} \right\} - \gamma_Z + \gamma'_Z \text{,}$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_1} and c_{q_2} if the computation result is 0 (S95).

[0103] Next, a processing performed by the party Z will be described. First, the second random number generation means 604 generates a random number ρ_Z and transmits the random number to the party X, and generates random numbers $\alpha Y2$ and $\beta Y2_q$ and transmits the random numbers to the party Y (S96). Then, the third computation means 605 computes random numbers

[FORMULA 119]

$$\alpha Y2 - \sum_{i,q}(s_{q\_Y} \cdot a2_{q\_i}) \quad ,$$

$$\beta Y2_q - s_{q\_Y} \cdot b2$$

transmits the random numbers to the party X, receives random numbers $\alpha Z0$ and $\beta Z0_q$ from the party X, computes a value γ_Z according to

[FORMULA 120]

$$\gamma_Z = \alpha Z0 \cdot b2 + \sum_{i,q}(a2_{q\_i} \cdot \beta Z0_q) + \rho_Z$$

and transmits the value to the party Y (S97). Then, the fourth computation means 606 receives a random number ρ_Y from the party Y, computes a value$\gamma\,'_Y$ according to

[FORMULA 121]

$$\gamma'_Y = -\sum_{q}(s_{q\_Y} \cdot r_{q\_Y}) + \rho_Y$$

and transmits the value to the party X (S98). Then, the misuse detection means 607 receives the value γ_X from the party X and random numbers γ'_X,

[FORMULA 122]

$$\alpha X1 - \sum_{i,q}(s_{q\_X} \cdot a1_{q\_i})$$

and

[FORMULA 123]

$$\beta X1_q - s_{q\_X} \cdot b1$$

from the party Y, computes

[FORMULA 124]

$$(\alpha X1 - \sum_{i,q}(s_{q\_X} \cdot a1_{q\_i})) \cdot b0$$

$$+ \sum_{q}\left\{\sum_{i}(a0_{q\_i}(\beta X1_q - s_{q\_X} \cdot b1)) + s_{q\_X} \cdot c_{q\_X}\right\} - \gamma_X + \gamma'_X \text{ ,}$$

ends the processing by outputting data indicating a misuse detection if the computation result is not 0, and outputs values c_{q_2} and c_{q_0} if the computation result is 0 (S99). In the processing described above, hash values or other values can be substituted for the random numbers.

[NINTH EMBODIMENT]

[0104] According to the sixth and seventh embodiments, two data strings $A = (a_{q\_0},..., a_{q\_n-1})$ and $B = (b_{q\_0}, ..., b_{q\_n-1})$ are divided into three fragment data strings A_0, A_1 and A_2 and B_0, B_1 and B_2, respectively, in such a manner that the fragments satisfy conditions that $A = A_0+A_1+A_2$ mod p and $B = B_0+B_1+B_2$ mod p, the data strings $A_0 = (a0_{q\_0}, ..., a0_{q\_na0-1})$, $A_1 = (a1_{q\_0}, ..., a1_{q\_na1-1})$, $B_0 = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ and $B_1 = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ are supplied to the party X as values to be concealed, the data strings A_1, $A_2 = (a2_{q\_0}, ..., a2_{q\_na2-1})$, B_1 and $B_2 = (b2_{q\_0}, ..., b2_{q\_nb2-1})$ are supplied to the party Y as values to be concealed, the data strings A_2, A_0, B_2 and B_0 are supplied to the party Z as valued to be concealed, and thus, the secure sum-of-product of these values expressed by the following formula can be securely computed by determining the value $c_{q\_0}+c_{q\_1}+c_{q\_2}$ from the values c_{q_0} and c_{q_1}, which are the results of the computation performed by the party X, the values c_{q_1} and c_{q_2}, which are the results of the computation performed by the party Y, and the values c_{q_2} and c_{q_0}, which are the results of the computation performed by the party Z.

[FORMULA 125]

$$\sum_{q\_i0,q\_j0}(e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1})$$
$$+ \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) + \sum_{q\_i1,q\_j1}(e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1})$$
$$+ \sum_{q\_i1,q\_j2}(e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j1}(e21_{q\_i2,q\_j1} \cdot a2_{q\_i2} \cdot b1_{q\_j1})$$
$$+ \sum_{q\_i2,q\_j2}(e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j0}(e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0})$$
$$+ \sum_{q\_i0,q\_j2}(e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0})$$

[0105] Focusing on the six terms $\Sigma a0_{q\_i0} \cdot b1_{q\_j1}$, $\Sigma a1_{q\_i1} \cdot b0_{q\_j0}$, $\Sigma a1_{q\_i1} \cdot b2_{q\_j2}$, $\Sigma a2_{q\_i2} \cdot b1_{q\_j1}$, $\Sigma a2_{q\_i2} \cdot b0_{q\_j0}$ and $\Sigma a0_{q\_i0} \cdot b2_{q\_j2}$ in the above formula of the secure sum-of-product computation, one party has both the two fragment values of each term, another party has one of the two fragment values, and the remaining party has the other of the two fragment values. For example, concerning the fragment values $a0_{q\_i0}$ and $b1_{q\_j1}$ of the term $\Sigma a0_{q\_i0} \cdot b1_{q\_j1}$, the party X has both the fragment values $a0_{q\_i0}$ and $b1_{q\_j1}$, the party Y has only the fragment value $b1_{q\_j1}$, and the party Z has only the fragment value $a0_{q\_i0}$. The same holds true for the term $\Sigma a1_{q\_i1} \cdot b0_{q\_j0}$. A secure sum-of-product computation system 900 according to a ninth embodiment implements a method of determining a sum-of-product of two fragment values in the case where any one of three parties has both the two fragment values, another of the three parties has one of the two fragment values, and the remaining one of the three parties has the other of the two fragment values, that is, a sum-of-product computation method on which the secure sum-of-product computation according to the sixth and seventh embodiments is based.

[0106] In the following, an example in which the party X has both the fragment values, the party Y has one of the two fragment values, and the party Z has the other of the two fragment values will be described. However, the computation can also be achieved in the same manner in the cases where the party Y has both the fragment values, the party X has one of the two fragment values, and the party Z has the other of the two fragment values and where the party Z has both the fragment values, the party X has one of the two fragment values, and the party Y has the other of the two fragment values.

[0107] Fig. 16 shows an example of a configuration of the secure sum-of-product computation system 900, and Fig. 17 shows an example of a flow of a processing performed by the secure sum-of-product computation system 900. The secure sum-of-product computation system 900 comprises a party X, a party Y and a party Z, which are computation apparatuses. The party X has party-X random number generation means 901 and party-X computation means 903, the party Y has party-Y random number generation means 902 and party-Y computation means 904, and the party Z has misuse detection means 905.

[0108] The secure sum-of-product computation system 900 performs a total of m sets of sum-of-product computations of data strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0-1})$ and $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_1na-1})$ and data strings $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ and $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ expressed as the following formula by cooperative computation by the three computation apparatuses, the parties X, Y and Z (i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, j1 = 0, ..., nb1-1, na0, na1, nb0 and nb1 represent natural numbers, $e01_{q\_i0,q\_j1}$ and $e10_{q\_i1,q\_j0}$ represent any numbers, q = 0, ..., m-1, and m represents an integer equal to or greater than 1) (the computations are performed in parallel in the case where m is equal to or greater than 2).

[FORMULA 126]

$$\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0})$$

[0109] Data strings A_{q_0}, A_{q_1}, B_{q_0} and B_{q_1} are input to the party X, data strings A_{q_1} and B_{q_1} are input to the party Y, and data strings A_{q_0} and B_{q_0} are input to the party Z (S101).

[0110] First, the party-X random number generation means 901 in the party X generates random numbers c_{q_1} and γ_1 and random number sequences $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_nb0-1})$ and $(\beta 1_{q\_0}, ..., \beta 1_{q\_na0-1})$ and transmits the random numbers and the random number sequences to the party Y (S102). In addition, the party-Y random number generation means 902 in the party Y generates a random number s_q and transmits the random number to the party Z (S103).

[0111] Then, the party-X computation means 903 in the party X computes random numbers c_{q_0} and γ_0 according to

[FORMULA 127]

$$c_{q\_0} = \sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) - c_{q\_1}$$

$$\gamma_0 = \sum_{i0,j0,q}(a0_{q\_i0} \cdot \beta 1_{q\_i0} + b0_{q\_j0} \cdot \alpha 1_{q\_j0}) - \gamma_1$$

and transmits the random numbers to the party Z (S104).

[0112] In addition, the party-Y computation means 904 in the party Y receives the random numbers c_{q_1} and γ_1 and the random number sequences $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_nb0-1})$ and $(\beta 1_{q\_0}, ..., \beta 1_{q\_na0-1})$ from the party X, computes number sequences $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_nb0-1})$ and $(\beta 0_{q\_0}, ..., \beta 0_{q\_na0-1})$ and a value γ' according to

[FORMULA 128]

$$\alpha 0_{q\_j0} = \sum_{q,\,q\_i1} s_q \cdot e10_{q\_i1,\,q\_j0} \cdot a1_{q\_i1} - \alpha 1_{q\_j0}$$

$$\beta 0_{q\_i0} = \sum_{q,\,q\_j1} s_q \cdot e01_{q\_i0,\,q\_j1} \cdot b1_{q\_j1} - \beta 1_{q\_i0},$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

and transmits the number sequences and the value to the party Z (S105).

[0113] Then, the misuse detection means 905 in the party Z receives the random numbers c_{q_0} and γ_0 from the party X and the random number s_q, the number sequences ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) and ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) and the value γ' from the party Y, computes

[FORMULA 129]

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma',$$

and ends the processing by outputting data indicating a misuse detection if the computation result is not 0 (S106).

[0114] If the result of the computation by the misuse detection means 905 is 0, the party X outputs the random numbers c_{q_0} and c_{q_1}, the party Y outputs the random number c_{q_1} and 0, and the party Z outputs 0 and the random number c_{q_0} (S107). In the processing described above, hash values or other values can be substituted for the random numbers.

[TENTH EMBODIMENT]

[0115] A tenth embodiment is a specific example of the ninth embodiment, in which na0 = na1 = na2 = nb0 = nb1 = nb2 = n, and e00 = e01 = e10 = e11 = e12 = e21 = e22 = e20 = e02 = 1. The configuration and the process flow are the same as those according to the ninth embodiment (an example of the configuration is shown in Fig. 16, and an example of the process flow is shown in Fig. 17). A secure sum-of-product computation system 910 according to the tenth embodiment performs a total of m sets of sum-of-product computations of data strings A_{q_0} = ($a0_{q\_0}$, ..., $a0_{q\_n-1}$) and A_{q_1} = ($a1_{q\_0}$, ..., $a1_{q\_n-1}$) and data stringsB_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_n-1}$) and B_{q_1} = ($b1_{q\_0}$, ..., $b1_{q\_n-1}$) expressed as the following formula by cooperative computation by the three computation apparatuses, the parties X, Y and Z (i = 0, ..., n-1, n represents a natural number, q = 0, ..., m-1, and m represents an integer equal to or greater than 1) (the computations are performed in parallel in the case where m is equal to or greater than 2).

[FORMULA 130]

$$\sum_{q\_i} a0_{q\_i} \cdot b1_{q\_i} + \sum_{q\_i} a1_{q\_i} \cdot b0_{q\_i}$$

[0116] Data strings A_{q_0}, A_{q_1}, B_{q_0} and B_{q_1} are input to the party X, data strings A_{q_1} and B_{q_1} are input to the party Y, and data strings A_{q_0} and B_{q_0} are input to the party Z (S101).

[0117] First, the party-X random number generation means 901 in the party X generates random numbers c_{q_1} and γ_1 and random number sequences ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) and ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_n-1}$) and transmits the random numbers and the random number sequences to the party Y (S 102). In addition, the party-Y random number generation means 902 in the party Y generates a random number s_q and transmits the random number to the party Z (S103).

[0118] Then, the party-X computation means 903 in the party X computes random numbers c_{q_0} and γ_0 according to

[FORMULA 131]

$$c_{q\_0} = \sum_{q\_i} a0_{q\_i} \cdot b1_{q\_i} + \sum_{q\_i} a1_{q\_i} \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = \sum_{i,q} (a0_{q\_i} \cdot \beta 1_{q\_i} + b0_{q\_i} \cdot \alpha 1_{q\_i}) - \gamma_1$$

and transmits the random numbers to the party Z (S104).

[0119] In addition, the party-Y computation means 904 in the party Y receives the random numbers c_{q_1} and γ_1 and the random number sequences ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) and ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_n-1}$) from the party X, computes number sequences ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) and ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_n-1}$) and a value γ' according to

[FORMULA 132]

$$\alpha 0_{q\_i} = s_q \cdot a1_{q\_i} - \alpha 1_{q\_i}$$

$$\beta 0_{q\_i} = s_q \cdot b1_{q\_i} - \beta 1_{q\_i},$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

and transmits the number sequences and the value to the party Z (S105).

[0120] Then, the misuse detection means 905 in the party Z receives the random numbers c_{q_0} and γ_0 from the party X and the random number s_q, the number sequences ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) and ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_n-1}$) and the value γ' from the party Y, computes

[FORMULA 133]

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i,q} (a0_{q\_i} \cdot \beta 0_{q\_i} + b0_{q\_i} \cdot \alpha 0_{q\_i}) + \gamma',$$

and ends the processing by outputting data indicating a misuse detection if the computation result is not 0 (S106).

[0121] If the result of the computation by the misuse detection means 905 is 0, the party X outputs the random numbers c_{q_0} and c_{q_1}, the party Y outputs the random number c_{q_1} and 0, and the party Z outputs 0 and the random number c_{q_0} (S107). In the processing described above, hash values or other values can be substituted for the random numbers.

[ELEVENTH EMBODIMENT]

[0122] A secure sum-of-product computation system 920 according to an eleventh embodiment is the secure sum-of-product computation system 910 according to the tenth embodiment that is improved so as to be able to more efficiently and securely perform the sum-of-product computation

[FORMULA 134]

$$\sum_{q\_i} a0_{q\_i} \cdot b1_{q\_i} + \sum_{q\_i} a1_{q\_i} \cdot b0_{q\_i}$$

with one of the multipliers in each term being fixed regardless of the values i and q, that is,

[FORMULA 135]

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} \cdot$$

[0123] The configuration and the process flow of the secure sum-of-product computation system 920 are the same as those according to the ninth and tenth embodiment (an example of the configuration is shown in Fig. 16, and an example of the process flow is shown in Fig. 17). However, data a0 and a1 and data strings $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_n-1})$ and $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_n-1})$ are input to the party X, the data a1 and the data string B_{q_1} are input to the party Y, and the data a0 and the data string B_{q_0} are input to the party Z (S 101).

[0124] First, the party-X random number generation means 901 in the party X generates random numbers c_{q_1} and γ_1, a random number sequence $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_n-1})$ and a random number $\beta 1$ and transmits the random numbers and the random number sequence to the party Y (S102).

[0125] In addition, the party-Y random number generation means 902 in the party Y generates a random number s_q and transmits the random number to the party Z (S103).

[0126] Then, the party-X computation means 903 in the party X computes random numbers c_{q_0} and γ_0 according to

[FORMULA 136

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

and transmits the random numbers to the party Z (S104).

[0127] In addition, the party-Y computation means 904 in the party Y receives the random numbers c_{q_1} and γ_1, the random number sequence $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_n-1})$ and the random number $\beta 1$ from the party X, computes a number sequence $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_n-1})$ and value $\beta 0$ and γ' according to

[FORMULA 137]

$$\alpha 0_{q\_i} = \sum_{q} s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1 \quad ,$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

and transmits the number sequence and the values to the party Z (S105).

[0128] Then, the misuse detection means 905 in the party Z receives the random numbers c_{q_0} and γ_0 from the party X and the random number s_q, the number sequence $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_n-1})$ and the values $\beta 0$ and γ' from the party Y, computes

[FORMULA 138]

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma',$$

and ends the processing by outputting data indicating a misuse detection if the computation result is not 0 (S106).

[0129] If the result of the computation by the misuse detection means 905 is 0, the party X outputs the random numbers c_{q_0} and c_{q_1}, the party Y outputs the random number c_{q_1} and 0, and the party Z outputs 0 and the random number c_{q_0} (S107). In the processing described above, hash values or other values can be substituted for the random numbers.

[0130] The processings in the secure sum-of-product computation methods according to the present invention performed by the secure sum-of-product computation systems according to the present invention described above can be performed not only sequentially in the order described above but also in parallel with each other or individually as required or depending on the processing power of the apparatus that performs the processings. The functions of components of the secure sum-of-product computation systems according to the present invention can be combined or divided as required. Furthermore, other various modifications can be appropriately made without departing form the spirit of the present invention. In the case where the secure sum-of-product computation systems according to the embodiments of the present invention are implemented by computers, the specific processings of the functions of the apparatuses and the components thereof are described in programs. The programs are stored in a hard disk drive, for example, and a required program or data is loaded into a random access memory (RAM) for execution. The computer implements the specific processing by the CPU executing the loaded program.

Claims

1. A computation apparatus that is used in performing a sum-of-product computation by three computation apparatuses in cooperation, the three computation apparatuses serving as a party X, a party Y and a party Z and performing symmetric processings,
wherein provided that any of the computation apparatuses is a party P, it is assumed that the party Z is a party P_-, and the party Y is a party P_+, and subscripts 0p, 1p and 2p are 0, 1 and 2, respectively, if the party P is the party X, the party X is the party P_-, the party Z is the party P_+, and the subscripts 0p, 1p and 1p are 1, 2 and 0, respectively, if the party P is the party Y, and the party Y is the party P_-, the party X is the party P_+, and the subscripts 0p, 1p and 2p are 2, 0 and 1, respectively, if the party P is the party Z,
m represents an integer equal to or greater than 1, na0p, na1p, na2p, nb0p and nb1p represent natural numbers, $q = 0, ..., m-1$, $i0p = 0, ..., na0p-1$, $i1p = 0, ..., na1p-1$, $i2p = 0, ..., na2p-1$, $j0p = 0, ..., nb0p-1$, and $j1p = 0, ..., nb1p-1$, and $e0p1p_{i0p,j1p}$, $e1p0p_{i1p,j0p}$, $e0p0p_{i0p,j0p}$ and $e1p1p_{i1p,j1p}$ represent any numbers,
characterized in that said party P comprises:

first random number generation means (101, 301) adapted to generate a number r_{q_P} and transmit the number to the party P_+;
first computation means (102, 302) adapted to receive data strings $A_{q\_0p} = (a0p_{q\_0}, ..., a0p_{q\_na0p-1})$, $A_{q\_1p} = (a1p_{q\_0}, ..., a1p_{q\_na1p-1})$, $B_{q\_0p} = (b0p_{q\_0}, ..., b0p_{q\_nb0p-1})$ and $B_{q\_1p} = (b1p_{q\_0}, ..., b1p_{q\_nb1p-1})$, compute a value c_{q_P} according to

$$c_{q\_P} = \sum_{q\_i0p,q\_j1p} (e0p1p_{q\_i0p,q\_j1p} \cdot a0p_{q\_i0p} \cdot b1p_{q\_j1p}) + \sum_{q\_i1p,q\_j0p} (e1p0p_{q\_i1p,q\_j0p} \cdot a1p_{q\_i1p} \cdot b0p_{q\_j0p}) + r_{q\_P},$$

and transmit the value to the party P_-; and
second computation means (103, 303) adapted to receive a number r_{q_P-} from the party P_-, a value c_{q_P+} from the party P_+, compute values c_{q_0p} and c_{q_1p} according to

$$c_{q\_0p} = \sum_{q\_i0p,q\_j0p} (e0p0p_{q\_i0p,q\_j0p} \cdot a0p_{q\_i0p} \cdot b0p_{q\_j0p}) + c_{q\_P} - r_{q\_P-}$$

$$c_{q\_1p} = \sum_{q\_i1p,q\_j1p} (e1p1p_{q\_i1p,q\_j1p} \cdot a1p_{q\_i1p} \cdot b1p_{q\_j1p}) + c_{q\_P+} - r_{q\_P}$$

2. The computation apparatus according to claim 1, **characterized in that**
the parties P_- and P previously share a number s_{q_P+}, the parties P and P_+ previously share a number s_{q_P-}, and the parties P_+ and P_- previously share a number s_{q_P}, and
the party P further comprises:

second random number generation means (304) adapted to generate a number sequence ($\alpha P_+1p_{q\_0}$, ..., $\alpha P_+1p_{q\_na1p-1}$) and a number ρ_P and transmit the number sequence and the number to the party P_+, and generate a number sequence ($\alpha P\_0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$) and transmit the number sequence to the party P_-;
third computation means (305) adapted to compute a number sequence ($\alpha P\_0p_{q\_0}$-s_{q_P-}·$a0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$-s_{q_P-}·$a0p_{q\_na0p-1}$) and transmit the number sequence to the party P_+, receive a number sequence ($\alpha P1p_{q\_0}$, ..., $\alpha P1p_{q\_na1p-1}$) from the party P_+ and a number sequence ($\alpha P0p_{q\_0}$ ... , $\alpha P0p_{q\_na0p-1}$) from the party P_-, compute a number sequence ($\alpha P_+1p_{q\_0}$-s_{q_P+}·alp_{q_0}, ..., $\alpha P_+1p_{q\_na1p-1}$-s_{q_P+}·$a1p_{q\_na1p-1}$) and a value

$$\gamma_P = \sum_{i0p,j1p,q} (e0p1p_{i0p,j1p} \cdot \alpha P0p_{q\_i0p} \cdot b1p_{q\_j1p}) + \sum_{i1p,j0p,q} (e1p0p_{i1p,j0p} \cdot \alpha P1p_{q\_i1p} \cdot b0p_{q\_j0p}) + \rho_P ,$$

and transmit the number sequence and the value to the party P_-;
fourth computation means (306) adapted to receive a number sequence ($\alpha P\_2p_{q\_0}$-s_{q_P-}·$a2p_{q\_0}$, ..., $\alpha P\_2p_{q\_na2p-1}$-s_{q_P}·$a2p_{q\_na2p-1}$) from the party P_+ and a value ρ_{P-} from the party P_-, compute a value γ'_{P-}

$$\gamma'_{P-} = \sum_{i2p,j0p,q} \{(\alpha P\_2p_{q\_i2p} - s_{q\_P-} \cdot a2p_{q\_i2p}) \cdot b0p_{q\_j0p} - s_{q\_P-} \cdot r_{q\_P-}\} + \rho_{P-} ,$$

and transmit the value to the party P_+; and
misuse detection means (307) adapted to receive a value γ_{P+} from the party P_+ and a value γ'_{P+} and a number sequence ($\alpha P+2p_{q\_0}$-s_{q_P+}·$a2p_{q\_0}$, ..., $\alpha P+2p_{q\_na2p-1}$-s_{q_P+}·$a2p_{q\_na2p-1}$) from the party P_-, compute

$$\sum_{i2p,j1p,q} \{(\alpha P_+2p_{q\_i2p} - s_{q\_P+} \cdot a2p_{q\_i2p}) \cdot b1p_{q\_j1p} + s_{q\_P+} \cdot c_{q\_P+}\} - \gamma_{P+} + \gamma'_{P+} ,$$

end the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and output a values c_{q_0p} and c_{q_1p} if the result of the computation is 0.

3. The computation apparatus according to claim 1, **characterized in that**
the parties P_- and P previously share a number s_{q_P+}, the parties P and P_+ previously share a number s_{q_P-}, and the parties P_+ and P_- previously share a number s_{q_P}, and
the party P further comprises:

second random number generation means (604) adapted to generate a number pp and transmit the number to the party P_+, and generate number sequences ($\alpha P\_0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$) and ($\beta P\_0p_{q\_0}$, ..., $\beta P\_0p_{q\_nb0p-1}$) and transmit the number sequences to the party P_-;
third computation means (605) adapted to compute number sequences ($\alpha P\_0p_{q\_0}$-s_{q_P-}·$a0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$-s_{q_P-}·$a0p_{q\_na0p-1}$) and (βP-$0p_{q\_0}$-s_{q_P-}·$b0p_{q\_0}$, ..., $\beta P\_0p_{q\_na0p-1}$-s_{q_P-}·$b0p_{q\_na0p-1}$) and transmit the number sequences to the party P_+, receive number sequences ($\alpha P1p_{q\_0}$, ..., $\alpha P1p_{q\_na1p-1}$) and ($\beta P1p_{q\_0}$, ..., $\beta P1p_{q\_nb1p-1}$) from the party P_+, compute a value

$$\gamma_P = \sum_{i1p,j0p,q} (e1p0p_{i1p,j0p} \cdot \alpha P1p_{q\_i1p} \cdot b0p_{q\_j0p}) + \sum_{i0p,j1p,q} (e0p1p_{i0p,j1p} \cdot a0p_{q\_i0p} \cdot \beta P1p_{q\_j1p} + \rho_P),$$

and transmit the value to the party P_-;
fourth computation means (606) adapted to receive a value ρ_{P-} from the party P_-, compute

$$\gamma'_{P-} = \sum_{q} (-s_{q\_P-} \cdot r_{q\_P-}) + \rho_{P-},$$

and transmit the value to the party P_+; and
misuse detection means (607) adapted to receive a value γ_{P+} from the party P_+ and a value γ'_{P+} and number sequences ($\alpha P+2p_{q\_0}$-s_{q_P+}·$a2p_{q\_0}$, ..., $\alpha P_+2p_{q\_na2p-1}$-s_{q_P+}·$a2p_{q\_na2p-1}$) and ($\beta P+2p_{q\_0}$-s_{q_P+}·$b2p_{q\_0}$, ..., $\beta P+2p_{q\_na2p-1}$-s_{q_P+}·$b2p_{q\_na2p-1}$) from the party P_-, compute

$$\sum_{i1p,i2p,j1p,j2p,q} \{(\alpha P_+2p_{q\_i2p} - s_{q\_P+} \cdot a2p_{q\_i2p}) \cdot b1p_{q\_j1p} + (\beta P_+2p_{q\_j2p} - s_{q\_P+} \cdot b2p_{q\_j2p}) \cdot a1p_{q\_i1p} + s_{q\_P+} \cdot c_{q\_P+}\}, - \gamma_{P+} + \gamma'_{P+}$$

end the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and output a values c_{q_0p} and c_{q_1p} if the result of the computation is 0.

4. A secure sum-of-product computation method used for performing, in parallel, a total of m sets of sum-of-product computations of data strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0-1})$, $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_na1-1})$ and $A_{q\_2} = (a2_{q\_0}), ..., a2_{q\_na2-1})$ and $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$, $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ and $B_{q\_2} = (b2_{q\_0}, ..., b2_{q\_nb2-1})$ by cooperative computation by three computation apparatuses, which are a party X, a party Y and a party Z, the sum-of-product computations being expressed as

$$\sum_{q\_i0,q\_j0}(e00_{q\_i0,q\_j0}\cdot a0_{q\_i0}\cdot b0_{q\_j0})+\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1}\cdot a0_{q\_i0}\cdot b1_{q\_j1})$$
$$+\sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0}\cdot a1_{q\_i1}\cdot b0_{q\_j0})+\sum_{q\_i1,q\_j1}(e11_{q\_i1,q\_j1}\cdot a1_{q\_i1}\cdot b1_{q\_j1})$$
$$+\sum_{q\_i1,q\_j2}(e12_{q\_i1,q\_j2}\cdot a1_{q\_i1}\cdot b2_{q\_j2})+\sum_{q\_i2,q\_j1}(e21_{q\_i2,q\_j1}\cdot a2_{q\_i2}\cdot b1_{q\_j1})$$
$$+\sum_{q\_i2,q\_j2}(e22_{q\_i2,q\_j2}\cdot a2_{q\_i2}\cdot b2_{q\_j2})+\sum_{q\_i2,q\_j0}(e20_{q\_i2,q\_j0}\cdot a2_{q\_i2}\cdot b0_{q\_j0})$$
$$+\sum_{q\_i0,q\_j2}(e02_{q\_i0,q\_j2}\cdot a2_{q\_i2}\cdot b0_{q\_i0})$$

where q = 0, ..., m-1, m represents an integer equal to or greater than 1, na0, na1, na2, nb0, nb1 and nb2 represent natural numbers, 10 = 0, ..., na0-1, i 1 = 0, ..., na1-1, i2 = 0, ..., na2-1, j0 = 0, ..., nb0- 1, j1 = 0, ..., nb1-1, and j2 = 0, ..., nb2-1, and $e01_{q\_i0,q\_j1}$, $e10_{q\_i1,q\_j0}$, $e00_{q\_i0,q\_j0}$, $e11_{q\_i1,q\_j1}$, $e12_{q\_i1,q\_j2}$, $e21_{q\_i2,q\_j1}$, $e22_{q\_i2,q\_j2}$; $e20_{q\_i2,q\_j0}$ and $e02_{q\_i0,q\_j2}$ represent any numbers, and the data strings A_{q_0}, A_{q_1}, B_{q_0} and B_{q_1} being input to the party X, the data strings A_{q_1}, A_{q_2}, B_{q_1} and B_{q_2} being input to the party Y, and the data strings A_{q_2}, A_{q_0}, B_{q_2} and B_{q_0} being input to the party Z,

characterized in that said secure sum-of-product computation method comprising:

a party-X first random number generation step (S2-1, S22-1) in which the party X generates a number r_{q_X} and transmits the number to the party Y;

a party-X first computation step (S2-2, S22-2) in which the party X computes a value c_{q_X} according to

$$c_{q\_X}=\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1}\cdot a0_{q\_i0}\cdot b1_{q\_j1})+\sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0}\cdot a1_{q\_i1}\cdot b0_{q\_j0})+r_{q\_X}$$

and transmits the value to the party Z;

a party-X second computation step (S3, S23) in which the party X receives a number r_{q_Z} from the party Z and a value c_{q_Y} from the party Y, computes values c_{q_0} and c_{q_1} according to

$$c_{q\_0}=\sum_{q\_i0,q\_j0}(e00_{q\_i0,q\_j0}\cdot a0_{q\_i0}\cdot b0_{q\_j0})+c_{q\_X}-r_{q\_Z}$$
$$c_{q\_1}=\sum_{q\_i1,q\_j1}(e11_{q\_i1,q\_j1}\cdot a1_{q\_i1}\cdot b1_{q\_j1})+c_{q\_Y}-r_{q\_X}\quad;$$

a party-Y first random number generation step (S4-1, S24-1) in which the party Y generates a number r_{q_Y} and transmits the number to the party Z;

a party-Y first computation step (S4-2, S24-2) in which the party Y computes the value c_{q_Y} according to

$$c_{q\_Y}=\sum_{q\_i1,q\_j2}(e12_{q\_i1,q\_j2}\cdot a1_{q\_i1}\cdot b2_{q\_j2})+\sum_{q\_i2,q\_j1}(e21_{q\_i2,q\_j1}\cdot a2_{q\_i2}\cdot b1_{q\_j1})+r_{q\_Y}$$

and transmits the value to the party X;
a party-Y second computation step (S5, S25) in which the party Y receives the number r_{q_X} from the party X and a value c_{q_Z} from the party Z, computes values c_{q_1} and c_{q_2} according to

$$c_{q\_1} = \sum_{q\_i1,q\_j1} (e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X}$$
$$c_{q\_2} = \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y} \quad ;$$

a party-Z first random number generation step (S6-1, S26-1) in which the party Z generates the number r_{q_Z} and transmits the number to the party X;
a party-Z first computation step (S6-2, S26-2) in which the party Z computes the value c_{q-Z} according to

$$c_{q\_Z} = \sum_{q\_i2,q\_j0} (e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j2} (e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0}) + r_{q\_Z}$$

and transmits the value to the party Y; and
a party-Z second computation step (S7, S27) in which the party Z receives the number r_{q_Y} from the party Y and the value c_{q_X} from the party X, computes the values c_{q_0} and c_{q_2} according to

$$c_{q\_0} = \sum_{q\_i0,q\_j0} (e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z}$$
$$c_{q\_2} = \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y} \quad .$$

5. The secure sum-of-product computation method according to claim 4, **characterized in that**
the parties X and Y previously sharing a number s_{q_Z}, the parties Y and Z previously sharing a number s_{q-X}, and the parties Z and X previously sharing a number s_{q_Y}, and
said secure sum-of-product computation method further comprising:

a party-X second random number generation step (S28) in which the party X generates a number sequence ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) and a number ρ_X and transmits the number sequence and the number to the party Y, and generates a number sequence ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) and transmits the number sequence to the party Z;
a party-X third computation step (S29) in which the party X computes a number sequence ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) and transmits the number sequence to the party Y, receives a number sequence ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) from the party Y and a number sequence ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) from the party Z, computes a number sequence ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-s_{q_Y}·$a1_{q\_na1-1}$) and a value

$$\gamma_X = \sum_{i0,j1,q} (e01_{q\_i0,q\_j1} \cdot \alpha X0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{i1,j0,q} (e10_{q\_i1,q\_j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \rho_X,$$

and transmits the number sequence and the value to the party Z;
a party-X fourth computation step (S30) in which the party X receives a number sequence ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-s_{q_Z}·$a2_{q\_na2-1}$) from the party Y and a value ρ_Z from the party Z, computes a value

$$\gamma'_Z = \sum_{i2,j0,q} \{e20_{q\_i2,q\_j0} \cdot (\alpha Z2_{q\_i2} - s_{q\_Z} \cdot a2_{q\_i2}) \cdot b0_{q\_j0} - s_{q\_Z} \cdot r_{q\_Z}\} + \rho_Z,$$

and transmits the value to the party Y;

a party-X misuse detection step (S31) in which the party X receives a value γ_Y from the party Y and a value γ'_Y and a number sequence ($\alpha Y2_{q\_0}$-s_{q_Y}.$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}.$a2_{q\_na2-1}$) from the party Z, computes

$$\sum_{i2,j1,q} \{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y,$$

ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and outputting the values c_{q_0} and c_{q_1} if the result of the computation is 0;

a party-Y second random number generation step (S32) in which the party Y generates a number sequence ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) and a number ρ_Y and transmits the number sequence and the number to the party Z, and generates the number sequence ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) and transmits the number sequence to the party X;

a party-Y third computation step (S33) in which the party Y computes a number sequence ($\alpha X1_{q\_0}$-s_{q_X}.$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}.$a1_{q\_na1-1}$) and transmits the number sequence to the party Z, receives the number sequence ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) from the party X and a number sequence ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) from the party Z, computes the number sequence ($\alpha Z2_{q\_0}$-s_{q_Z}.$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-s_{q_Z}.$a2_{q\_na2-1}$) and the value

$$\gamma_Y = \sum_{i1,j2,q} (e12_{q\_i1,q\_j2} \cdot \alpha Y1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{i2,j1,q} (e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \rho_Y,$$

and transmits the number sequence and the value to the party X;

a party-Y fourth computation step (S34) in which the party Y receives the number ρ_X from the party X and a number sequence ($\alpha X0_{q\_0}$-s_{q_X}.$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-s_{q_X}.$a0_{q\_na0-1}$) from the party Z, computes a value

$$\gamma'_X = \sum_{i0,j1,q} \{e01_{q\_i0,q\_j1} \cdot (\alpha X0_{q\_i0} - s_{q\_X} \cdot a0_{q\_i0}) \cdot b1_{q\_j1} - s_{q\_X} \cdot r_{q\_X}\} + \rho_X,$$

and transmits the value to the party Z;

a party-Y misuse detection step (S35) in which the party Y receives the value γ'_Z and the number sequence ($\alpha Z0_{q\_0}$-s_{q_Z}.$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}.$a0_{q\_na0-1}$) from the party X and a value γ_Z from the party Z, computes

$$\sum_{i0,j2,q} \{e02_{q\_i0,q\_j2} \cdot (\alpha Z0_{q\_i0} - s_{q\_Z} \cdot a0_{q\_i0}) \cdot b2_{q\_j2} + s_{q\_Z} \cdot c_{q\_Z}\} - \gamma_Z + \gamma'_Z,$$

ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and outputs the values c_{q_1} and c_{q_2} if the result of the computation is 0;

a party-Z second random number generation step (S36) in which the party Z generates the number sequence ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) and the number ρ_Z and transmits the number sequence and the number to the party X, and generates the number sequence ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) and transmits the number sequence to the party Y;

a party-Z third computation step (S37) in which the party Z computes the number sequence

($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$) and transmits the number sequence to the party X, receives the number sequence ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) from the party X and the number sequence ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) from the party Y, computes the number sequence ($\alpha X0_{q\_0}$-s_{q_X}·$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-s_{q_X}·$a0_{q\_na0-1}$) and the value

$$\gamma_Z = \sum_{i2,j0,q}(e20_{q\_i2,q\_j0} \cdot \alpha Z2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{i0,j2,q}(e02_{q\_i0,q\_j2} \cdot \alpha Z0_{q\_i0} \cdot b2_{q\_j2}) + \rho_Z,$$

and transmits the number sequence and the value to the party Y;
a party-Z fourth computation step (S38) in which the party Z receives the number sequence ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-s_{q_Y}·$a1_{q\_na1-1}$) from the party X and the number ρ_Y from the party Y, computes a value

$$\gamma'_Y = \sum_{i1,j2,q}\{e12_{q\_i1,q\_j2} \cdot (\alpha Y1_{q\_i1} - s_{q\_Y} \cdot a1_{q\_i1}) \cdot b2_{q\_j2} - s_{q\_Y} \cdot r_{q\_Y}\} + \rho_Y,$$

and transmits the value to the party X; and
a party-Z misuse detection step (S39) in which the party Z receives a value γ_X from the party X and a value γ'_X and the number sequence ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) from the party Y, computes

$$\sum_{i1,j0,q}\{e10_{q\_i1,q\_j0} \cdot (\alpha X1_{q\_i1} - s_{q\_X} \cdot a1_{q\_i1}) \cdot b0_{q\_j0} + s_{q\_X} \cdot c_{q\_X}\} - \gamma_X + \gamma'_X,$$

ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and outputs the values c_{q_2} and c_{q_0}) if the result of the computation is 0.

6. The secure sum-of-product computation method according to claim 4, **characterized in that**
the parties X and Y previously sharing a number s_{q_Z}, the parties Y and Z previously sharing a number s_{q_X}, and the parties Z and X previously sharing a number s_{q_Y}, and
said secure sum-of-product computation method further comprising:

a party-X second random number generation step (S68) in which the party X generates a number ρ_x and transmits the number to the party Y, and generates number sequences ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) and ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$) and transmits the number sequences to the party Z;
a party-X third computation step (S69) in which the party X computes number sequences ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) and ($\beta Z0_{q\_0}$-s_{q_Z}·$b0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$-s_{q_Z}·$b0_{q\_nb0-1}$) and transmits the number sequences to the party Y, receives number sequences ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) and ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$) from the party Y, computes a value

$$\gamma_X = \sum_{i1,j0,q}(e10_{i1,j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \sum_{i0,j1,q}(e01_{i0,j1} \cdot a0_{q\_i0} \cdot \beta X1_{q\_j1}) + \rho_X,$$

and transmits the value to the party Z;
a party-X fourth computation step (S70) in which the party X receives a value ρ_Z from the party Z, computes a value

$$\gamma'_Z = \sum_q (-s_{q\_z} \cdot r_{q\_z}) + \rho_Z,$$

and transmits the value to the party Y;

a party-X misuse detection step (S71) in which the party X receives a value γ_Y from the party Y and a value γ'_Y and number sequences ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$) and ($\beta Y2_{q\_0}$-s_{q_Y}·$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$-s_{q_Y}·$b2_{q\_nb2-1}$) from the party Z, computes

$$\sum_{i1,i2,j1,j2,q} \{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + e12_{q\_i1,q\_j2} \cdot (\beta Y2_{q\_j2} - s_{q\_Y} \cdot b2_{q\_j2}) \cdot a1_{q\_i1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y,$$

ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and outputting the values c_{q_0} and c_{q_1} if the result of the computation is 0;

a party-Y second random number generation step (S72) in which the party Y generates a number ρ_Y and transmits the number to the party Z, and generates the number sequences ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) and ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$) and transmits the number sequences to the party X;

a party-Y third computation step (S73) in which the party Y computes number sequences ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) and ($\beta X1_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-s_{q_X}·$b1_{q\_nb1-1}$) and transmits the number sequences to the party Z, receives number sequences ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) and ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) from the party Z, computes a value

$$\gamma_Y = \sum_{i2,j1,q} (e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \sum_{i1,j2,q} (e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot \beta Y2_{q\_j2}) + \rho_Y,$$

and transmits the value to the party X;

a party-Y fourth computation step (S74) in which the party Y receives the number ρ_X from the party X, computes a value

$$\gamma'_X = \sum_q (-s_{q\_x} \cdot r_{q\_x}) + \rho_X,$$

and transmits the value to the party Z;

a party-Y misuse detection step (S75) in which the party Y receives a value γ'_Z and the number sequences ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) and ($\beta Z0_{q\_0}$-s_{q_Z}·$b0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$-s_{q_Z}·$b0_{q\_nb0-1}$) from the party X and a value γ_Z from the party Z, computes

$$\sum_{i0,i2,j0,j2,q} \{e02_{q\_i0,q\_j2} \cdot (\alpha Z0_{q\_i0} - s_{q\_Z} \cdot a0_{q\_i0}) \cdot b2_{q\_j2} + e20_{q\_i2,q\_j0} \cdot (\beta Z0_{q\_j0} - s_{q\_Z} \cdot b0_{q\_j0}) \cdot a2_{q\_i2} + s_{q\_Z} \cdot c_{q\_Z}\} - \gamma_Z + \gamma'_Z,$$

ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0,

and outputs the values c_{q_1} and c_{q_2} if the result of the computation is 0;
a party-Z second random number generation step (S76) in which the party Z generates the number ρ_Z and transmits the number to the party X, and generates the number sequences ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) and ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) and transmits the number sequences to the party Y;
a party-Z third computation step (S77) in which the party Z computes the number sequences ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$) and ($\beta Y2_{q\_0}$-s_{q_Y}·$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$-s_{q_Y}·$b2_{q\_nb2-1}$) and transmits the number sequences to the party X, receives the number sequences ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) and ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$) from the party X, computes the value

$$\gamma_Z = \sum_{i0,j2,q}(e02_{q\_i0,q\_j2}\cdot\alpha Z0_{q\_i0}\cdot b2_{q\_j0}) + \sum_{i2,j0,q}(e20_{q\_i2,q\_j0}\cdot a2_{q\_i2}\cdot\beta Z0_{q\_j0}) + \rho_Z\ ,$$

and transmits the value to the party Y;
a party-Z fourth computation step (S78) in which the party Z receives the number ρ_Y from the party Y, computes a value

$$\gamma'_Y = \sum_{q}(-s_{q\_Y}\cdot r_{q\_Y}) + \rho_Y,$$

and transmits the value to the party X; and
a party-Z misuse detection step (S79) in which the party Z receives a value γ_X from the party X and a value γ'_X and the number sequences ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) and ($\beta X1_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-s_{q_X}·$b1_{q\_nb1-1}$) from the party Y, computes

$$\sum_{i0,i1,j0,j1,q}\{e10_{q\_i1,q\_j0}\cdot(\alpha X1_{q\_i1} - s_{q\_x}\cdot a1_{q\_i1})\cdot b0_{q\_j0}\} + e01_{q\_i0,q\_j1}\cdot(\beta X1_{q\_j1} - s_{q\_x}\cdot b1_{q\_j1})\cdot a0_{q\_i0} + s_{q\_x}\cdot c_{q\_x}\} - \gamma_X + \gamma'_X\ ,$$

ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and outputs the values c_{q_2} and c_{q_0} if the result of the computation is 0.

7. A secure sum-of-product computation method used for performing, in parallel, a total of m sets of sum-of-product computations of data strings A_{q_0} = ($a0_{q\_0}$, ..., $a0_{q\_na0-1}$) and A_{q_1} = ($a1_{q\_0}$, ..., $a1_{q\_na1-1}$) and B_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_nb0-1}$) and B_{q_1} = ($b1_{q\_0}$, ..., $b1_{q\_nb1-1}$) by cooperative computation by three computation apparatuses, which are a party X, a party Y and a party Z, the sum-of-product computations being expressed as

$$\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1}\cdot a0_{q\_i0}\cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0}\cdot a1_{q\_i1}\cdot b0_{q\_j0})$$

where q = 0, ..., m-1, m represents an integer equal to or greater than 1, na0, na1, nb0 and nb1 represent natural numbers, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, and j1 = 0, ..., nb1-1, and $e01_{q\_i0,q\_j1}$ and $e10_{q\_i1,q\_j0}$ represent any numbers, and the data strings A_{q_0}, A_{q_1}, B_{q_0} and B_{q_1} being input to the party X, the data strings A_{q_1} and B_{q_1} being input to the party Y, and the data strings A_{q_0} and B_{q_0}) being input to the party Z,
characterized in that the secure sum-of-product computation method comprising:

a party-X random number generation step (S102) in which the party X generates numbers c_{q_1} and γ_1 and number sequences ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_nb0-1}$) and ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_na0-1}$) and transmits the numbers and the number sequences to the party Y;
a party-Y random number generation step (S103) in which the party Y generates a number s_q and transmits the number to the party Z;
a party-X computation step (S104) in which the party X computes values c_{q_0} and γ_0 according to

$$c_{q\_0} = \sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) - c_{q\_1}$$

$$\gamma_0 = \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 1_{q\_i0} + b0_{q\_j0} \cdot \alpha 1_{q\_j0}) - \gamma_1$$

and transmits the values to the party Z;
a party-Y computation step (S105) in which the party Y receives the numbers c_{q_1} and γ_1 and the number sequences($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_nb0-1}$) and ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_na0-1}$) from the party X, computes number sequences ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) and ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) and a value γ' according to

$$\alpha 0_{q\_j0} = \sum_{q,q\_i1} s_q \cdot e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} - \alpha 1_{q\_j0}$$

$$\beta 0_{q\_i0} = \sum_{q,q\_j1} s_q \cdot e01_{q\_i0,q\_j1} \cdot b1_{q\_j1} - \beta 1_{q\_i0},$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

and transmits the number sequences and the value to the party Z; and
a misuse detection step (S106) in which the party Z receives the values c_{q_0} and γ_0 from the party X and the number s_q, the number sequences ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) and ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) and the value γ' from the party Y, computes

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma',$$

and ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0, wherein if the result of the computation in the misuse detection step is 0, the party X outputs the values c_{q_0} and c_{q_1}, the party Y outputs the value c_{q_1} and 0, and the party Z outputs 0 and the value c_{q_0}.

8. A secure sum-of-product computation method used for performing, in parallel, a total of m sets of sum-of-product computations of data a0 and a1 and data strings $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ and $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ by cooperative computation by three computation apparatuses, which are a party X, a party Y and a party Z, the sum-of-product computations being expressed as

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i}$$

where q = 0, ..., m-1, m represents an integer equal to or greater than 1, n represents a natural number, and i = 0, ..., n-1, and the data a0 and a1 and the data strings B_{q_0}) and B_{q_1} being input to the party X, the data a1 and the data string B_{q-1} being input to the party Y, and the data a0 and the data string B_{q_0}) being input to the party Z, **characterized in that** the secure sum-of-product computation method comprising:

a party-X random number generation step (S102) in which the party X generates numbers c_{q_1} and γ_1, a number sequence ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) and a number $\beta 1$ and transmits the numbers and the number sequence to the party Y;
a party-Y random number generation step (S103) in which the party Y generates a number s_q and transmits the number to the party Z;
a party-X computation step (S104) in which the party X computes values c_{q_0} and γ_0 according to

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

and transmits the values to the party Z;
a party-Y computation step (S 105) in which the party Y receives the numbers c_{q_1} and γ_1, the number sequence ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) and the numberβ 1 from the party X, computes a number sequence ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) and numbers $\beta 0$ and γ' according to

$$\alpha 0_{q\_i} = \sum_{q} s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1 \quad ,$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

and transmits the number sequence and the values to the party Z; and
a misuse detection step (S106) in which the party Z receives the values c_{q_0} and γ_0 from the party X and the number s_q, the number sequence ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) and the values $\beta 0$ and γ' from the party Y, computes

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma',$$

and ends the processing by outputting data indicating a misuse detection if the result of the computation is not 0,

wherein if the result of the computation in the misuse detection step is 0, the party X outputs the values c_{q_0} and c_{q_1}, the party Y outputs the value c_{q_1} and 0, and the party Z outputs 0 and the value c_{q_0}.

9. A secure sum-of-product computation system using three said computation apparatuses according to claim 1 as a party X, a party Y and a party Z.

10. A secure sum-of-product computation system using three said computation apparatuses according to claim 2 as a party X, a party Y and a party Z.

11. The secure sum-of-product computation system using three said computation apparatuses according to claim 3 as a party X, a party Y and a party Z.

12. A secure sum-of-product computation system used for performing, in parallel, a total of m sets of sum-of-product computations of data strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0\text{-}1})$ and $A_{q\_1} = (a1_{q\_0}, ..., a1_{q-na1\text{-}1})$ and $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0\text{-}1})$ and $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1\text{-}1})$ by cooperative computation by three computation apparatuses, which are a party X, a party Y and a party Z, the sum-of-product computations being expressed as

$$\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0})$$

where q = 0, ..., m-1, m represents an integer equal to or greater than 1, na0, na1, nb0 and nb1 represent natural numbers, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, and j1 = 0, ..., nb1-1, and $e01_{q\_i0,q\_j1}$ and $e10_{q\_i1,q\_j0}$ represent any numbers, and the data strings A_{q_0}, A_{q_1}, B_{q_0}) and B_{q_1} being input to the party X, the data strings A_{q_1} and B_{q_1} being input to the party Y, and the data strings A_{q_0} and B_{q_0} being _1input to the party Z,
characterized in that the party X comprises party-X random number generation means (901) and party-X computation means (903),
the party-X random number generation means (901) adapted to generate numbers c_{q_1} and γ_1 and number sequences $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_nb0\text{-}1})$ and $(\beta 1_{q\_0}, ..., \beta 1_{q\_na0\text{-}1})$ and transmit the numbers and the number sequences to the party Y,
the party-X computation means (903) adapted to compute values c_{q_0} and γ_0 according to

$$c_{q\_0} = \sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) - c_{q\_1}$$

$$\gamma_0 = \sum_{i0,j0,q}(a0_{q\_i0} \cdot \beta 1_{q\_i0} + b0_{q\_j0} \cdot \alpha 1_{q\_j0}) - \gamma_1$$

and transmit the values to the party Z,
the party Y comprises party-Y random number generation means (902) and party-Y computation means (904),
the party-Y random number generation means (902) adapted to generate a number s_q and transmit the number to the party Z,
the party-Y computation means (904) adapted to receive the numbers c_{q_1} and γ_1 and the number sequences$(\alpha 1_{q_0}, ..., \alpha 1_{q_nb0\text{-}1})$ and $(\beta 1_{q\_0}, ..., \beta 1_{q\_na0\text{-}1})$ from the party X, compute number sequences $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_nb0\text{-}1})$ and $(\beta 0_{q\_0}, ..., \beta 0_{q\_na0\text{-}1})$ and a value γ' according to

$$\alpha 0_{q\_j0} = \sum_{q,q\_i1} s_q \cdot e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} - \alpha 1_{q\_j0}$$

$$\beta 0_{q\_i0} = \sum_{q,q\_j1} s_q \cdot e01_{q\_i0,q\_j1} \cdot b1_{q\_j1} - \beta 1_{q\_i0},$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

and transmit the number sequences and the value to the party Z,
the party Z comprises misuse detection means (905) adapted to receive the values c_{q_0} and γ_0 from the party X and the number s_q, the number sequences ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) and ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) and the value γ' from the party Y, compute

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma',$$

and end the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and the party X outputs the values c_{q_0} and c_{q_1}, the party Y outputs the value c_{q_1} and 0, and the party Z outputs 0 and the value c_{q_0} if the result of the computation by the misuse detection means is 0.

13. A secure sum-of-product computation system used four performing, in parallel, a total of m sets of sum-of-product computations of data a0 and a1 and data strings B_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_nb0-1}$) and B_{q_1} = ($b1_{q\_0}$, ..., $b1_{q\_nb1-1}$) by cooperative computation by three computation apparatuses, which are a party X, a party Y and a party Z, the sum-of-product computations being expressed as

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i}$$

where q = 0, ..., m-1, m represents an integer equal to or greater than 1, n represents a natural number, and i = 0, ..., n-1, and the data a0 and a1 and the data strings B_{q_0} and B_{q_1} being input to the party X, the data a1 and the data string B_{q_1} being input to the party Y, and the data a0 and the data string B_{q_0}) being input to the party Z,
characterized in that the party X comprises party-X random number generation means (901) and party-X computation means (903),
the party-X random number generation means (901) adapted to generate numbers c_{q_1} and γ_1, a number sequence ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) and a number $\beta 1$ and transmit the numbers and the number sequence to the party Y,
the party-X computation means (903) adapted to compute values c_{q-0}) and γ_0 according to

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

and transmit the values to the party Z,
the party Y comprises party-Y random number generation means (902) and party-Y computation means (904),

the party-Y random number generation means (902) adapted to generate a number s_q and transmit the number to the party Z,
the party-Y computation means (904) adapted to receive the numbers c_{q_1} and γ_1, the number sequence ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) and the number $\beta 1$ from the party X, compute a number sequence ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) and numbers $\beta 0$ and γ' according to

$$\alpha 0_{q\_i} = \sum_q s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1 \quad ,$$

$$\gamma' = \sum_q s_q \cdot c_{q\_1} - \gamma_1$$

and transmit the number sequence and the values to the party Z,
the party Z comprises misuse detection means (905) adapted to receive the values c_{q_0} and γ_0 from the party X and the number s_q, the number sequence ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) and the values $\beta 0$ and γ' from the party Y, compute

$$\sum_q s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma',$$

and end the processing by outputting data indicating a misuse detection if the result of the computation is not 0, and the party X outputs the values c_{q_0} and c_{q_1}, the party Y outputs the value c_{q_1} and 0, and the party Z outputs 0 and the value c_{q_0} if the result of the computation by the misuse detection means is 0.

14. A program that makes a computer function as a computation apparatus according to any one of claims 1 to 3 or a secure sum-of-product computation system according to any one of claims 9 to 13.

Patentansprüche

1. Rechenvorrichtung, die bei der Ausführung einer Produktsummenberechnung durch drei Rechenvorrichtungen in Zusammenarbeit verwendet wird, wobei die drei Rechenvorrichtungen als eine Partei X, eine Partei Y und eine Partei Z dienen und symmetrische Verarbeitungen ausführen,
wobei unter der Voraussetzung, dass jede der Rechenvorrichtungen eine Partei P ist, angenommen wird, dass die Partei Z eine Partei P_- ist und die Partei Y eine Partei P_+ ist, und Indices 0p, 1p und 2p 0, 1 bzw. 2 sind, wenn die Partei P die Partei X ist, die Partei X die Partei P_- ist, die Partei Z die Partei P_+ ist, und die Indices 0p, 1p und 1p 1, 2 bzw. 0 sind, wenn die Partei P die Partei Y ist und die Partei Y die Partei P_- ist, die Partei X die Partei P_+ ist, und die Indices 0p, 1p und 2p 2, 0 bzw. 1 sind, wenn die Partei P die Partei Z ist,
m eine ganze Zahl gleich oder größer 1 darstellt, na0p, na1p, na2p, nb0p und nb1p natürliche Zahlen darstellen, q = 0, ..., m-1, i0p = 0, ..., na0p-1, i1p = 0, ..., na1p-1, i2p = 0, ..., na2p-1, j0p = 0, ..., nb0p-1, und j1p = 0, ..., nb1p-1, und $e0p1p_{i0p,j1p}$, $e1p0p_{i1p,j0p}$, $e0p0p_{i0p,j0p}$ und $e1p1p_{i1p,j1p}$ beliebige Zahlen darstellen,
dadurch gekennzeichnet, dass die Partei P umfasst:

eine erste Zufallszahlerzeugungseinrichtung (101, 301), die dafür ausgebildet ist, eine Zahl r_{q_P} zu erzeugen und die Zahl an die Partei P_+ zu senden;
eine erste Recheneinrichtung (102, 302), die dafür ausgebildet ist, Daten-Strings A_{q_0p} = ($a0p_{q\_0}$, ..., $a0p_{q\_na0p-1}$), A_{q_1p} = ($a1p_{q\_0}$,..., $a1p_{q\_na1p-1}$), $Bq_{\_0p}$ = ($b0p_{q\_0}$, ..., $b0p_{q\_nb0p-1}$) und B_{q_1p} = ($b1p_{q\_0}$, ...,

$b1p_{q\_nb1p-1}$) zu empfangen, einen Wert c_{q_P} gemäß

$$c_{q\_P} = \sum_{q\_i0p,q\_j1p} (e0p1p_{q\_i0p,q\_j1p} \cdot a0p_{q\_i0p} \cdot b1p_{q\_j1p}) \cdot$$
$$+ \sum_{q\_i1p,q\_j0p} (e1p0p_{q\_i1p,q\_j0p} \cdot a1p_{q\_i1p} \cdot b0p_{q\_j0p}) + r_{q\_P}$$

zu berechnen und den Wert an die Partei P_- zu senden: und
eine zweite Recheneinrichtung (103, 303), die dafür ausgebildet ist, eine Zahl r_{q_P-} von der Partei P_-, einen Wert c_{q_P+} von der Partei P_+ zu empfangen, Werte c_{q_0p} und c_{q_1p} gemäß

$$c_{q\_0p} = \sum_{q\_i0p,q\_j0p} (e0p0p_{q\_i0p,q\_j0p} \cdot a0p_{q\_i0p} \cdot b0p_{q\_j0p}) + c_{q\_P} - r_{q\_P-}$$
$$c_{q\_1p} = \sum_{q\_i1p,q\_j1p} (e1p1p_{q\_i1p,q\_j1p} \cdot a1p_{q\_i1p} \cdot b1p_{q\_j1p}) + c_{q\_P+} - r_{q\_P}$$

zu berechnen.

2. Rechenvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass**
die Parteien P_- und P zuvor eine Zahl s_{q_P+} teilen, die Parteien P und P_+ zuvor eine Zahl s_{q_P-} teilen und die Parteien P_+ und P_- zuvor eine Zahl s_{q_P} teilen, und
die Partei P ferner umfasst:

eine zweite Zufallszahlerzeugungseinrichtung (304), die dafür ausgebildet ist, eine Zahlenfolge ($\alpha P_+1p_{q\_0}$, ..., $\alpha P_{+1}p_{q\_na1p-1}$) und eine Zahl ρ_P zu erzeugen und die Zahlenfolge und die Zahl an die Partei P_+ zu senden und eine Zahlenfolge ($\alpha P\_0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$) zu erzeugen und die Zahlenfolge an die Partei P_- zu senden;
eine dritte Recheneinrichtung (305), die dafür ausgebildet ist, eine Zahlenfolge ($\alpha P\_0p_{q\_0}$-s_{q_P-}·$a0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$-s_{q_P-}·$a0p_{q\_na0p-1}$) zu berechnen und die Zahlenfolge an die Partei P_+ zu senden, eine Zahlenfolge ($\alpha P1p_{q\_0}$, ..., $\alpha P1p_{q\_nal\ p-1}$) von der Partei P_+ und eine Zahlenfolge ($\alpha P0_{pq\_0}$, ..., $\alpha P0p_{q\_na0p-1}$) von der Partei P- zu empfangen, eine Zahlenfolge ($\alpha P_+1p_{q\_0}$-s_{q_P+}·$a1p_{q\_0}$, ..., $\alpha P+1p_{q\_na1p-1}$-s_{q_P+}·$a1p_{q\_na1p-1}$) und einen Wert

$$\gamma_P = \sum_{i0p,j1p,q} (e0p1p_{i0p,j1p} \cdot \alpha P0p_{q\_i0p} \cdot b1p_{q\_j1p})$$
$$+ \sum_{i1p,j0p,q} (e1p0p_{i1p,j0p} \cdot \alpha P1p_{q\_i1p} \cdot b0p_{q\_j0p}) + \rho_P$$

zu berechnen und die Zahlenfolge und den Wert an die Partei P_- zu senden;
eine vierte Recheneinrichtung (306), die dafür ausgebildet ist, eine Zahlenfolge ($\alpha P\_2p_{q\_0}$-s_{q_P-}·$a2p_{q\_0}$, ..., $\alpha P\_2p_{q\_na2p-1}$-s_{q_P-}·$a2p_{q\_na2p-1}$) von der Partei P_+ und einen Wert ρ_{P-} von der Partei P_- zu empfangen, einen Wert γ'_{P-}

$$\gamma'_{P-} = \sum_{i2p,j0p,q} \{(\alpha P\_2p_{q\_i2p} - s_{q\_P-} \cdot a2p_{q\_i2p}) \cdot b0p_{q\_j0p} - s_{q\_P-} \cdot r_{q\_P-}\} + \rho_{P-}$$

zu berechnen und den Wert an die Partei P_+ zu senden; und
eine Missbrauchsdetektionseinrichtung (307), die dafür ausgebildet ist, einen Wert γ_{P+} von der Partei P_+ und einen Wert γ'_{P+} und eine Zahlenfolge ($\alpha P_+2p_{q\_0}$-s_{q_P+}·$a2p_{q\_0}$, ..., $\alpha P_+2p_{q\_na2p-1}$-s_{q_P+}·$a2p_{q\_na2p-1}$) von der Partei P_- zu empfangen,

$$\sum_{i2p,j1p,q}\left\{(\alpha P_+2p_{q\_i2p}-s_{q\_P+}\cdot a2p_{q\_i2p})\cdot b1p_{q\_j1p}+s_{q\_P+}\cdot c_{q\_P+}\right\}-\gamma_{P+}+\gamma'_{P+}$$

zu berechnen,
die Verarbeitung zu beenden durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und Werte c_{q_0p} und c_{q_1p} auszugeben, wenn das Ergebnis der Berechnung 0 ist.

3. Rechenvorrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass**
die Parteien P_- und P zuvor eine Zahl s_{q_P+} teilen, die Parteien P und P_+ zuvor eine Zahl s_{q_P-} teilen und die Parteien P_+ und P_- zuvor eine Zahl s_{q_P} teilen, und
die Partei P ferner umfasst:

eine zweite Zufallszahlerzeugungseinrichtung (604), die dafür ausgebildet ist, eine Zahl ρ_P zu erzeugen und die Zahl an die Partei P_+ zu senden und Zahlenfolgen (αP-$0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$) und ($\beta P\_0_{q\_0}$, ..., $\beta P\_0p_{q\_nb0p-1}$) zu erzeugen und die Zahlenfolgen an die Partei P_- zu senden;
eine dritte Recheneinrichtung (605), die dafür ausgebildet ist, Zahlenfolgen ($\alpha P\_0p_{q\_0}$-s_{q_P-}·$a0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$-s_{q_P-}·$a0p_{q\_na0p-1}$) und ($\beta P\_0p_{q\_0}$-s_{q_P-}·$b0_{pq\_0}$, ..., $\beta P\_0p_{q\_na0p-1}$-s_{q_P-}·$b0p_{q\_na0p-1}$) zu berechnen und die Zahlenfolgen an die Partei P_+ zu senden, Zahlenfolgen ($\alpha P1p_{q\_0}$, ..., $\alpha P1p_{q\_nalp-1}$) und ($\beta P1p_{q\_0}$, ..., $\beta P1p_{q\_nb1p-1}$) von der Partei P_+ zu empfangen, einen Wert

$$\gamma_P=\sum_{i1p,j0p,q}(e1p0p_{i1p,j0p}\cdot\alpha P1p_{q\_i1p}\cdot b0p_{q\_j0p})+\sum_{i0p,j1p,q}(e0p1p_{i0p,j1p}\cdot a0p_{q\_i0p}\cdot\beta P1p_{q\_j1p}+\rho_P$$

zu berechnen und den Wert an die Partei P_- zu senden;
eine vierte Recheneinrichtung (606), die dafür ausgebildet ist, einen Wert ρ_{P-} von der Partei P_- zu empfangen,

$$\gamma'_{P-}=\sum_q(-s_{q\_P-}\cdot r_{q\_P-})+\rho_{P-}$$

zu berechnen und den Wert an die Partei P_+ zu senden; und
eine Missbrauchsdetektionseinrichtung (607), die dafür ausgebildet ist, einen Wert γ_{P+} von der Partei P_+ und einen Wert γ'_{P+} und Zahlenfolgen ($\alpha P_+2p_{q\_0}$-s_{q_P+}·$a2p_{q\_0}$, ..., $\alpha P_+2p_{q\_na2p-1}$-s_{q_P+}·$a2_{p\_na2p-1}$) und ($\beta P_+2_{q\_0}$-s_{q_P+}·$b2p_{q\_0}$, ..., $\beta P+2p_{q\_na2p-1}$-s_{q_P+}·$b2p_{q\_na2p-1}$) von der Partei P_- zu empfangen,

$$\sum_{i1p,i2p,j1p,j2p,q}\left\{(\alpha P_+2p_{q\_i2p}-s_{q\_P+}\cdot a2p_{q\_i2p})\cdot b1p_{q\_j1p}+(\beta P_+2p_{q\_j2p}-s_{q\_P+}\cdot b2p_{q\_j2p})\cdot a1p_{q\_i1p}+s_{q\_P+}\cdot c_{q\_P+}\right\}-\gamma_{P+}+\gamma'_{P+}$$

zu berechnen, die Verarbeitung zu beenden durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und Werte c_{q_0p} und c_{q_1p} auszugeben, wenn das Ergebnis der

Berechnung 0 ist.

4. Sicheres Produktsummenberechnungsverfahren, das zur parallelen Ausführung einer Gesamtmenge von m Sätzen von Produktsummenberechnungen von Daten-Strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0\text{-}1})$, $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_na1\text{-}1})$ und $A_{q\_2} = (a2_{q\_0}, ..., a2_{q\_na2\text{-}1})$ und $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0\text{-}1})$, $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1\text{-}1})$ und $B_{q\_2} = (b2_{q\_0}, ..., b2_{q\_nb2\text{-}1})$ durch gemeinsame Berechnung durch drei Rechenvorrichtungen verwendet wird, die eine Partei X, eine Partei Y und eine Partei Z sind, wobei die Produktsummenberechnungen ausgedrückt werden als

$$\begin{aligned}
&\sum_{q_i0,q_j0}(e00_{q_i0,q_j0} \cdot a0_{q_i0} \cdot b0_{q_j0}) + \sum_{q_i0,q_j1}(e01_{q_i0,q_j1} \cdot a0_{q_i0} \cdot b1_{q_j1}) \\
&+ \sum_{q_i1,q_j0}(e10_{q_i1,q_j0} \cdot a1_{q_i1} \cdot b0_{q_j0}) + \sum_{q_i1,q_j1}(e11_{q_i1,q_j1} \cdot a1_{q_i1} \cdot b1_{q_j1}) \\
&+ \sum_{q_i1,q_j2}(e12_{q_i1,q_j2} \cdot a1_{q_i1} \cdot b2_{q_j2}) + \sum_{q_i2,q_j1}(e21_{q_i2,q_j1} \cdot a2_{q_i2} \cdot b1_{q_j1}) \\
&+ \sum_{q_i2,q_j2}(e22_{q_i2,q_j2} \cdot a2_{q_i2} \cdot b2_{q_j2}) + \sum_{q_i2,q_j0}(e20_{q_i2,q_j0} \cdot a2_{q_i2} \cdot b0_{q_j0}) \\
&+ \sum_{q_i0,q_j2}(e02_{q_i0,q_j2} \cdot a2_{q_i2} \cdot b0_{q_i0})
\end{aligned},$$

wobei q = 0, ..., m-1, m eine ganze Zahl gleich oder größer 1 darstellt, na0, na1, na2, nb0, nb1 und nb2 natürliche Zahlen darstellen, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, i2 = 0, ..., na2-1, j0 = 0, ..., nb0-1, j1 = 0, ..., nb1-1, und j2 = 0, ..., nb2-1, und $e01_{q\_i0,q\_j1}$, $e10_{q\_i1,q\_j0}$, $e00_{q\_i0,q\_j0}$, $e11_{q\_i1,q\_j1}$, $e12_{q\_i1,q\_j2}$, $e21_{q\_i2,q\_j1}$, $e22_{q\_i2,q\_j2}$, $e20_{q\_i2,q\_j0}$ und $e02_{q\_i0,q\_j2}$ beliebige Zahlen darstellen, und die Daten-Strings A_{q_0}, A_{q_1}, B_{q_0} und B_{q_1} in die Partei X eingegeben werden, die Daten-Strings A_{q_1}, A_{q_2}, B_{q_1} und B_{q_2} in die Partei Y eingegeben werden und die Daten-Strings A_{q_2}, A_{q_0}, B_{q_2} und B_{q_0} in die Partei Z eingegeben werden,
dadurch gekennzeichnet, dass das sichere Produktsummenberechnungsverfahren umfasst:

einen Partei-X ersten Zufallszahlerzeugungsschritt (S2-1, S22-1), in dem die Partei X eine Zahl r_{q_X} erzeugt und die Zahl an die Partei Y sendet;
einen Partei-X ersten Berechnungsschritt (S2-2, S22-2), in dem die Partei X einen Wert c_{q_x} gemäß

$$c_{q\_X} = \sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) + r_{q\_X}$$

berechnet und den Wert an die Partei Z sendet;
einen Partei-X zweiten Berechnungsschritt (S3, S23), in dem die Partei X eine Zahl r_{q_Z} von der Partei Z und einen Wert c_{q_Y} von der Partei Y empfängt, Werte c_{q_0} und c_{q_1} gemäß

$$c_{q\_0} = \sum_{q\_i0,q\_j0}(e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z}$$

$$c_{q\_1} = \sum_{q\_i1,q\_j1}(e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X}$$

berechnet;
einen Partei-Y ersten Zufallszahlerzeugungsschritt (S4-1, S24-1), in dem die Partei Y eine Zahl r_{q_Y} erzeugt und die Zahl an die Partei Z sendet;
einen Partei-Y ersten Berechnungsschritt (S4-2, S24-2), in dem die Partei Y den Wert c_{q_Y} gemäß

$$c_{q\_Y} = \sum_{q\_i1,q\_j2}(e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j1}(e21_{q\_i2,q\_j1} \cdot a2_{q\_i2} \cdot b1_{q\_j1}) + r_{q\_Y}$$

berechnet und den Wert an die Partei X sendet;
einen Partei-Y zweiten Berechnungsschritt (S5, S25), in dem die Partei Y die Zahl r_{q_X} von der Partei X und einen Wert c_{q-Z} von der Partei Z empfängt, Werte c_{q_1} und c_{q_2} gemäß

$$c_{q\_1} = \sum_{q\_i1,q\_j1}(e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X}$$
$$c_{q\_2} = \sum_{q\_i2,q\_j2}(e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y}$$

berechnet;
einen Partei-Z ersten Zufallszahlerzeugungsschritt (S6-1, S26-1), in dem die Partei Z die Zahl r_{q_Z} erzeugt und die Zahl an die Partei X sendet;
einen Partei-Z ersten Berechnungsschritt (S6-2, S26-2), in dem die Partei Z den Wert c_{q_Z} gemäß

$$c_{q\_Z} = \sum_{q\_i2,q\_j0}(e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j2}(e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0}) + r_{q\_Z}$$

berechnet und den Wert an die Partei Y sendet; und
einen Partei-Z zweiten Berechnungsschritt (S7, S27), in dem die Partei Z die Zahl r_{q_Y} von der Partei Y und den Wert c_{q_X} von der Partei X empfängt, die Werte c_{q_0} und c_{q_2} gemäß

$$c_{q\_0} = \sum_{q\_i0,q\_j0}(e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z}$$
$$c_{q\_2} = \sum_{q\_i2,q\_j2}(e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y}$$

berechnet.

5. Sicheres Produktsummenberechnungsverfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** die Parteien X und Y zuvor eine Zahl s_{q_Z} teilen, die Parteien Y und Z zuvor eine Zahl s_{q_X} teilen und die Parteien Z und X zuvor eine Zahl s_{q_Y} teilen, und
das sichere Produktsummenberechnungsverfahren ferner umfasst:

einen Partei-X zweiten Zufallszahlerzeugungsschritt (S28), in dem die Partei X eine Zahlenfolge ($\alpha Y1_{q\_0}$), ..., $\alpha Y1_{q\_na1-1}$) und eine Zahl ρ_x erzeugt und die Zahlenfolge und die Zahl an die Partei Y sendet und eine Zahlenfolge ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) erzeugt und die Zahlenfolge an die Partei Z sendet;

einen Partei-X dritten Berechnungsschritt (S29), in dem die Partei X eine Zahlenfolge ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) berechnet und die Zahlenfolge an die Partei Y sendet, eine Zahlenfolge ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) von der Partei Y und eine Zahlenfolge ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) von der Partei Z empfängt, eine Zahlenfolge ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-s_{q_Y}·$a1_{q\_na1-1}$) und einen Wert

$$\gamma_X = \sum_{i0,j1,q}(e01_{q\_i0,q\_j1} \cdot \alpha X0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{i1,j0,q}(e10_{q\_i1,q\_j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \rho_X$$

berechnet und die Zahlenfolge und den Wert an die Partei Z sendet;
einen Partei-X vierten Berechnungsschritt (S30), in dem die Partei X eine Zahlenfolge ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-S_{q_Z}·$a2_{q\_na2-1}$) von der Partei Y und einen Wert ρ_z von der Partei Z empfängt, einen Wert

$$\gamma'_Z = \sum_{i2,j0,q}\{e20_{q\_i2,q\_j0} \cdot (\alpha Z2_{q\_i2} - s_{q\_Z} \cdot a2_{q\_i2}) \cdot b0_{q\_j0} - s_{q\_Z} \cdot r_{q\_Z}\} + \rho_Z$$

berechnet und den Wert an die Partei Y sendet;
einen Partei-X Missbrauchsdetektionsschritt (S31), in dem die Partei X einen Wert γ_Y von der Partei Y und einen Wert γ'_Y und eine Zahlenfolge ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-S_{q_Y}·$a2_{q\_na2-1}$) von der Partei Z empfängt,

$$\sum_{i2,j1,q}\{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y$$

berechnet, die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und die Werte c_{q_0} und c_{q_1} ausgibt, wenn das Ergebnis der Berechnung 0 ist;
einen Partei-Y zweiten Zufallszahlerzeugungsschritt (S32), in dem die Partei Y eine Zahlenfolge ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) und eine Zahl ρ_Y erzeugt und die Zahlenfolge und die Zahl an die Partei Z sendet und die Zahlenfolge ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) erzeugt und die Zahlenfolge an die Partei X sendet;
einen Partei-Y dritten Berechnungsschritt (S33), in dem die Partei Y eine Zahlenfolge ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) berechnet und die Zahlenfolge an die Partei Z sendet, die Zahlenfolge ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) von der Partei X und eine Zahlenfolge ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) von der Partei Z empfängt, die Zahlenfolge ($\alpha Z2_{q\_0}$-s_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-s_{q_Z}·$a2_{q\_na2-1}$) und den Wert

$$\gamma_Y = \sum_{i1,j2,q}(e12_{q\_i1,q\_j2} \cdot \alpha Y1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{i2,j1,q}(e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \rho_Y$$

berechnet und die Zahlenfolge und den Wert an die Partei X sendet;
einen Partei-Y vierten Berechnungsschritt (S34), in dem die Partei Y die Zahl ρ_X von der Partei X und eine Zahlenfolge ($\alpha X0_{q\_0}$-$s_{q\text{-}X}$·$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-s_{q_X}·$a0_{q\_na0-1}$) von der Partei Z empfängt, einen Wert

$$\gamma'_X = \sum_{i0,j1,q}\{e01_{q\_i0,q\_j1} \cdot (\alpha X0_{q\_i0} - s_{q\_X} \cdot a0_{q\_i0}) \cdot b1_{q\_j1} - s_{q\_X} \cdot r_{q\_X}\} + \rho_X$$

berechnet und den Wert an die Partei Z sendet;

einen Partei-Y Missbrauchsdetektionsschritt (S35), in dem die Partei Y den Wert γ'_Z und die Zahlenfolge ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) von der Partei X und einen Wert γ_Z von der Partei Z empfängt,

$$\sum_{i0,j2,q}\left\{e02_{q\_i0,q\_j2}\cdot(\alpha Z0_{q\_i0}-s_{q\_Z}\cdot a0_{q\_i0})\cdot b2_{q\_j2}+s_{q\_Z}\cdot c_{q\_Z}\right\}-\gamma_Z+\gamma'_Z$$

berechnet, die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und die Werte c_{q_1} und c_{q_2} ausgibt, wenn das Ergebnis der Berechnung 0 ist;
einen Partei-Z zweiten Zufallszahlerzeugungsschritt (S36), in dem die Partei Z die Zahlenfolge ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) und die Zahl ρ_Z erzeugt und die Zahlenfolge und die Zahl an die Partei X sendet, und die Zahlenfolge ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) erzeugt und die Zahlenfolge an die Partei Y sendet;
einen Partei-Z dritten Berechnungsschritt (S37), in dem die Partei Z die Zahlenfolge ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-$s_{q\text{-}Y}$·$a2_{q\_na2-1}$) berechnet und die Zahlenfolge an die Partei X sendet, die Zahlenfolge ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) von der Partei X und die Zahlenfolge ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) von der Partei Y empfängt, die Zahlenfolge ($\alpha X0_{q\_0}$-s_{q_X}.$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-s_{q_X}·$a0_{q\_na0-1}$) und den Wert

$$\gamma_Z=\sum_{i2,j0,q}(e20_{q\_i2,q\_j0}\cdot\alpha Z2_{q\_i2}\cdot b0_{q\_j0})+\sum_{i0,j2,q}(e02_{q\_i0,q\_j2}\cdot\alpha Z0_{q\_i0}\cdot b2_{q\_j2})+\rho_Z$$

berechnet und die Zahlenfolge und den Wert an die Partei Y sendet;
einen Partei-Z vierten Berechnungsschritt (S38), in dem die Partei Z die Zahlenfolge ($\alpha Y1_{q\_0}$-s_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-s_{q_Y}·$a1_{q\_na1-1}$) von der Partei X und die Zahl ρ_Y von der Partei Y empfängt, einen Wert

$$\gamma'_Y=\sum_{i1,j2,q}\left\{e12_{q\_i1,q\_j2}\cdot(\alpha Y1_{q\_i1}-s_{q\_Y}\cdot a1_{q\_i1})\cdot b2_{q\_j2}-s_{q\_Y}\cdot r_{q\_Y}\right\}+\rho_Y$$

berechnet und den Wert an die Partei X sendet; und
einen Partei-Z Missbrauchsdetektionsschritt (S39), in dem die Partei Z einen Wert γ_X von der Partei X und einen Wert γ'_X und die Zahlenfolge ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}s_{q\_X}$·$a1_{q\_na1-1}$) von der Partei Y empfängt,

$$\sum_{i1,j0,q}\left\{e10_{q\_i1,q\_j0}\cdot(\alpha X1_{q\_i1}-s_{q\_X}\cdot a1_{q\_i1})\cdot b0_{q\_j0}+s_{q\_X}\cdot c_{q\_X}\right\}-\gamma_X+\gamma'_X$$

berechnet, die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und die Werte c_{q_2} und c_{q_0} ausgibt, wenn das Ergebnis der Berechnung 0 ist.

6. Sicheres Produktsummenberechnungsverfahren nach Anspruch 4, **dadurch gekennzeichnet, dass**
die Parteien X und Y zuvor eine Zahl s_{q_Z} teilen, die Parteien Y und Z zuvor eine Zahl s_{q-X} teilen und die Parteien Z und X zuvor eine Zahl s_{q_Y} teilen und
das sichere Produktsummenberechnungsverfahren ferner beinhaltet:

einen Partei-X zweiten Zufallszahlerzeugungsschritt (S68), in dem die Partei X eine Zahl ρ_X erzeugt und die Zahl an die Partei Y sendet und Zahlenfolgen ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) und ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$) erzeugt und die Zahlenfolgen an die Partei Z sendet;

einen Partei-X dritten Berechnungsschritt (S69), in dem die Partei X Zahlenfolgen ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) und ($\beta Z0_{q\_0}$-s_{q_Z}·b_{q_0}, ..., $\beta Z0_{q\_nb0-1}$-s_{q_Z}·$b0_{q\_nb0-1}$) berechnet und die Zahlenfolgen an die Partei Y sendet, Zahlenfolgen ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) und ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$) von der Partei Y empfängt, einen Wert

$$\gamma_X = \sum_{i1,j0,q}(e10_{i1,j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \sum_{i0,j1,q}(e01_{i0,j1} \cdot a0_{q\_i0} \cdot \beta X1_{q\_j1}) + \rho_X$$

berechnet und den Wert an die Partei Z sendet;
einen Partei-X vierten Berechnungsschritt (S70), in dem die Partei X einen Wert ρ_Z von der Partei Z empfängt, einen Wert

$$\gamma'_Z = \sum_{q}(-s_{q\_Z} \cdot r_{q\_Z}) + \rho_Z$$

berechnet und den Wert an die Partei Y sendet;
einen Partei-X Missbrauchsdetektionsschritt (S71), in dem die Partei X einen Wert γ_Y von der Partei Y und einen Wert γ'_Y und Zahlenfolgen ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-s_{q_Y}·$a2_{q\_na2-1}$) und ($\beta Y2_{q\_0}$-s_{q_Y}·$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$-s_{q_Y}·$b2_{q\_nb2-1}$) von der Partei Z empfängt,

$$\sum_{i1,i2,j1,j2,q}\{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + e12_{q\_i1,q\_j2} \cdot (\beta Y2_{q\_j2} - s_{q\_Y} \cdot b2_{q\_j2}) \cdot a1_{q\_i1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y$$

berechnet, die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und die Werte c_{q_0} und c_{q_1} ausgibt, wenn das Ergebnis der Berechnung 0 ist;
einen Partei-Y zweiten Zufallszahlerzeugungsschritt (S72), in dem die Partei Y eine Zahl ρ_Y erzeugt und die Zahl an die Partei Z sendet und die Zahlenfolgen ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) und ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$) erzeugt und die Zahlenfolgen an die Partei X sendet;
einen Partei-Y dritten Berechnungsschritt (S73), in dem die Partei Y Zahlenfolgen ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) und ($\beta X1_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-s_{q_X}·$b1_{q\_nb1-1}$) berechnet und die Zahlenfolgen an die Partei Z sendet, Zahlenfolgen ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) und ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) von der Partei Z empfängt, einen Wert

$$\gamma_Y = \sum_{i2,j1,q}(e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \sum_{i1,j2,q}(e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot \beta Y2_{q\_j2}) + \rho_Y$$

berechnet und den Wert an die Partei X sendet;
einen Partei-Y vierten Berechnungsschritt (S74), in dem die Partei Y die Zahl ρ_X von der Partei X empfängt, einen Wert

$$\gamma'_X = \sum_q (-s_{q\_X} \cdot r_{q\_X}) + \rho_X$$

berechnet und den Wert an die Partei Z sendet;
einen Partei-Y Missbrauchsdetektionsschritt (S75), in dem die Partei Y einen Wert γ'_Z und die Zahlenfolgen ($\alpha Z0_{q\_0}$-s_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-s_{q_Z}·$a0_{q\_na0-1}$) und ($\beta Z0_{q\_0}$-s_{q_Z}·$b0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$-s_{q_Z}·$b0_{q\_nb0-1}$) von der Partei X und einen Wert γ_Z von der Partei Z empfängt,

$$\sum_{i0,i2,j0,j2,q} \{e02_{q\_i0,q\_j2} \cdot (\alpha Z0_{q\_i0} - s_{q\_Z} \cdot a0_{q\_i0}) \cdot b2_{q\_j2} + e20_{q\_i2,q\_j0} \cdot (\beta Z0_{q\_j0} - s_{q\_Z} \cdot b0_{q\_j0}) \cdot a2_{q\_i2} + s_{q\_Z} \cdot c_{q\_Z}\} - \gamma_Z + \gamma'_Z$$

berechnet, die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und die Werte c_{q_1} und c_{q_2} ausgibt, wenn das Ergebnis der Berechnung 0 ist;
einen Partei-Z zweiten Zufallszahlerzeugungsschritt (S76), in dem die Partei Z die Zahl ρ_Z erzeugt und die Zahl an die Partei X sendet und die Zahlenfolgen ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) und ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) erzeugt und die Zahlenfolgen an die Partei Y sendet;
einen Partei-Z dritten Berechnungsschritt (S77), in dem die Partei Z die Zahlenfolgen ($\alpha Y2_{q\_0}$-s_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q_na2-1}$$s_{q_Y}$·$a2_{q_na2-1}$) und ($\beta Y2_{q_0}$-$s_{q_Y}$·$b2_{q_0}$, ..., $\beta Y2_{q\_nb2-1}$-s_{q_Y}·$b2_{q\_nb2-1}$) berechnet und die Zahlenfolgen an die Partei X sendet, die Zahlenfolgen ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) und ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$) von der Partei X empfängt, den Wert

$$\gamma_Z = \sum_{i0,j2,q} (e02_{q\_i0,q\_j2} \cdot \alpha Z0_{q\_i0} \cdot b2_{q\_j0}) + \sum_{i2,j0,q} (e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot \beta Z0_{q\_j0}) + \rho_Z$$

berechnet und den Wert an die Partei Y sendet;
einen Partei-Z vierten Berechnungsschritt (S78), in dem die Partei Z die Zahl ρ_Y von der Partei Y empfängt, einen Wert

$$\gamma'_Y = \sum_q (-s_{q\_Y} \cdot r_{q\_Y}) + \rho_Y$$

berechnet und den Wert an die Partei X sendet; und
einen Partei-Z Missbrauchsdetektionsschritt (S79), in dem die Partei Z einen Wert γ_X von der Partei X und einen Wert γ'_X und die Zahlenfolgen ($\alpha X1_{q\_0}$-s_{q_X}·$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-s_{q_X}·$a1_{q\_na1-1}$) und ($\beta X1_{q\_0}$-s_{q_X}·$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-s_{q_X}·$b1_{q\_nb1-1}$) von der Partei Y empfängt,

$$\sum_{i0,i1,j0,j1,q} \{e10_{q\_i1,q\_j0} \cdot (\alpha X1_{q\_i1} - s_{q\_X} \cdot a1_{q\_i1}) \cdot b0_{q\_j0}\} + e01_{q\_i0,q\_j1} \cdot (\beta X1_{q\_j1} - s_{q\_X} \cdot b1_{q\_j1}) \cdot a0_{q\_i0} + s_{q\_X} \cdot c_{q\_X}\} - \gamma_X + \gamma'_X$$

berechnet, die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und die Werte c_{q_2} und c_{q_0} ausgibt, wenn das Ergebnis der Berechnung 0 ist.

7. Sicheres Produktsummenberechnungsverfahren, das zur parallelen Ausführung einer Gesamtmenge von m Sätzen von Produktsummenberechnungen von Daten-Strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0-1})$ und $A_{q\_1}, = (a1_{q\_0}, ..., a1_{q\_na1-1})$ und $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ und $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ durch gemeinsame Berechnung durch drei Rechenvorrichtungen verwendet wird, die eine Partei X, eine Partei Y und eine Partei Z sind, wobei die Produktsummenberechnungen ausgedrückt werden als

$$\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}),$$

wobei q = 0, ..., m-1, m eine ganze Zahl gleich oder größer 1 darstellt, na0, na1, nb0 und nb1 natürliche Zahlen darstellen, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, und j1 = 0, ..., nb1-1, und $e01_{q\_i0,q\_j1}$ und $e10_{q\_i1,q\_j0}$ jegliche Zahlen darstellen, und die Daten-Strings $A_{q\_}0$, A_{q_1}, B_{q_0} und B_{q_1} in die Partei X eingegeben werden, die Daten-Strings A_{q_1} und B_{q_1} in die Partei Y eingegeben werden und die Daten-Strings A_{q_0} und B_{q_0} in die Partei Z eingegeben werden,
dadurch gekennzeichnet, dass das sichere Produktsummenberechnungsverfahren umfasst:

einen Partei-X Zufallszahlerzeugungsschritt (S 102), in dem die Partei X Zahlen c_{q_1} und γ_1 und Zahlenfolgen $(\alpha 1_{q\_0}), ..., \alpha 1_{q\_nb0-1})$ und $(\beta 1_{q\_0}, ..., \beta 1_{q\_na0-1})$ erzeugt und die Zahlen und die Zahlenfolgen an die Partei Y sendet;
einen Partei-Y Zufallszahlerzeugungsschritt (S103), in dem die Partei Y eine Zahl s_q erzeugt und die Zahl an die Partei Z sendet;
einen Partei-X Berechnungsschritt (S 104), in dem die Partei X Werte c_{q_0} und γ_0 gemäß

$$c_{q\_0} = \sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) - c_{q\_1}$$

$$\gamma_0 = \sum_{i0,j0,q}(a0_{q\_i0} \cdot \beta 1_{q\_i0} + b0_{q\_j0} \cdot \alpha 1_{q\_j0}) - \gamma_1$$

berechnet und die Werte an die Partei Z sendet;
einen Partei-Y Berechnungsschritt (S 105), in dem die Partei Y die Zahlen c_{q_1} und γ_1 und die Zahlenfolgen $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_nb0-1})$ und $(\beta 1_{q\_0}, ..., \beta 1_{q\_na0-1})$ von der Partei X empfängt, Zahlenfolgen $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_nb0-1})$ und $(\beta 0_{q\_0}, ..., \beta 0_{q\_na0-1})$ und einen Wert γ' gemäß

$$\alpha 0_{q\_j0} = \sum_{q, q\_i1} s_q \cdot e10_{q\_i1, q\_j0} \cdot a1_{q\_i1} - \alpha 1_{q\_j0}$$

$$\beta 0_{q\_i0} = \sum_{q, q\_j1} s_q \cdot e01_{q\_i0, q\_j1} \cdot b1_{q\_j1} - \beta 1_{q\_i0}$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

berechnet und die Zahlenfolgen und den Wert an die Partei Z sendet; und

einen Missbrauchsdetektionsschritt (S106), in dem die Partei Z die Werte c_{q_0} und γ_0 von der Partei X und die Zahl s_q, die Zahlenfolgen ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) und ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) und den Wert γ' von der Partei Y empfängt,

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma'$$

berechnet und die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist,
wobei, wenn das Ergebnis der Berechnung in dem Missbrauchsdetektionsschritt 0 ist, die Partei X die Werte c_{q_0} und c_{q_1} ausgibt, die Partei Y die Werte c_{q_1} und 0 ausgibt und die Partei Z 0 und den Wert c_{q_0} ausgibt.

8. Sicheres Produktsummenberechnungsverfahren, das zur parallelen Ausführung einer Gesamtmenge von m Sätzen von Produktsummenberechnungen von Daten a0 und a1 und Daten-Strings B_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_nb0-1}$) und B_{q_1} = ($b1_{q\_0}$, ..., $b1_{q\_nb1-1}$) durch gemeinsame Berechnung durch drei Rechenvorrichtungen verwendet wird, die eine Partei X, eine Partei Y und eine Partei Z sind, wobei die Produktsummenberechnungen ausgedrückt werden als

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i},$$

wobei q = 0, ..., m-1, m eine ganze Zahl gleich oder größer 1 darstellt, n eine natürliche Zahl darstellt, und i = 0, ..., n-1, und die Daten a0 und a1 und die Daten-Strings B_{q_0} und B_{q_1} in die Partei X eingegeben werden, die Daten a1 und der Daten-String B_{q_1} in die Partei Y eingegeben werden und die Daten a0 und der Daten-String B_{q_0} in die Partei Z eingegeben werden,
dadurch gekennzeichnet, dass das sichere Produktsummenberechnungsverfahren umfasst:

einen Partei-X Zufallszahlerzeugungsschritt (S 102), in dem die Partei X Zahlen c_{q_1}, und γ_1, eine Zahlenfolge ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) und eine Zahl $\beta 1$ erzeugt und die Zahlen und die Zahlenfolge an die Partei Y sendet;
einen Partei-Y Zufallszahlerzeugungsschritt (S103), in dem die Partei Y eine Zahl s_q erzeugt und die Zahl an die Partei Z sendet;
einen Partei-X Berechnungsschritt (S104), in dem die Partei X Werte c_{q_0} und γ_0 gemäß

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

berechnet und die Werte an die Partei Z sendet;
einen Partei-Y Berechnungsschritt (S 105), in dem die Partei Y die Zahlen c_{q_1} und γ_1, die Zahlenfolge ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) und die Zahl $\beta 1$ von der Partei X empfängt, eine Zahlenfolge ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) und Zahlen $\beta 0$ und γ' gemäß

$$\alpha 0_{q\_i} = \sum_{q} s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

berechnet und die Zahlenfolge und die Werte an die Partei Z sendet; und

einen Missbrauchsdetektionsschritt (S 106), in dem die Partei Z die Werte c_{q_0} und γ_0 von der Partei X und die Zahl s_q, die Zahlenfolge ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) und die Werte $\beta 0$ und γ' von der Partei Y empfängt,

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma'$$

berechnet und die Verarbeitung beendet durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist,

wobei, wenn das Ergebnis der Berechnung in dem Missbrauchsdetektionsschritt 0 ist, die Partei X die Werte c_{q_0} und c_{q_1} ausgibt, die Partei Y den Wert c_{q_1} und 0 ausgibt, und die Partei Z 0 und den Wert c_{q_0} ausgibt.

9. Sicheres Produktsummenberechnungssystem, das die drei Rechenvorrichtungen nach Anspruch 1 als eine Partei X, eine Partei Y und eine Partei Z verwendet.

10. Sicheres Produktsummenberechnungssystem, das die drei Rechenvorrichtungen nach Anspruch 2 als eine Partei X, eine Partei Y und eine Partei Z verwendet.

11. Sicheres Produktsummenberechnungssystem, das die drei Rechenvorrichtungen nach Anspruch 3 als eine Partei X, eine Partei Y und eine Partei Z verwendet.

12. Sicheres Produktsummenberechnungssystem, das zur parallelen Ausführung einer Gesamtmenge von m Sätzen von Produktsummenberechnungen von Daten-Strings $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0-1})$ und $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_na1-1})$ und $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ und $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ durch gemeinsame Berechnung durch drei Rechenvorrichtungen verwendet wird, die eine Partei X, eine Partei Y und eine Partei Z sind, wobei die Produktsummenberechnungen ausgedrückt werden als

$$\sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}),$$

wobei q = 0, ..., m-1, m eine ganze Zahl gleich oder größer 1 darstellt, na0, na1, nb0 und nb1 natürliche Zahlen darstellen, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb1-1, und j1 = 0, ..., nb1-1, und $e01_{q\_i0,q\_j1}$ und $e10_{q\_i1,q\_j0}$ beliebige Zahlen darstellen und die Daten-Strings A_{q_0}, A_{q_1}, B_{q_0} und B_{q_1} in die Partei X eingegeben werden, die Daten-Strings A_{q_1} und B_{q_1} in die Partei Y eingegeben werden und die Daten-Strings A_{q_0} und B_{q_0} in die Partei Z eingegeben werden,

dadurch gekennzeichnet, dass die Partei X eine Partei-X Zufallszahlerzeugungseinrichtung (901) und eine Partei-X Recheneinrichtung (903) umfasst,

die Partei-X Zufallszahlerzeugungseinrichtung (901) dafür ausgebildet ist, Zahlen c_{q_1} und γ_1 und Zahlenfolgen ($\alpha 1_{q\_0}$, ⋯, $\alpha 1_{q\_nb0-1}$) und ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_na0-1}$) zu erzeugen und die Zahlen und die Zahlenfolgen an die Partei Y zu senden,

die Partei-X Recheneinrichtung (903) dafür ausgebildet ist, Werte c_{q_0} und γ_0 gemäß

$$c_{q\_0} = \sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) - c_{q\_1}$$

$$\gamma_0 = \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 1_{q\_i0} + b0_{q\_j0} \cdot \alpha 1_{q\_j0}) - \gamma_1$$

zu berechnen und die Werte an die Partei Z zu senden,
die Partei Y eine Partei-Y Zufallszahlerzeugungseinrichtung (902) und eine Partei-Y Recheneinrichtung (904) umfasst,
die Partei-Y Zufallszahlerzeugungseinrichtung (902) dafür ausgebildet ist, eine Zahl s_q zu erzeugen und die Zahl an die Partei Z zu senden,
die Partei-Y Recheneinrichtung (904) dafür ausgebildet ist, die Zahlen c_{q_1} und γ_1 und die Zahlenfolgen ($\alpha 1_{q\_0}$, ···, $\alpha 1_{q\_nb0-1}$) und ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_na0-1}$) von der Partei X zu empfangen, Zahlenfolgen ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) und ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) und einen Wert γ' gemäß

$$\alpha 0_{q\_j0} = \sum_{q,\, q\_i1} s_q \cdot e10_{q\_i1,\, q\_j0} \cdot a1_{q\_i1} - \alpha 1_{q\_j0}$$

$$\beta 0_{q\_i0} = \sum_{q,\, q\_j1} s_q \cdot e01_{q\_i0,\, q\_j1} \cdot b1_{q\_j1} - \beta 1_{q\_i0}$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

zu berechnen und die Zahlenfolgen und den Wert an die Partei Z zu senden,
die Partei Z eine Missbrauchsdetektionseinrichtung (905) umfasst, die dafür ausgebildet ist, die Werte c_{q_0} und γ_0 von der Partei X und die Zahl s_q, die Zahlenfolgen ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) und ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) und den Wert γ' von der Partei Y zu empfangen,

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma'$$

zu berechnen und die Verarbeitung zu beenden durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und
die Partei X die Werte c_{q_0} und c_{q_1} ausgibt, die Partei Y die Werte c_{q_1} und 0 ausgibt und die Partei Z 0 und den Wert c_{q_0} ausgibt, wenn das Ergebnis der Berechnung durch die Missbrauchsdetektionseinrichtung 0 ist.

13. Sicheres Produktsummenberechnungssystem, das zur parallelen Ausführung einer Gesamtmenge von m Sätzen von Produktsummenberechnungen von Daten a0 und a1 und Daten-Strings B_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_nb0-1}$) und B_{q_1}= ($b1_{q\_0}$, ..., $b1_{q\_nb1-1}$) durch gemeinsame Berechnung durch drei Rechenvorrichtungen verwendet wird, die eine Partei X, eine Partei Y und eine Partei Z sind, wobei die Produktsummenberechnungen ausgedrückt werden als

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i},$$

wobei q = 0, ..., m-1, m eine ganze Zahl gleich oder größer 1 darstellt, n eine natürliche Zahl darstellt, und i = 0, ..., n-1, und die Daten a0 und a1 und die Daten-Strings B_{q_0} und B_{q_1} in die Partei X eingegeben werden, die Daten a1 und der Daten-String B_{q_1} in die Partei Y eingegeben werden, und die Daten a0 und der Daten-String B_{q_0} in die Partei Z eingegeben werden,

dadurch gekennzeichnet, dass die Partei X eine Partei-X Zufallszahlerzeugungseinrichtung (901) und eine Partei-X Recheneinrichtung (903) umfasst,
die Partei-X Zufallszahlerzeugungseinrichtung (901) dafür ausgebildet ist, Zahlen c_{q_1} und γ_1, eine Zahlenfolge $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_n-1})$ und eine Zahl $\beta 1$ zu erzeugen und die Zahlen und die Zahlenfolge an die Partei Y zu senden,
die Partei-X Recheneinrichtung (903) dafür ausgebildet ist, Werte c_{q_0} und γ_0 gemäß

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

zu berechnen und die Werte an die Partei Z zu senden,
die Partei Y eine Partei-Y Zufallszahlerzeugungseinrichtung (902) und eine Partei-Y Recheneinrichtung (904) umfasst,
die Partei-Y Zufallszahlerzeugungseinrichtung (902) dafür ausgebildet ist, eine Zahl s_q zu erzeugen und die Zahl an die Partei Z zu senden,
die Partei-Y Recheneinrichtung (904) dafür ausgebildet ist, die Zahlen c_{q_1} und γ_1, die Zahlenfolge $(\alpha 1_{q\_0}, ..., \alpha 1_{q\_n-1})$ und die Zahl $\beta 1$ von der Partei X zu empfangen, eine Zahlenfolge $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_n-1})$ und Zahlen $\beta 0$ und γ' gemäß

$$\alpha 0_{q\_i} = \sum_{q} s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

zu berechnen und die Zahlenfolge und die Werte an die Partei Z zu senden,
die Partei Z eine Missbrauchsdetektionseinrichtung (905) umfasst, die dafür ausgebildet ist, die Werte c_{q_0} und γ_0 von der Partei X und die Zahl s_q, die Zahlenfolge $(\alpha 0_{q\_0}, ..., \alpha 0_{q\_n-1})$ und die Werte $\beta 0$ und γ' von der Partei Y zu empfangen,

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma'$$

zu berechnen und die Verarbeitung zu beenden durch Ausgeben von Daten, die eine Missbrauchsdetektion angeben, wenn das Ergebnis der Berechnung nicht 0 ist, und
die Partei X die Werte c_{q_0} und c_{q_1} ausgibt, die Partei Y die Werte c_{q_1} und 0 ausgibt und die Partei Z 0 und den Wert c_{q_0} ausgibt, wenn das Ergebnis der Berechnung durch die Missbrauchsdetektionseinrichtung 0 ist.

14. Programm, das eine Rechenfunktion als eine Rechenvorrichtung nach einem der Ansprüche 1 bis 3 oder ein sicheres Produktsummenberechnungssystem nach einem der Ansprüche 9 bis 13 schafft.

Revendications

1. Appareil de calcul qui est utilisé pour effectuer un calcul de somme de produits à l'aide de trois appareils de calcul qui coopèrent, les trois appareils de calcul servant de partie X, de partie Y et de partie Z, et pour effectuer des traitements symétriques,
dans lequel, à condition qu'un quelconque des appareils de calcul soit une partie P, il est supposé que la partie Z est une partie P_-, et la partie Y est une partie P_+, et les indices 0p, 1p et 2p sont 0, 1 et 2, respectivement, si la partie P est la partie X, la partie X est la partie P_-, la partie Z est la partie P_+, et les indices 0p, 1p et 2p sont 1, 2, et 0, respectivement, si la partie P est la partie Y, et la partie Y est la partie P_-, la partie X est la partie P_+, et les indices 0p, 1p et 2p sont 2, 0 et 1, respectivement, si la partie P est la partie Z,
m représente un entier égal ou supérieur à 1, na0p, na1p, na2p, nb0p et nb1p représentent des nombres naturels, q = 0, ..., m-1, i0p = 0, ..., na0p-1, i1p = 0, ..., nalp-1, i2p = 0, ..., na2p-1 , j0p = 0, ..., nb0p-1, et j1p = 0, ..., nb1p-1, et $e0p1p_{i0pj1p}$, $e1p0p_{i1pj0p}$, $e0p0p_{i0pj0p}$ et $e1p1p_{i1pj1p}$ représentent n'importe quel nombre,
caractérisé en ce que ladite partie P comprend :

un premier moyen de génération de nombre aléatoire (101, 301) adapté pour générer un nombre r_{q_P} et transmettre le nombre à la partie P_+ ;
un premier moyen de calcul (102, 302) adapté pour recevoir des chaînes de données $A_{q\_0p} = (a0p_{q\_0}, ..., a0p_{q\_na0p-1})$, $A_{q\_1p} = (a1p_{q\_0}, ..., a1p_{q\_na1p-1})$, $B_{q\_0p} = (b0p_{q\_0}, ... , b0p_{q\_nb0p-1})$ et $B_{q\_1p} = (b1p_{q\_0}, ..., b1p_{q\_nb1p-1})$, calculer une valeur C_{q_p} selon

$$c_{q\_P} = \sum_{q\_i0p,q\_j1p} (e0p1p_{q\_i0p,q\_j1p} \cdot a0p_{q\_i0p} \cdot b1p_{q\_j1p}) + \sum_{q\_i1p,q\_j0p} (e1p0p_{q\_i1p,q\_j0p} \cdot a1p_{q\_i1p} \cdot b0p_{q\_j0p}) + r_{q\_P},$$

et transmettre la valeur à la partie P_- ; et
un second moyen de calcul (103, 303) adapté pour recevoir un nombre r_{q_P-} de la part de la partie P_-, une valeur C_{q_p+} de la part de la partie P_+, pour calculer des valeurs C_{q_0p} et C_{q_1p} selon

$$c_{q\_0p} = \sum_{q\_i0p,q\_j0p} (e0p0p_{q\_i0p,q\_j0p} \cdot a0p_{q\_i0p} \cdot b0p_{q\_j0p}) + c_{q\_P} - r_{q\_P-}$$

$$c_{q\_1p} = \sum_{q\_i1p,q\_j1p} (e1p1p_{q\_i1p,q\_j1p} \cdot a1p_{q\_i1p} \cdot b1p_{q\_j1p}) + c_{q\_P+} - r_{q\_P}.$$

2. Appareil de calcul selon la revendication 1, **caractérisé en ce que**
les parties P_- et P partagent préalablement un nombre $S_{q\_}P_+$, les parties P et P_+ partagent préalablement un nombre $S_{q\_P}-$, et les parties P_+ et P-partagent préalablement un nombre S_{q_p}, et
la partie P comprend en outre :

un second moyen de génération de nombre aléatoire (304) adapté pour générer une séquence de nombres ($\alpha P+1p_{q\_0}$, ... , $\alpha P+1p_{q\_na1p-1}$) et un nombre ρ_P, et pour transmettre la séquence de nombres et le nombre à la partie P_+, et générer une séquence de nombres ($\alpha P.0p_{q\_0}$, ... , $\alpha P.0p_{q\_na0p-1}$) et transmettre la séquence de nombres à la partie P_- ;
un troisième moyen de calcul (305) adapté pour calculer une séquence de nombres ($\alpha P\_0_{q\_0}$-S_{q_P}-.$a0p_{q\_0}$, ... , $\alpha P\_0p_{q\_na0p-1}$-S_{q_P}-.$a0p_{q\_na0p-1}$) et pour transmettre la séquence de nombres à la partie P_+, recevoir une séquence de nombres ($\alpha P1p_{q\_0}$, ... , $\alpha P1p_{q\_na1p-1}$) de la part de la partie P_+ et une séquence de nombres ($\alpha P0p_{q\_0}$, ... , $\alpha P0P_{q\_na0p-1}$) de la part de la partie P_-, calculer une séquence de nombres ($\alpha P+1p_{q\_0}$-s_{q_P+}.$a1p_{q\_0}$, ..., $\alpha P+1p_{q\_na1p-1}$-S_{q_P+}.$a1p_{q\_na1p-1}$) et une valeur

$$\gamma_P = \sum_{i0p,j1p,q} (e0p1p_{i0p,j1p} \cdot \alpha P0p_{q\_i0p} \cdot b1p_{q\_j1p}) + \sum_{i1p,j0p,q} (e1p0p_{i1p,j0p} \cdot \alpha P1p_{q\_i1p} \cdot b0p_{q\_j0p}) + \rho_P ,$$

et transmettre la séquence de nombres et la valeur à la partie P_- ;

un quatrième moyen de calcul (306) adapté pour recevoir une séquence de nombres ($\alpha P\_2p_{q\_0}$-s_{q_P-}.$a2p_{q\_0}$, ..., αP-$2p_{q\_na2p-1}$-S_{q_P-}.$a2p_{q\_na2p-1}$) de la part de la partie P_+ et une valeur ρ_{P-} de la part de la partie P_-, calculer une valeur $\gamma'_{P\_}$

$$\gamma'_{P-} = \sum_{i2p,j0p,q} \{(\alpha P\_2p_{q\_i2p} - s_{q\_P-} \cdot a2p_{q\_i2p}) \cdot b0p_{q\_j0p} - s_{q\_P-} \cdot r_{q\_P-}\} + \rho_{P-} ,$$

et transmettre la valeur à la partie P_+ ; et

un moyen de détection de mauvaise utilisation (307) adapté pour recevoir une valeur γ_{P+} de la part de la partie P_+ et une valeur γ'_{p+} et une séquence de nombres (αp+$2p_{q\_0}$-s_{q_P+}. $a2p_{q\_0}$, ... , αP+$2p_{q\_na2p-1}$-S_{q_P+}.$a2p_{q\_na2p-1}$) de la part de la partie P_-, calculer

$$\sum_{i2p,j1p,q} \{(\alpha P_+ 2p_{q\_i2p} - s_{q\_P+} \cdot a2p_{q\_i2p}) \cdot b1p_{q\_j1p} + s_{q\_P+} \cdot c_{q\_P+}\} - \gamma_{P+} + \gamma'_{P+} ,$$

mettre fin au traitement en délivrant des données qui indiquent la détection d'une mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant des valeurs C_{q_0p} et C_{q_1p} si le résultat du calcul est 0.

3. Appareil de calcul selon la revendication 1, **caractérisé en ce que**
les parties P_- et P partagent préalablement un nombre S_{q_P+}, les parties P et P_+ partagent préalablement un nombre S_{q_P-}, et les parties P_+ et P_- partagent préalablement un nombre S_{q_p}, et
la partie P comprend en outre :

un second moyen de génération de nombre aléatoire (604) adapté pour générer un nombre ρ_P et transmettre le nombre à la partie P_+, et générer des séquences de nombres (αP-$0p_{q\_0}$, ..., $\alpha P\_0p_{q\_na0p-1}$) et ($\beta P\_0p_{q\_0}$, ..., $\beta P\_0p_{q\_nb0p-1}$) et transmettre les séquences de nombres à la partie P_- ;

un troisième moyen de calcul (605) adapté pour calculer des séquences de nombres ($\alpha P\_0p_{q\_0}$-S_{q_P-}.$a0p_{q\_0}$, ... , $\alpha P\_0p_{q\_na0p-1}$-S_{q_P-}.$a0p_{q\_na0p-1}$) et ($\beta P\_0p_{q\_0}$-S_{q_P-}.$b0p_{q\_0}$, ..., $\beta P\_0p_{q\_na0p-1}$-S_{q_P-}.$b0p_{q\_na0p-1}$) et transmettre les séquences de nombres à la partie P_+, recevoir des séquences de nombres (αP_{1pq_0}, ... , $\alpha P_1p_{q\_na1p-1}$) et ($\beta P_1p_{q\_0}$, ..., $\beta P_1p_{q\_nb1p-1}$) de la part de la partie P_+, calculer une valeur

$$\gamma_P = \sum_{i1p,j0p,q} (e1p0p_{i1p,j0p} \cdot \alpha P1p_{q\_i1p} \cdot b0p_{q\_j0p}) + \sum_{i0p,j1p,q} (e0p1p_{i0p,j1p} \cdot a0p_{q\_i0p} \cdot \beta P1p_{q\_j1p} + \rho_P ,$$

et transmettre la valeur à la partie P_- ;

un quatrième moyen de calcul (606) adapté pour recevoir une valeur ρ_{P-} de la part de la partie P_-, calculer

$$\gamma'_{P-} = \sum_{q}(-s_{q\_P-} \cdot r_{q\_P-}) + \rho_{P-},$$

et transmettre la valeur à la partie P_+ ; et
un moyen de détection de mauvaise utilisation (607) adapté pour recevoir une valeur γ_{P+} de la part de la partie P_+ et une valeur γ'_{P+} et des séquences de nombres ($\alpha P_+ 2p_{q\_0}$-S_{q_P+}. $a2p_{q\_0}$, ... , $\alpha P_+ 2p_{q\_na2p-1}$-S_{q_P+}.$a2p_{q\_na2p-1}$) et ($\beta P_+ 2p_{q\_0}$-S_{q_P+}.$b2p_{q\_0}$, ..., $\beta P_+ 2p_{q\_na2p-1}$-S_{q_P+}.$b2p_{q\_na2p-1}$) de la part de la partie P_-, calculer

$$\sum_{i1p,i2p,j1p,j2p,q}\{(\alpha P_+ 2p_{q\_i2p} - s_{q\_P+} \cdot a2p_{q\_i2p}) \cdot b1p_{q\_j1p} + (\beta P_+ 2p_{q\_j2p} - s_{q\_P+} \cdot b2p_{q\_j2p}) \cdot a1p_{q\_i1p} + s_{q\_P+} \cdot c_{q\_P+}\},$$
$$-\gamma_{P+} + \gamma'_{P+}$$

mettre fin au traitement en délivrant des données qui indiquent la détection d'une mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant des valeurs C_{q_0p} et C_{q_1p} si le résultat du calcul est 0.

4. Procédé de calcul sécurisé de somme de produits utilisé pour effectuer, en parallèle, un total de m groupes de calculs de somme de produits de chaînes de données $A_{q\_0} = (a0_{q\_0}, \ldots, a0_{q\_na0-1})$, $A_{q\_1} = (a1_{q\_0}, \ldots, a1_{q\_na1-1})$ et $A_{q\_2} = (A0_{q\_0}, \ldots, a2_{q\_na2-1})$ et $B_{q\_0} = (b0_{q\_0}, \ldots, b0_{q\_nb0-1})$ et $B_{q\_2} = (b2_{q\_0}, \ldots, b2_{q\_nb2-1})$ à l'aide d'un calcul coopératif par trois appareils de calcul, qui sont une partie X, une partie Y et une partie Z, les calculs de somme de produits étant exprimés comme suit

$$\sum_{q\_i0,q\_j0}(e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1})$$
$$+ \sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) + \sum_{q\_i1,q\_j1}(e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1})$$
$$+ \sum_{q\_i1,q\_j2}(e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j1}(e21_{q\_i2,q\_j1} \cdot a2_{q\_i2} \cdot b1_{q\_j1})$$
$$+ \sum_{q\_i2,q\_j2}(e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j0}(e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0})$$
$$+ \sum_{q\_i0,q\_j2}(e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0})$$

où q = 0, ..., m-1, m représente un entier égal ou supérieur à 1, na0, na1, na2, nb0, nb1 et nb2 représentent des nombres naturels, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, i2 = 0, ..., na2-1, j0 = 0, ..., nb0-1, j1 = 0, ..., nb1-1, et j2 = 0, ..., nb2-1, et $e01_{q\_i0,q\_j1}$, $e10_{q\_i1,q\_j0}$, $e00_{q\_i0,q\_j0}$, $e11_{q\_i1,q\_j1}$, $e12_{q\_i1,q\_j2}$, $e21_{q\_i2,q\_j1}$, $e22_{q\_i2,q\_j2}$, $e20_{q\_i2,q\_j0}$ et $e02_{q\_i0,q\_j2}$ représentent n'importe quel nombre, et les chaînes de données A_{q_0}, A_{q_1}, B_{q_0} et B_{q_1} sont fournies à la partie X, les chaînes de données A_{q_1}, A_{q_2}, B_{q_1} et B_{q_2} sont fournies à la partie Y, et les chaînes de données A_{q_2}, A_{q_0}, B_{q_2} et B_{q_0} sont fournies à la partie Z,
caractérisé en ce que ledit procédé de calcul sécurisé de somme de produits comprend :

une première étape de génération de nombre aléatoire de partie X (S2-1, S22-1), au cours de laquelle la partie X génère un nombre r_{q_x} et transmet le nombre à la partie Y ;
une première étape de calcul de partie X (S2-2, S22-2), au cours de laquelle la partie X calcule une valeur c_{q_x} selon

$$c_{q\_X} = \sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) + r_{q\_X}$$

et transmet la valeur à la partie Z ;
une seconde étape de calcul de partie X (S3, S23) au cours de laquelle la partie X reçoit un nombre r_{q_Z} de la part de la partie Z et une valeur C_{q_Y} de la part de la partie Y, calcule des valeurs c_{q_0} et C_{q_1} selon

$$\begin{aligned} c_{q\_0} &= \sum_{q\_i0,q\_j0} (e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z} \\ c_{q\_1} &= \sum_{q\_i1,q\_j1} (e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X} \end{aligned} ;$$

une première étape de génération de nombre aléatoire de partie Y (S4-1, S24-1), au cours de laquelle la partie Y génère un nombre r_{q_Y} et transmet le nombre à la partie Z ;
une première étape de calcul de partie Y (S4-2, S24-2), au cours de laquelle la partie Y calcule la valeur c_{q_Y} selon

$$c_{q\_Y} = \sum_{q\_i1,q\_j2} (e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{q\_i2,q\_j1} (e21_{q\_i2,q\_j1} \cdot a2_{q\_i2} \cdot b1_{q\_j1}) + r_{q\_Y}$$

et transmet la valeur à la partie X ;
une seconde étape de calcul de partie Y (S5, S25), au cours de laquelle la partie Y reçoit le nombre r_{q_X} de la part de la partie X et une valeur C_{q_Z} de la part de la partie Z, calcule des valeurs c_{q_1} et c_{q_2} selon

$$\begin{aligned} c_{q\_1} &= \sum_{q\_i1,q\_j1} (e11_{q\_i1,q\_j1} \cdot a1_{q\_i1} \cdot b1_{q\_j1}) + c_{q\_Y} - r_{q\_X} \\ c_{q\_2} &= \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y} \end{aligned} ;$$

une première étape de génération de nombre aléatoire de partie Z (S6-1, S26-1), au cours de laquelle la partie Z génère le nombre r_{q_Z} et transmet le nombre à la partie X ;
une première étape de calcul de partie Z (S6-2, S26-2), au cours de laquelle la partie Z calcule la valeur C_{q_Z} selon

$$c_{q\_Z} = \sum_{q\_i2,q\_j0} (e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{q\_i0,q\_j2} (e02_{q\_i0,q\_j2} \cdot a2_{q\_i2} \cdot b0_{q\_i0}) + r_{q\_Z}$$

et transmet la valeur à la partie Y ; et
une seconde étape de calcul de partie Z (S7, S27), au cours de laquelle la partie Z reçoit le nombre r_{q_Y} de la part de la partie Y et une valeur C_{q_X} de la part de la partie X, calcule des valeurs C_{q_0} et c_{q_2} selon

$$c_{q\_0} = \sum_{q\_i0,q\_j0} (e00_{q\_i0,q\_j0} \cdot a0_{q\_i0} \cdot b0_{q\_j0}) + c_{q\_X} - r_{q\_Z}$$

$$c_{q\_2} = \sum_{q\_i2,q\_j2} (e22_{q\_i2,q\_j2} \cdot a2_{q\_i2} \cdot b2_{q\_j2}) + c_{q\_Z} - r_{q\_Y}$$

5. Procédé de calcul sécurisé de somme de produits selon la revendication 4, **caractérisé en ce que** les parties X et Y partagent préalablement un nombre S_{q_Z}, les parties Y et Z partagent préalablement un nombre S_{q_X}, et les parties Z et X partagent préalablement un nombre S_{q_Y}, et
ledit procédé sécurisé de calcul de somme de produits comprend en outre :

une seconde étape de génération de nombre aléatoire de partie X (S28), au cours de laquelle la partie X génère une séquence de nombres ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) et un nombre ρ_x, et transmet la séquence de nombres et le nombre à la partie Y, et génère une séquence de nombres ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) et transmet la séquence de nombres à la partie Z ;
une troisième étape de calcul de partie X (S29), au cours de laquelle la partie X calcule une séquence de nombres ($\alpha Z0_{q\_0}$-S_{q_Z}·$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-S_{q_Z}·$a0_{q\_na0-1}$) et transmet la séquence de nombres à la partie Y, reçoit une séquence de nombres ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) de la part de la partie Y et une séquence de nombres ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) de la part de la partie Z, calcule une séquence de nombres ($\alpha Y1_{q\_0}$-S_{q_Y}·$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-S_{q_Y}·$a1_{q\_na1-1}$) et une valeur

$$\gamma_X = \sum_{i0,j1,q} (e01_{q\_i0,q\_j1} \cdot \alpha X0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{i1,j0,q} (e10_{q\_i1,q\_j0} \cdot \alpha X1_{q\_i1} \cdot b0_{q\_j0}) + \rho_X',$$

et transmet la séquence de nombres et la valeur à la partie Z ;
une quatrième étape de calcul de partie X (S30), au cours de laquelle la partie X reçoit une séquence de nombres ($\alpha Z2_{q\_0}$-S_{q_Z}·$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-S_{q_Z}·$a2_{q\_na2-1}$) de la part de la partie Y et une valeur ρ_Z de la part de la partie Z, calcule une valeur

$$\gamma'_Z = \sum_{i2,j0,q} \{e20_{q\_i2,q\_j0} \cdot (\alpha Z2_{q\_i2} - s_{q\_z} \cdot a2_{q\_i2}) \cdot b0_{q\_j0} - s_{q\_z} \cdot r_{q\_z}\} + \rho_Z',$$

et transmet la valeur à la partie Y ;
une étape de détection de mauvaise utilisation de partie X (S31), au cours de laquelle la partie X reçoit une valeur γ_Y de la part de la partie Y et une valeur γ'_Y et une séquence de nombres ($\alpha Y2_{q\_0}$-S_{q_Y}·$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-S_{qY}·$a2_{qna2-1}$) de la part de la partie Z, calcule

$$\sum_{i2,j1,q} \{e21_{q\_i2,q\_j1} \cdot (\alpha Y2_{q\_i2} - s_{q\_Y} \cdot a2_{q\_i2}) \cdot b1_{q\_j1} + s_{q\_Y} \cdot c_{q\_Y}\} - \gamma_Y + \gamma'_Y,$$

met fin au traitement en délivrant des données qui indiquent la détection d'une mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant les valeurs c_{q_0} et C_{q_1} si le résultat du calcul est 0 ;
une seconde étape de génération de nombre aléatoire de partie Y (S32), au cours de laquelle la partie Y génère une séquence de nombres ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) et un nombre ρ_Y et transmet la séquence de nombres et le nombre à la partie Z, et génère la séquence de nombres ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) et transmet la séquence de nombres à la partie X ;
une troisième étape de calcul de partie Y (S33), au cours de laquelle la partie Y calcule une séquence de nombres ($\alpha X1_{q\_0}$-S_{q_X}.$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-S_{q_X}.$a1_{q\_na1-1}$) et transmet la séquence de nombres à la partie Z,

reçoit la séquence de nombres ($\alpha Y1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$) de la part de la partie X et une séquence de nombres ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) de la part de la partie Z, calcule la séquence de nombres ($\alpha Z2_{q\_0}$-S_{q_Z}.$a2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$-S_{q_Z}.$a2_{q\_na2-1}$) et la valeur

$$\gamma_Y = \sum_{i1,j2,q} (e12_{q\_i1,q\_j2} \cdot \alpha Y1_{q\_i1} \cdot b2_{q\_j2}) + \sum_{i2,j1,q} (e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \rho_Y,$$

et transmet la séquence de nombres et la valeur à la partie X ;

une quatrième étape de calcul de partie Y (S34), au cours de laquelle la partie Y reçoit le nombre ρ_X de la part de la partie X et une séquence de nombres ($\alpha X0_{q\_0}$-S_{q_X}.$a0_{q\_0}$, ... , $\alpha X0_{q\_na0-1}$-S_{q_X}.$a0_{q\_na0-1}$) de la part de la partie Z, calcule une valeur

$$\gamma'_X = \sum_{i0,j1,q} \{e01_{q\_i0,q\_j1} \cdot (\alpha X0_{q\_i0} - s_{q\_x} \cdot a0_{q\_i0}) \cdot b1_{q\_j1} - s_{q\_x} \cdot r_{q\_x}\} + \rho_X,$$

et transmet la valeur à la partie Z ;

une étape de détection de mauvaise utilisation de partie Y (S35), au cours de laquelle la partie Y reçoit la valeur γ'_Z et la séquence de nombres ($\alpha Z0_{q\_0}$-S_{q_Z}.$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-S_{q_Z}.$a0_{q\_na0-1}$) de la part de la partie X et une valeur γ_Z de la part de la partie Z, calcule

$$\sum_{i0,j2,q} \{e02_{q\_i0,q\_j2} \cdot (\alpha Z0_{q\_i0} - s_{q\_Z} \cdot a0_{q\_i0}) \cdot b2_{q\_j2} + s_{q\_Z} \cdot c_{q\_Z}\} - \gamma_Z + \gamma'_Z,$$

met fin au traitement en délivrant des données qui indiquent une détection de mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant les valeurs c_{q_1} et c_{q_2} si le résultat du calcul est 0 ;

une seconde étape de génération de nombre aléatoire de partie Z (S36), au cours de laquelle la partie Z génère la séquence de nombres ($\alpha X0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$) et le nombre ρ_Z et transmet la séquence de nombres et le nombre à la partie X, et génère la séquence de nombres ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) et transmet la séquence de nombres à la partie Y ;

une troisième étape de calcul de partie Z (S37), au cours de laquelle la partie Z calcule la séquence de nombres ($\alpha Y2_{q\_0}$-S_{q_Y}.$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-S_{q_Y}.$a2_{q\_na2-1}$) et transmet la séquence de nombres à la partie X, reçoit la séquence de nombres ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) de la part de la partie X et la séquence de nombres ($\alpha Z2_{q\_0}$, ..., $\alpha Z2_{q\_na2-1}$) de la part de la partie Y, calcule la séquence de nombres ($\alpha X0_{q\_0}$-S_{q_X}.$a0_{q\_0}$, ..., $\alpha X0_{q\_na0-1}$-S_{q_X}.$a0_{q\_na0-1}$) et la valeur

$$\gamma_Z = \sum_{i2,j0,q} (e20_{q\_i2,q\_j0} \cdot \alpha Z2_{q\_i2} \cdot b0_{q\_j0}) + \sum_{i0,j2,q} (e02_{q\_i0,q\_j2} \cdot \alpha Z0_{q\_i0} \cdot b2_{q\_j2}) + \rho_Z,$$

et transmet la séquence de nombres et la valeur à la partie Y ;

une quatrième étape de calcul de partie Z (S38), au cours de laquelle la partie Z reçoit la séquence de nombres ($\alpha Y1_{q\_0}$-S_{q_Y}.$a1_{q\_0}$, ..., $\alpha Y1_{q\_na1-1}$-S_{q_Y}.$a1_{q\_na1-1}$) de la part de la partie X et le nombre ρ_Y de la part de la partie Y, calcule une valeur

$$\gamma'_Y = \sum_{i1,j2,q} \{e12_{q\_i1,q\_j2} \cdot (\alpha Y1_{q\_i1} - s_{q\_Y} \cdot a1_{q\_i1}) \cdot b2_{q\_j2} - s_{q\_Y} \cdot r_{q\_Y}\} + \rho_Y,$$

et transmet la valeur à la partie X ; et

une étape de détection de mauvaise utilisation de partie Z (S39), au cours de laquelle la partie Z reçoit une valeur γ_X de la part de la partie X et une valeur γ'_X et la séquence de nombres ($\alpha X1_{q\_0}$-S_{q_X}.$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-S_{q_X}.$a1_{q\_na1-1}$) de la part de la partie Y, calcule

$$\sum_{i1,j0,q}\{e10_{q\_i1,q\_j0}\cdot(\alpha X1_{q\_i1}-s_{q\_x}\cdot a1_{q\_i1})\cdot b0_{q\_j0}+s_{q\_x}\cdot c_{q\_x}\}-\gamma_X+\gamma'_X,$$

met fin au traitement en délivrant des données qui indiquent la détection d'une mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant les valeurs c_{q_2} et C_{q_0} si le résultat du calcul est 0.

6. Procédé de calcul sécurisé de somme de produits selon la revendication 4, **caractérisé en ce que** les parties X et Y partagent préalablement un nombre S_{q_Z}, les parties Y et Z partagent préalablement un nombre S_{q_X}, et les parties Z et X partagent préalablement un nombre S_{q_Y}, et
ledit procédé sécurisé de calcul de somme de produits comprend en outre :

une seconde étape de génération de nombre aléatoire de partie X (S68), au cours de laquelle la partie X génère un nombre ρ_X et transmet le nombre à la partie Y, et génère des séquences de nombres ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) et ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$) et transmet les séquences de nombres à la partie Z ;
une troisième étape de calcul de partie X (S69), au cours de laquelle la partie X calcule des séquences de nombres ($\alpha Z0_{q\_0}$-S_{q_Z}.$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-S_{q_Z}.$a0_{q\_na0-1}$) et ($\beta Z0_{q\_0}$-S_{q_Z}.$b0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$-S_{q_Z}.$b0_{q\_nb0-1}$) et transmet les séquences de nombres à la partie Y, reçoit les séquences de nombres ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) et ($\beta X1_{q\_0}$, ..., $\beta X1_{q\ nb1-1}$) de la part de la partie Y, calcule une valeur

$$\gamma_X=\sum_{i1,j0,q}(e10_{i1,j0}\cdot\alpha X1_{q\_i1}\cdot b0_{q\_j0})+\sum_{i0,j1,q}(e01_{i0,j1}\cdot a0_{q\_i0}\cdot\beta X1_{q\_j1})+\rho_X,$$

et transmet la valeur à la partie Z ;
une quatrième étape de calcul de partie X (S70) au cours de laquelle la partie X reçoit une valeur ρ_Z de la part de la partie Z, calcule une valeur

$$\gamma'_Z=\sum_{q}(-s_{q\_z}\cdot r_{q\_z})+\rho_Z,$$

et transmet la valeur à la partie Y ;
une étape de détection de mauvaise utilisation de partie X (S71), au cours de laquelle la partie X reçoit une valeur γ_Y de la part de la partie Y, et une valeur γ'_Y et des séquences de nombres ($\alpha Y2_{q\_0}$-S_{q_Y}.$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-S_{q_Y}.$a2_{q\_na2-1}$) et ($\beta Y2_{q\_0}$-S_{q_Y}.$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$-S_{q_Y}.$b2_{q\ nb2-1}$) de la part de la partie Z, calcule

$$\sum_{i1,i2,j1,j2,q}\{e21_{q\_i2,q\_j1}\cdot(\alpha Y2_{q\_i2}-s_{q\_Y}\cdot a2_{q\_i2})\cdot b1_{q\_j1}+e12_{q\_i1,q\_j2}\cdot(\beta Y2_{q\_j2}-s_{q\_Y}\cdot b2_{q\_j2})\cdot a1_{q\_i1}+s_{q\_Y}\cdot c_{q\_Y}\}-\gamma_Y+\gamma'_Y,$$

met fin au traitement en délivrant des données qui indiquent la détection d'une mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant les valeurs C_{q_0} et c_{q_1} si le résultat du calcul est 0 ;
une seconde étape de génération de nombre aléatoire de partie Y (S72), au cours de laquelle la partie Y génère un nombre ρ_Y et transmet le nombre à la partie Z, et génère les séquences de nombres ($\alpha X1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$) et ($\beta X1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$) et transmet les séquences de nombres à la partie X ;
une troisième étape de calcul de partie Y (S73), au cours de laquelle la partie Y calcule des séquences de nombres ($\alpha X1_{q\_0}$-S_{q_X}.$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-S_{q_X}.$a1_{q\_na1-1}$) et ($\beta X1_{q\_0}$-S_{q_X}.$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-S_{q_X}.$b1_{q\_nb1-1}$) et transmet les séquences de nombres à la partie Z, reçoit les séquences de nombres ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) et ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) de la part de la partie Z, calcule une valeur

$$\gamma_Y = \sum_{i2,j1,q}(e21_{q\_i2,q\_j1} \cdot \alpha Y2_{q\_i2} \cdot b1_{q\_j1}) + \sum_{i1,j2,q}(e12_{q\_i1,q\_j2} \cdot a1_{q\_i1} \cdot \beta Y2_{q\_j2}) + \rho_Y,$$

et transmet la valeur à la partie X ;
une quatrième étape de calcul de partie Y (S74), au cours de laquelle la partie Y reçoit le nombre Px de la part de la partie X, calcule une valeur

$$\gamma'_X = \sum_q(-s_{q\_x} \cdot r_{q\_x}) + \rho_X,$$

et transmet la valeur à la partie Z ;
une étape de détection de mauvaise utilisation de partie Y (S75), au cours de laquelle la partie Y reçoit une valeur γ'_Z et les séquences de nombres ($\alpha Z0_{q\_0}$-S_{q_Z}.$a0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$-S_{q_Z}.$a0_{q\_na0-1}$) et ($\beta Z0_{q\_0}$-S_{q_Z}.$b0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$-S_{q_Z}.$b0_{q\_nb0-1}$) de la part de la partie X, et une valeur γ_Z de la part de la partie Z, calcule

$$\sum_{i0,i2,j0,j2,q}\{e02_{q\_i0,q\_j2} \cdot (\alpha Z0_{q\_i0} - s_{q\_z} \cdot a0_{q\_i0}) \cdot b2_{q\_j2} + e20_{q\_i2,q\_j0} \cdot (\beta Z0_{q\_j0} - s_{q\_z} \cdot b0_{q\_j0}) \cdot a2_{q\_i2} + s_{q\_z} \cdot c_{q\_z}\} - \gamma_Z + \gamma'_Z,$$

met fin au traitement en délivrant des données qui indiquent la détection d'une mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant les valeurs c_{q_1} et c_{q_2} si le résultat du calcul est 0 ;
une seconde étape de génération de partie Z (S76), au cours de laquelle la partie Z génère le nombre ρ_Z et transmet le nombre à la partie X, et génère les séquences de nombres ($\alpha Y2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$) et ($\beta Y2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$) et transmet les séquences de nombres à la partie Y ;
une troisième étape de calcul de partie Z (S77), au cours de laquelle la partie Z calcule les séquences de nombres ($\alpha Y2_{q\_0}$-S_{q_Y}.$a2_{q\_0}$, ..., $\alpha Y2_{q\_na2-1}$-S_{q_Y}.$a2_{q\_na2-1}$) et ($\beta Y2_{q\_0}$-S_{q_Y}.$b2_{q\_0}$, ..., $\beta Y2_{q\_nb2-1}$-S_{q_Y}.$b2_{q\_nb2-1}$) et transmet les séquences de nombres à la partie X, reçoit les séquences de nombres ($\alpha Z0_{q\_0}$, ..., $\alpha Z0_{q\_na0-1}$) et ($\beta Z0_{q\_0}$, ..., $\beta Z0_{q\_nb0-1}$) de la part de la partie X, calcule la valeur

$$\gamma_Z = \sum_{i0,j2,q}(e02_{q\_i0,q\_j2} \cdot \alpha Z0_{q\_i0} \cdot b2_{q\_j0}) + \sum_{i2,j0,q}(e20_{q\_i2,q\_j0} \cdot a2_{q\_i2} \cdot \beta Z0_{q\_j0}) + \rho_Z,$$

et transmet la valeur à la partie Y ;
une quatrième étape de calcul de partie Z (S78) au cours de laquelle la partie Z reçoit le nombre ρ_Y de la part de la partie Y, calcule une valeur

$$\gamma'_Y = \sum_q(-s_{q\_Y} \cdot r_{q\_Y}) + \rho_Y,$$

et transmet la valeur à la partie X ; et
une étape de détection de mauvaise utilisation de partie Z (S79), au cours de laquelle la partie Z reçoit une valeur γ_X de la part de la partie X et une valeur γ'_X et les séquences de nombres ($\alpha X1_{q\_0}$-S_{q_X}.$a1_{q\_0}$, ..., $\alpha X1_{q\_na1-1}$-S_{q_X}.$a1_{q\_na1-1}$) et ($\beta X1_{q\_0}$-S_{q_X}.$b1_{q\_0}$, ..., $\beta X1_{q\_nb1-1}$-S_{q_X}.$b1_{q\_nb1-1}$) de la part de la partie Y, calcule

$$\sum_{i0,i1,j0,j1,q}\{e10_{q\_i1,q\_j0}\cdot(\alpha X1_{q\_i1}-s_{q\_x}\cdot a1_{q\_i1})\cdot b0_{q\_j0}\}$$
$$+e01_{q\_i0,q\_j1}\cdot(\beta X1_{q\_j1}-s_{q\_x}\cdot b1_{q\_j1})\cdot a0_{q\_i0}+s_{q\_x}\cdot c_{q\_x}\}-\gamma_X+\gamma'_X,$$

met fin au traitement en délivrant des données qui indiquent une détection de mauvaise utilisation si le résultat du calcul est différent de 0, et en délivrant les valeurs c_{q_2} et C_{q_0} si le résultat du calcul est 0.

7. Procédé de calcul sécurisé de somme de produits utilisé pour effectuer, en parallèle, un total de m groupes de calculs de somme de produits de chaînes de données $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0-1})$ et $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_na1-1}$ et $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ et $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ à l'aide d'un calcul coopératif par trois appareils de calcul, qui sont une partie X, une partie Y et une partie Z, les calculs de somme de produits étant exprimés comme suit

$$\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1}\cdot a0_{q\_i0}\cdot b1_{q\_j1})+\sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0}\cdot a1_{q\_i1}\cdot b0_{q\_j0})$$

où q = 0, ..., m-1, m représente un entier égal ou supérieur à 1, na0, na1, nb0 et nb1 représentent des nombres naturels, i0 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, et 1 = 0, ..., nb1-1, et $e01_{q\_i0,q\_j1}$ et $e10_{q\_i1,q\_j0}$ représentent n'importe quel nombre, et les chaînes de données A_{q_0}, A_{q_1}, B_{q_0} et B_{q_1} sont fournies à la partie X, les chaînes de données A_{q_1} et B_{q_1} sont fournies à la partie Y, et les chaînes de données A_{q_0} et B_{q_0} sont fournies à la partie Z,

caractérisé en ce que ledit procédé de calcul sécurisé de somme de produits comprend :

une étape de génération de nombre aléatoire de partie X (S102), au cours de laquelle la partie X génère des nombres c_{q_1} et γ_1 et les séquences de nombres $(\alpha1_{q\_0}, ..., \alpha1_{q\_nb0-1})$ et $(\beta1_{q\_0}, ..., \beta1_{q\_na0-1})$ et transmet les nombres et les séquences de nombres à la partie Y ;

une étape de génération de nombre aléatoire de partie Y (S103), au cours de laquelle la partie Y génère un nombre S_Q et transmet le nombre à la partie Z ;

une étape de calcul de partie X (S104), au cours de laquelle la partie X calcule des valeurs C_{q_0} et γ_0 selon

$$c_{q\_0}=\sum_{q\_i0,q\_j1}(e01_{q\_i0,q\_j1}\cdot a0_{q\_i0}\cdot b1_{q\_j1})+\sum_{q\_i1,q\_j0}(e10_{q\_i1,q\_j0}\cdot a1_{q\_i1}\cdot b0_{q\_j0})-c_{q\_1}$$
$$\gamma_0=\sum_{i0,j0,q}(a0_{q\_i0}\cdot\beta1_{q\_i0}+b0_{q\_j0}\cdot\alpha1_{q\_j0})-\gamma_1$$

et transmet les valeurs à la partie Z ;

une étape de calcul de partie Y (S105), au cours de laquelle la partie Y reçoit les nombres C_{q_1} et γ_1 et les séquences de nombres $(\alpha1_{q\_0}, ..., \alpha1_{q\_nb0-1})$ et $(\beta1_{q\_0}, ..., \beta1_{q\_na0-1})$ de la part de la partie X, calcule les séquences de nombres $(\alpha0_{q\_0}, ..., \alpha0_{q\_nb0-1})$ et $(\beta0_{q\_0}, ..., \beta0_{q\_na0-1})$ et une valeur γ' selon

$$\alpha0_{q\_j0}=\sum_{q,q\_i1}s_q\cdot e10_{q\_i1,q\_j0}\cdot a1_{q\_i1}-\alpha1_{q\_j0}$$
$$\beta0_{q\_i0}=\sum_{q,q\_j1}s_q\cdot e01_{q\_i0,q\_j1}\cdot b1_{q\_j1}-\beta1_{q\_i0}$$
$$\gamma'=\sum_{q}s_q\cdot c_{q\_1}-\gamma_1$$

et transmet les séquences de nombres et la valeur à la partie Z ; et
une étape de détection de mauvaise utilisation (S106), au cours de laquelle la partie Z reçoit les valeurs C_{q_0} et γ_0 de la part de la partie X et le nombre S_q, les séquences de nombres ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) et ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) et la valeur γ' de la part de la partie Y, calcule

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma',$$

et met fin au traitement en délivrant des données qui indiquent une détection de mauvaise utilisation si le résultat du calcul est différent de 0,
où, si le résultat du calcul à l'étape de détection de mauvaise utilisation est 0, la partie X délivre les valeurs C_{q_0} et c_{q_1}, la partie Y délivre la valeur c_{q_1} et 0, et la partie Z délivre 0 et la valeur C_{q_0}.

8. Procédé de calcul sécurisé de somme de produits utilisé pour effectuer, en parallèle, un total de m groupes de calculs de somme de produits de données a0 et a1 et de chaînes de données B_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_nb0-1}$) et B_{q_1} = ($b1_{q\_0}$, ..., $b1_{q\_nb1-1}$) à l'aide d'un calcul coopératif par trois appareils de calcul, qui sont une partie X, une partie Y et une partie Z, les calculs de somme de produits étant exprimés comme suit

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i}$$

où q = 0, ..., m-1, m représente un entier égal ou supérieur à 1, n représente un nombre naturel, et i = 0, ..., n-1, et les données a0 et a1 et les chaînes de données B_{q_0} et B_{q_1} sont fournies à la partie X, les données a1 et la chaîne de données B_{q_1} sont fournies à la partie Y, et les données a0 et la chaîne de données B_{q_0} sont fournies à la partie Z, **caractérisé en ce que** ledit procédé de calcul sécurisé de somme de produits comprend :

une étape de génération de nombre aléatoire de partie X (S102), au cours de laquelle la partie X génère des nombres c_{q_1} et γ_1 et une séquence de nombres ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) et un nombre $\beta 1$, et transmet les nombres et la séquence de nombre à la partie Y,
une étape de génération de nombre aléatoire de partie Y (S103), au cours de laquelle la partie Y génère un nombre S_q et transmet le nombre à la partie Z ;
une étape de calcul de partie X (S104), au cours de laquelle la partie X calcule des valeurs C_{q_0} et γ_0 selon

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

et transmet la valeur à la partie Z ;
une étape de calcul de partie Y (S105), au cours de laquelle la partie Y reçoit les nombres c_{q_1} et γ_1 et la séquence de nombres ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) et le nombre $\beta 1$ de la part de la partie X, calcule une séquence de nombres ($\alpha 0_{q0}$, ..., $\alpha 0_{q\ n-1}$) et des nombres $\beta 0$ et γ' selon

$$\alpha 0_{q\_i} = \sum_{q} s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1 \quad ,$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

et transmet la séquence de nombres et les valeurs à la partie Z ; et

une étape de détection de mauvaise utilisation (S106), au cours de laquelle la partie Z reçoit les valeurs c_{q_0} et γ_0 de la part de la partie X et le nombre S_q, la séquence de nombres (α_{q_0}, ..., $\alpha 0_{q\_n-1}$) et les valeurs $\beta 0$ et γ' de la part de la partie Y, calcule

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma',$$

et met fin au traitement en délivrant des données qui indiquent une détection de mauvaise utilisation si le résultat du calcul est différent de 0,

où, si le résultat du calcul au cours de l'étape de détection de mauvaise utilisation est 0, la partie X délivre les valeurs C_{q_0} et c_{q_1}, la partie Y délivre la valeur c_{q_1} et 0, et la partie Z délivre 0 et la valeur C_{q_0}.

9. Système de calcul sécurisé de somme de produits qui utilise trois appareils de calcul selon la revendication 1, comme partie X, partie Y et partie Z.

10. Système de calcul sécurisé de somme de produits qui utilise trois appareils de calcul selon la revendication 2, comme partie X, partie Y et partie Z.

11. Système de calcul sécurisé de somme de produits qui utilise trois appareils de calcul selon la revendication 3, comme partie X, partie Y et partie Z.

12. Système de calcul sécurisé de somme de produits utilisé pour effectuer, en parallèle, un total de m groupes de calculs de somme de produits de chaînes de données $A_{q\_0} = (a0_{q\_0}, ..., a0_{q\_na0-1})$ et $A_{q\_1} = (a1_{q\_0}, ..., a1_{q\_na1-1})$ et $B_{q\_0} = (b0_{q\_0}, ..., b0_{q\_nb0-1})$ et $B_{q\_1} = (b1_{q\_0}, ..., b1_{q\_nb1-1})$ à l'aide d'un calcul coopératif par trois appareils de calcul, qui sont une partie X, une partie Y et une partie Z, les calculs de somme de produits étant exprimés comme suit

$$\sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0})$$

où q = 0, ..., m-1, m représente un entier égal ou supérieur à 1, na0, na1, nb0 et nb1 représentent des nombres naturels, 10 = 0, ..., na0-1, i1 = 0, ..., na1-1, j0 = 0, ..., nb0-1, et j1 = 0, ..., nb1-1, et $e01_{q\_i0,q\_j1}$ et $e10_{q\_i1,q\_j0}$ représentent n'importe quel nombre, et les chaînes de données A_{q_0}, A_{q_1}, B_{q_0} et B_{q_1} sont fournies à la partie X, les chaînes de données A_{q_1} et B_{q_1} sont fournies à la partie Y, et les chaînes de données A_{q_0} et B_{q_0} sont fournies à la partie Z,

caractérisé en ce que la partie X comprend un moyen de génération de nombre aléatoire de partie X (901) et un moyen de calcul de partie X (903),

le moyen de génération de nombre aléatoire de partie X (901) étant adapté pour générer des nombres C_{q_1} et γ_1 et des séquences de nombres ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_nb0-1}$) et ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_na0-1}$) et transmettent les nombres et les séquences de nombres à la partie Y,

le moyen de calcul de partie X (903) étant adapté pour calculer des valeurs C_{q_0} et γ_0 selon

$$c_{q\_0} = \sum_{q\_i0,q\_j1} (e01_{q\_i0,q\_j1} \cdot a0_{q\_i0} \cdot b1_{q\_j1}) + \sum_{q\_i1,q\_j0} (e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} \cdot b0_{q\_j0}) - c_{q\_1}$$

$$\gamma_0 = \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 1_{q\_i0} + b0_{q\_j0} \cdot \alpha 1_{q\_j0}) - \gamma_1$$

et transmettre les valeurs à la partie Z,
la partie Y comprend un moyen de génération de nombre aléatoire de partie Y (902) et un moyen de calcul de partie Y (904),
le moyen de génération de nombre aléatoire de partie Y (902) étant adapté pour générer un nombre Sq et transmettre le nombre à la partie Z,
le moyen de calcul de partie Y (904) étant adapté pour recevoir les nombres C_{q_1} et γ_1 et les séquences de nombres ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_nb0-1}$) et ($\beta 1_{q\_0}$, ..., $\beta 1_{q\_na0-1}$) de la part de la partie X, calculer des séquences de nombres ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\ nb0-1}$) et ($\beta 0_{q0}$, ..., $\beta 0_{q\ na0-1}$) et une valeur γ' selon

$$\alpha 0_{q\_j0} = \sum_{q,q\_i1} s_q \cdot e10_{q\_i1,q\_j0} \cdot a1_{q\_i1} - \alpha 1_{q\_j0}$$

$$\beta 0_{q\_i0} = \sum_{q,q\_j1} s_q \cdot e01_{q\_i0,q\_j1} \cdot b1_{q\_j1} - \beta 1_{q\_i0},$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

et transmettre les séquences de nombres et la valeur à la partie Z,
la partie Z comprend un moyen de détection de mauvaise utilisation (905), adapté pour recevoir les valeurs c_{q_0} et γ_0 de la part de la partie X et le nombre Sq, les séquences de nombres ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_nb0-1}$) et ($\beta 0_{q\_0}$, ..., $\beta 0_{q\_na0-1}$) et la valeur γ' de la part de la partie Y, calculer

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - \sum_{i0,j0,q} (a0_{q\_i0} \cdot \beta 0_{q\_i0} + b0_{q\_j0} \cdot \alpha 0_{q\_j0}) + \gamma',$$

et mettre fin au traitement en délivrant des données qui indiquent une détection de mauvaise utilisation si le résultat du calcul est différent de 0, et
la partie X délivre les valeurs c_{q_0} et c_{q_1}, la partie Y délivre la valeur c_{q_1} et 0, et la partie Z délivre 0 et la valeur c_{q_0} si le résultat du calcul par le moyen de détection de mauvaise utilisation est 0.

13. Système de calcul sécurisé de somme de produits utilisé pour effectuer, en parallèle, un total de m groupes de calculs de somme de produits de données a0 et a1 et de chaînes de données B_{q_0} = ($b0_{q\_0}$, ..., $b0_{q\_nb0-1}$) et B_{q_1} = ($b1_{q\_0}$, ..., $b1_{q\_nb1-1}$) à l'aide d'un calcul coopératif par trois appareils de calcul, qui sont une partie X, une partie Y et une partie Z, les calculs de somme de produits étant exprimés comme suit

$$\sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i}$$

où q = 0, ..., m-1, m représente un entier égal ou supérieur à 1, n représente un nombre naturel, et i = 0, ..., n-1, et les données a0 et a1 et les chaînes de données B_{q_0} et B_{q_1} sont fournies à la partie X, les données a1 et la chaîne de données B_{q_1} sont fournies à la partie Y, et les données a0 et la chaîne de données B_{q_0} sont fournies à la partie Z, **caractérisé en ce que** la partie X comprend un moyen de génération de nombre aléatoire de partie X (901) et un

moyen de calcul de partie X (903),
le moyen de génération de nombre aléatoire de partie X (901) étant adapté pour générer des nombres c_{q_1} et γ_1, une séquence de nombres ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) et un nombre $\beta 1$, et transmettre les nombres et la séquence de nombres à la partie Y,
le moyen de calcul de partie X (903) étant adapté pour calculer des valeurs C_{q_0} et γ_0 selon

$$c_{q\_0} = \sum_{q\_i} a0 \cdot b1_{q\_i} + \sum_{q\_i} a1 \cdot b0_{q\_i} - c_{q\_1}$$

$$\gamma_0 = a0 \cdot \beta 1 + \sum_{i,q} b0_{q\_i} \cdot \alpha 1_{q\_i} - \gamma_1$$

et transmettre les valeurs à la partie Z,
la partie Y comprend un moyen de génération de nombre aléatoire de partie Y (902) et un moyen de calcul de partie Y (904),
le moyen de génération de nombre aléatoire de partie Y (902) étant adapté pour générer un nombre sq et transmettre le nombre à la partie Z,
le moyen de calcul de partie Y (904) étant adapté pour recevoir les nombres C_{q_1} et γ_1, la séquence de nombres ($\alpha 1_{q\_0}$, ..., $\alpha 1_{q\_n-1}$) et le nombre $\beta 1$ de la part de la partie X, calculer une séquence de nombres ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\ n-1}$) et des nombres $\beta 0$ et γ' selon

$$\alpha 0_{q\_i} = \sum_{q} s_q \cdot a1 - \alpha 1_{q\_i}$$

$$\beta 0 = \sum_{i,q} s_q \cdot b1_{q\_i} - \beta 1 \quad ,$$

$$\gamma' = \sum_{q} s_q \cdot c_{q\_1} - \gamma_1$$

et transmettre la séquence de nombres et la valeur à la partie Z,
la partie Z comprend un moyen de détection de mauvaise utilisation (905) adapté pour recevoir les valeurs C_{q_0} et γ_0 de la part de la partie X et le nombre Sq, la séquence de nombres ($\alpha 0_{q\_0}$, ..., $\alpha 0_{q\_n-1}$) et les valeurs $\beta 0$ et γ' de la part de la partie Y, calculer

$$\sum_{q} s_q \cdot c_{q\_0} - \gamma_0 - a0 \cdot \beta 0 - \sum_{i,q} b0_{q\_i} \cdot \alpha 0_{q\_i} + \gamma' :$$

et mettre fin au traitement en délivrant des données qui indiquent une détection de mauvaise utilisation si le résultat du calcul est différent de 0, et
la partie X délivre les valeurs C_{q_0} et C_{q_1}, la partie Y délivre la valeur C_{q_1} et 0, et la partie Z délivre 0 et la valeur C_{q_0} si le résultat du calcul par le moyen de détection de mauvaise utilisation est 0.

14. Programme qui exécute une fonction informatique en guise d'appareil de calcul selon l'une quelconque des revendications 1 à 3, ou système sécurisé de calcul de somme de produits selon l'une quelconque des revendications 9 à 13.

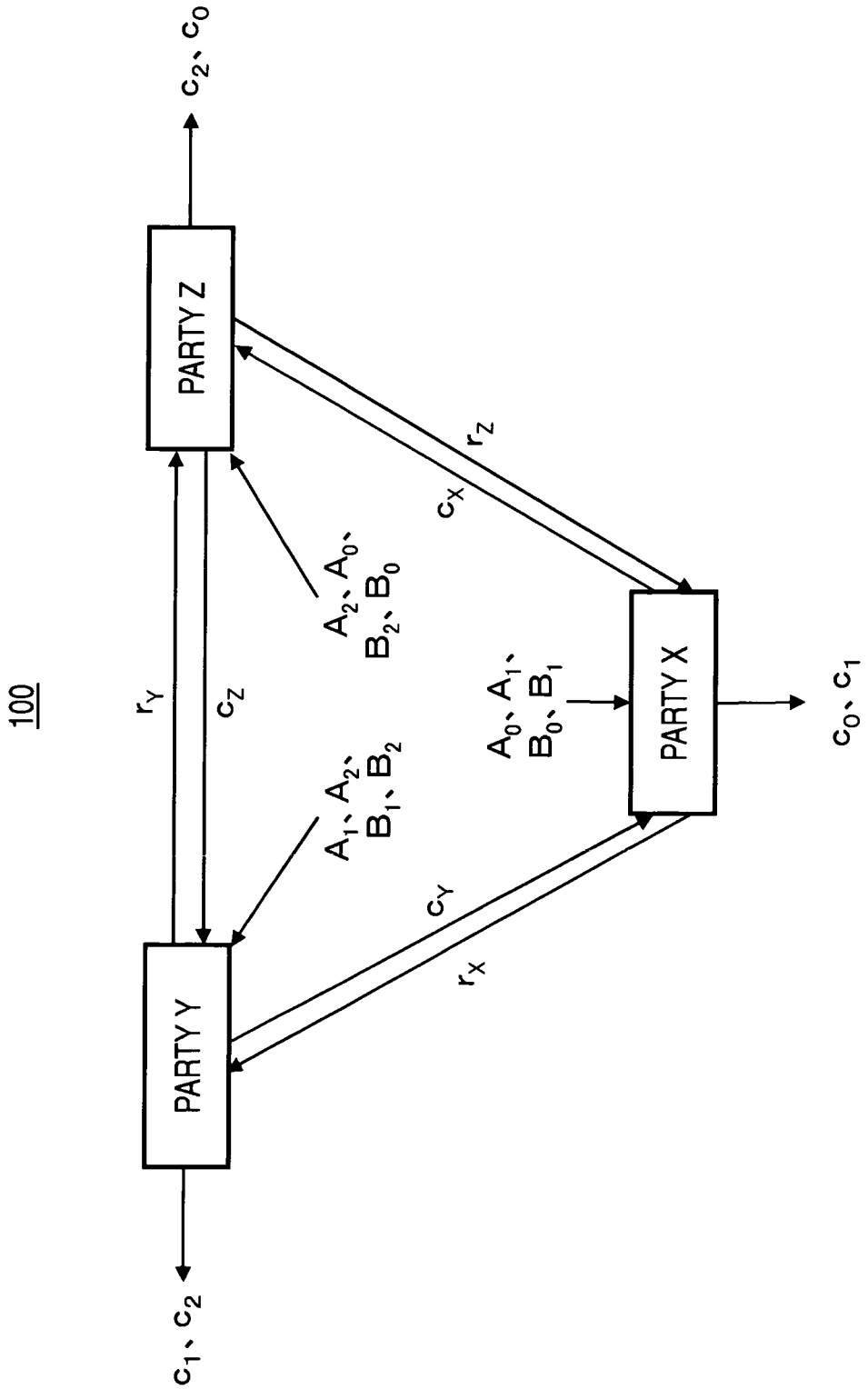
100
PARTY Z
PARTY X
PARTY Y
c_2、c_0
c_0、c_1
c_1、c_2
r_Z
c_X
r_Y
c_Z
A_2、A_0、
B_2、B_0
A_0、A_1、
B_0、B_1
A_1、A_2、
B_1、B_2
c_Y
r_X

FIG. 1

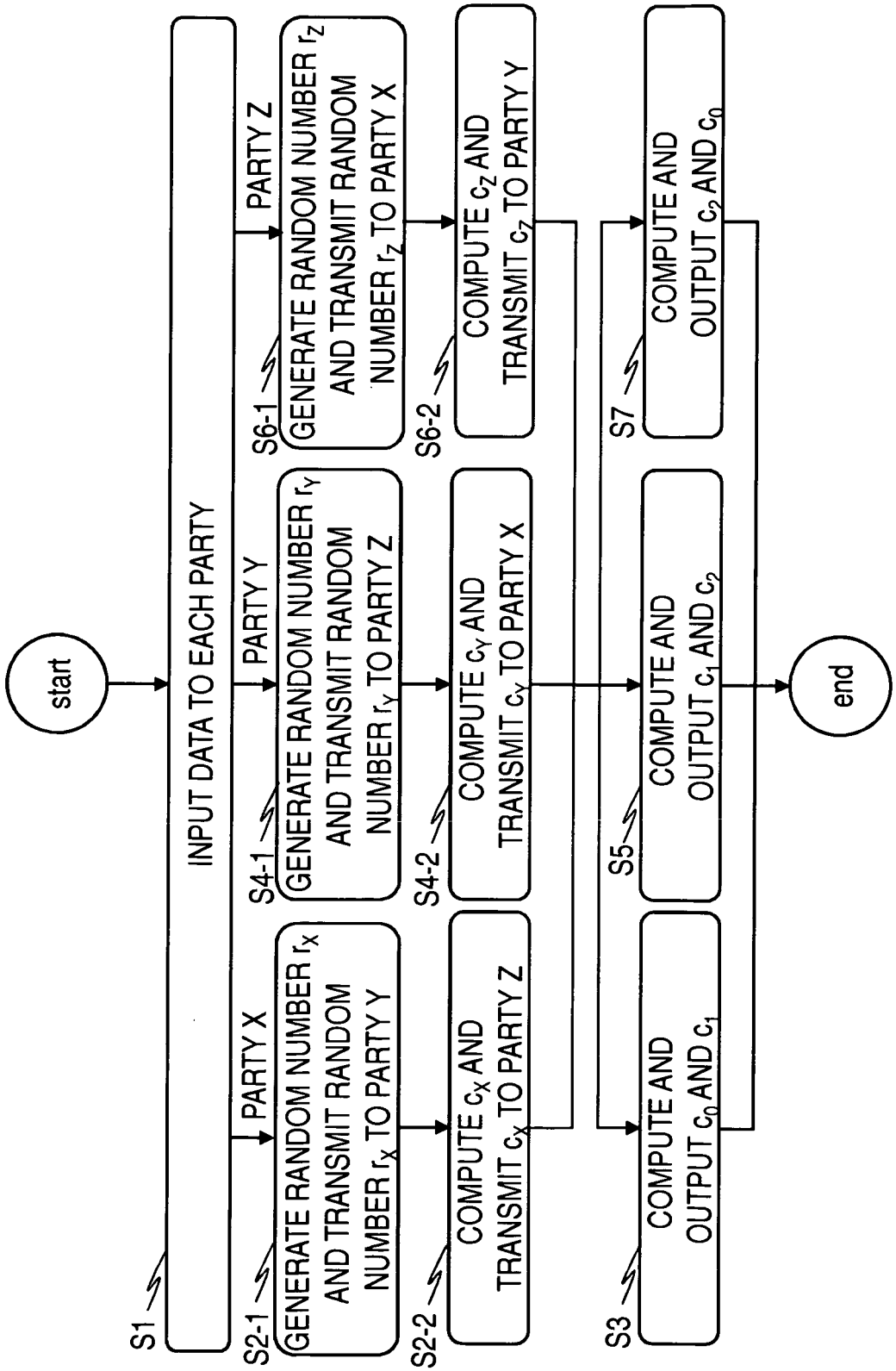
start
INPUT DATA TO EACH PARTY
S1
PARTY X
S2-1
GENERATE RANDOM NUMBER r_X AND TRANSMIT RANDOM NUMBER r_X TO PARTY Y
S2-2
COMPUTE c_X AND TRANSMIT c_X TO PARTY Z
PARTY Y
S4-1
GENERATE RANDOM NUMBER r_Y AND TRANSMIT RANDOM NUMBER r_Y TO PARTY Z
S4-2
COMPUTE c_Y AND TRANSMIT c_Y TO PARTY X
PARTY Z
S6-1
GENERATE RANDOM NUMBER r_Z AND TRANSMIT RANDOM NUMBER r_Z TO PARTY X
S6-2
COMPUTE c_Z AND TRANSMIT c_Z TO PARTY Y
S3
COMPUTE AND OUTPUT c_0 AND c_1
S5
COMPUTE AND OUTPUT c_1 AND c_2
S7
COMPUTE AND OUTPUT c_2 AND c_0
end

FIG. 2

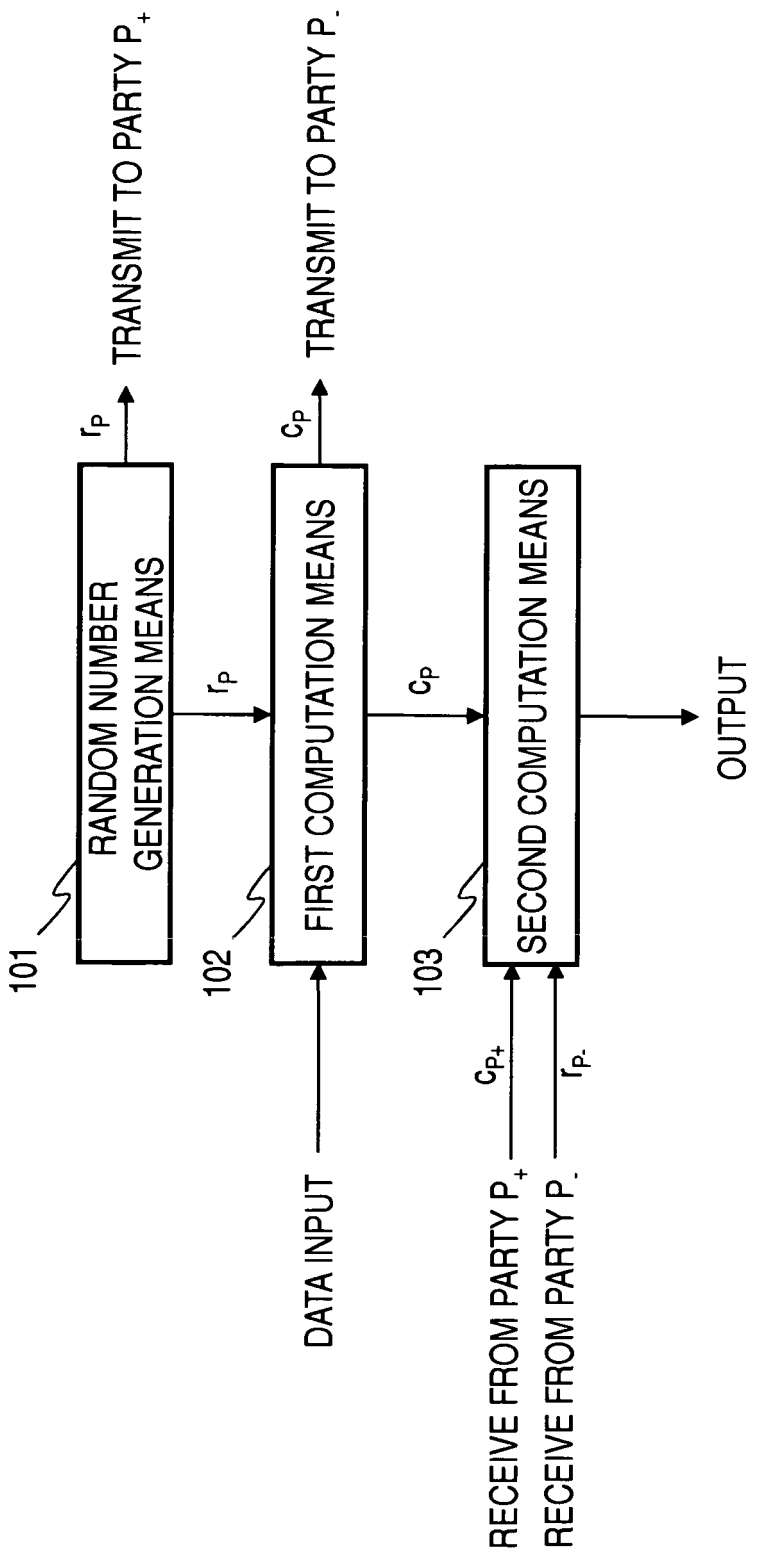
RANDOM NUMBER GENERATION MEANS
FIRST COMPUTATION MEANS
SECOND COMPUTATION MEANS
101
102
103
r_P
c_P
TRANSMIT TO PARTY P_+
TRANSMIT TO PARTY P_-
DATA INPUT
RECEIVE FROM PARTY P_+
RECEIVE FROM PARTY P_-
c_{P+}
r_{P-}
OUTPUT

FIG. 3

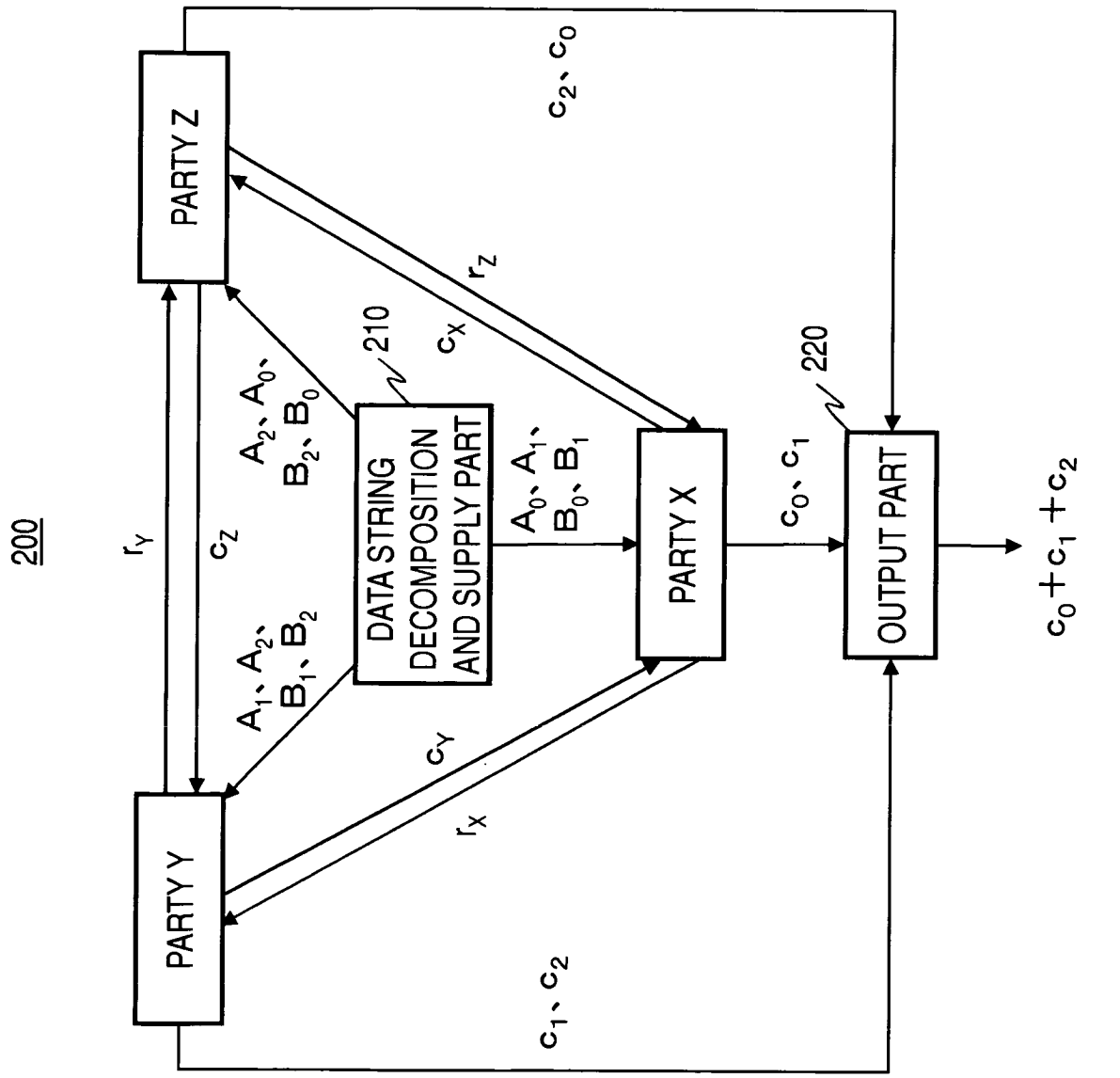
200
PARTY Z
PARTY Y
PARTY X
DATA STRING DECOMPOSITION AND SUPPLY PART
210
220
OUTPUT PART
r_Y
c_Z
r_Z
c_X
r_X
c_Y
A_2、A_0、B_2、B_0
A_1、A_2、B_1、B_2
A_0、A_1、B_0、B_1
c_0、c_1
c_2、c_0
c_1、c_2
$c_0+c_1+c_2$

FIG. 4

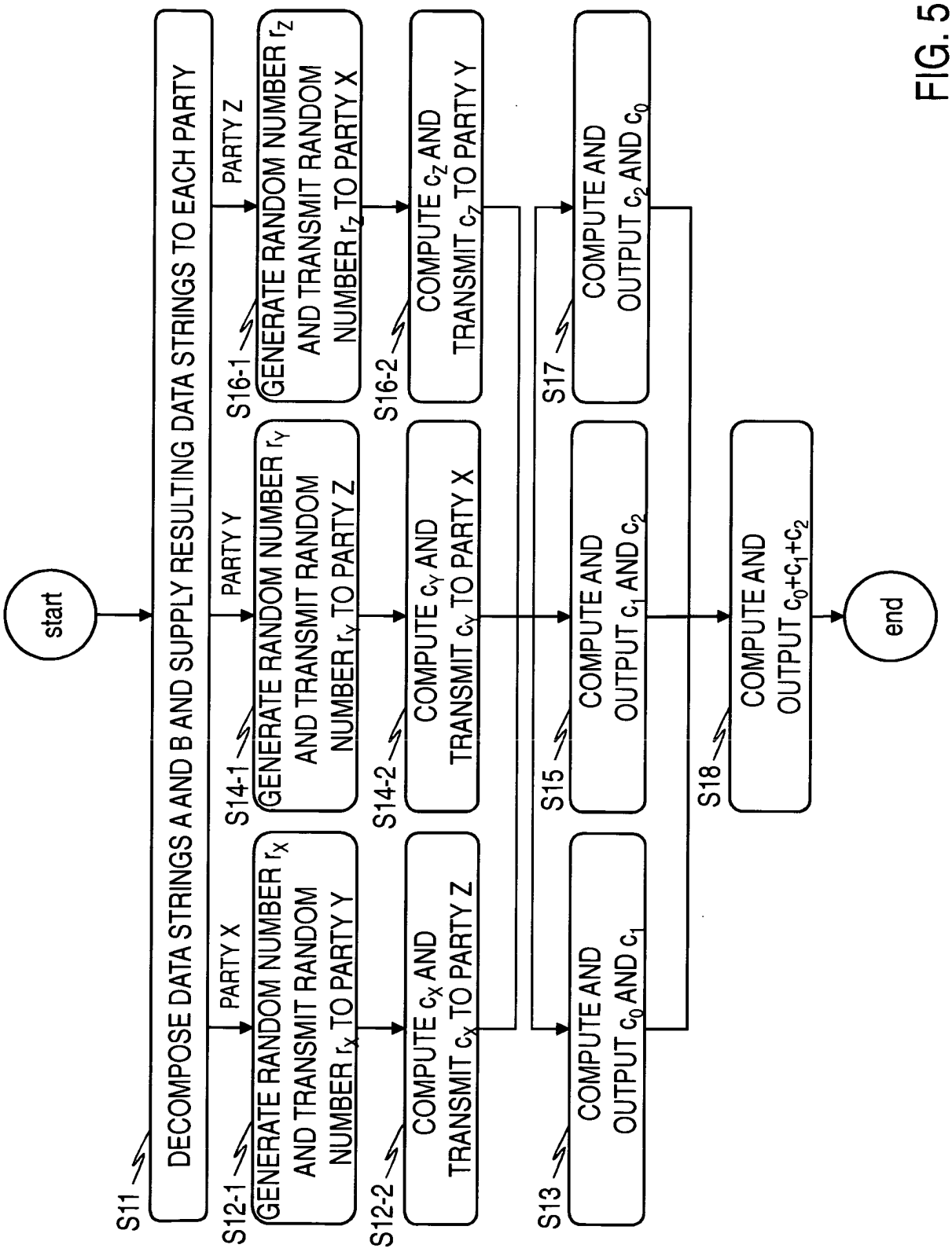
start
S11
DECOMPOSE DATA STRINGS A AND B AND SUPPLY RESULTING DATA STRINGS TO EACH PARTY
PARTY X
PARTY Y
PARTY Z
S12-1
GENERATE RANDOM NUMBER r_X AND TRANSMIT RANDOM NUMBER r_X TO PARTY Y
S14-1
GENERATE RANDOM NUMBER r_Y AND TRANSMIT RANDOM NUMBER r_Y TO PARTY Z
S16-1
GENERATE RANDOM NUMBER r_Z AND TRANSMIT RANDOM NUMBER r_Z TO PARTY X
S12-2
COMPUTE c_X AND TRANSMIT c_X TO PARTY Z
S14-2
COMPUTE c_Y AND TRANSMIT c_Y TO PARTY X
S16-2
COMPUTE c_Z AND TRANSMIT c_Z TO PARTY Y
S13
COMPUTE AND OUTPUT c_0 AND c_1
S15
COMPUTE AND OUTPUT c_1 AND c_2
S17
COMPUTE AND OUTPUT c_2 AND c_0
S18
COMPUTE AND OUTPUT $c_0+c_1+c_2$
end

FIG. 5

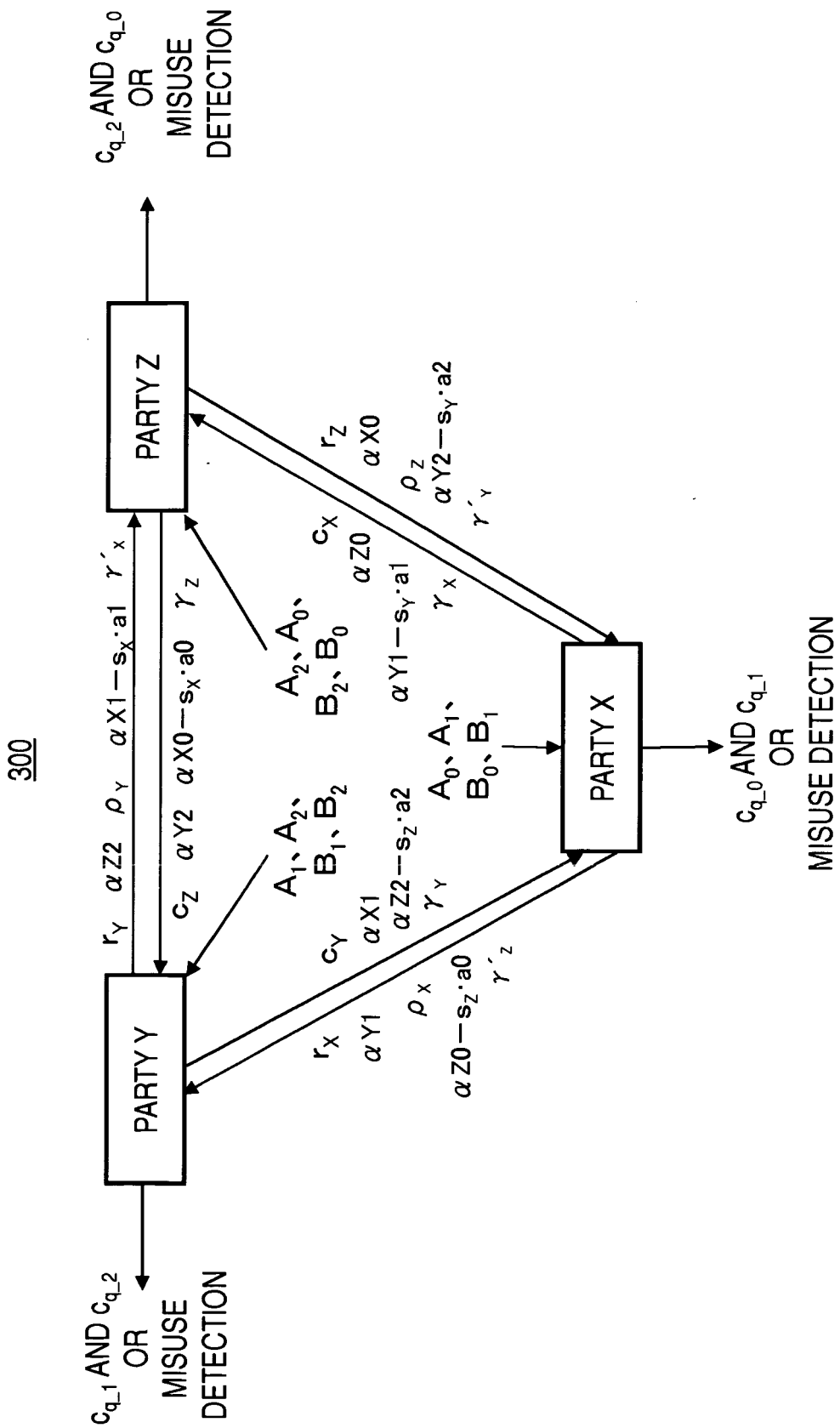
300
PARTY Z
PARTY Y
PARTY X
c_{q_2} AND c_{q_0} OR MISUSE DETECTION
c_{q_1} AND c_{q_2} OR MISUSE DETECTION
c_{q_0} AND c_{q_1} OR MISUSE DETECTION
r_Y $\alpha Z2$ ρ_Y $\alpha X1-s_X \cdot a1$ γ'_X
c_Z $\alpha Y2$ $\alpha X0-s_X \cdot a0$ γ_Z
A_1, A_2, B_1, B_2
A_2, A_0, B_2, B_0
c_Y $\alpha X1$ $\alpha Z2-s_Z \cdot a2$ γ_Y
A_0, A_1, B_0, B_1
r_X $\alpha Y1$ ρ_X $\alpha Z0-s_Z \cdot a0$ γ'_Z
c_X $\alpha Z0$ $\alpha Y1-s_Y \cdot a1$ γ_X
r_Z $\alpha X0$ ρ_Z $\alpha Y2-s_Y \cdot a2$ γ'_Y

FIG. 6

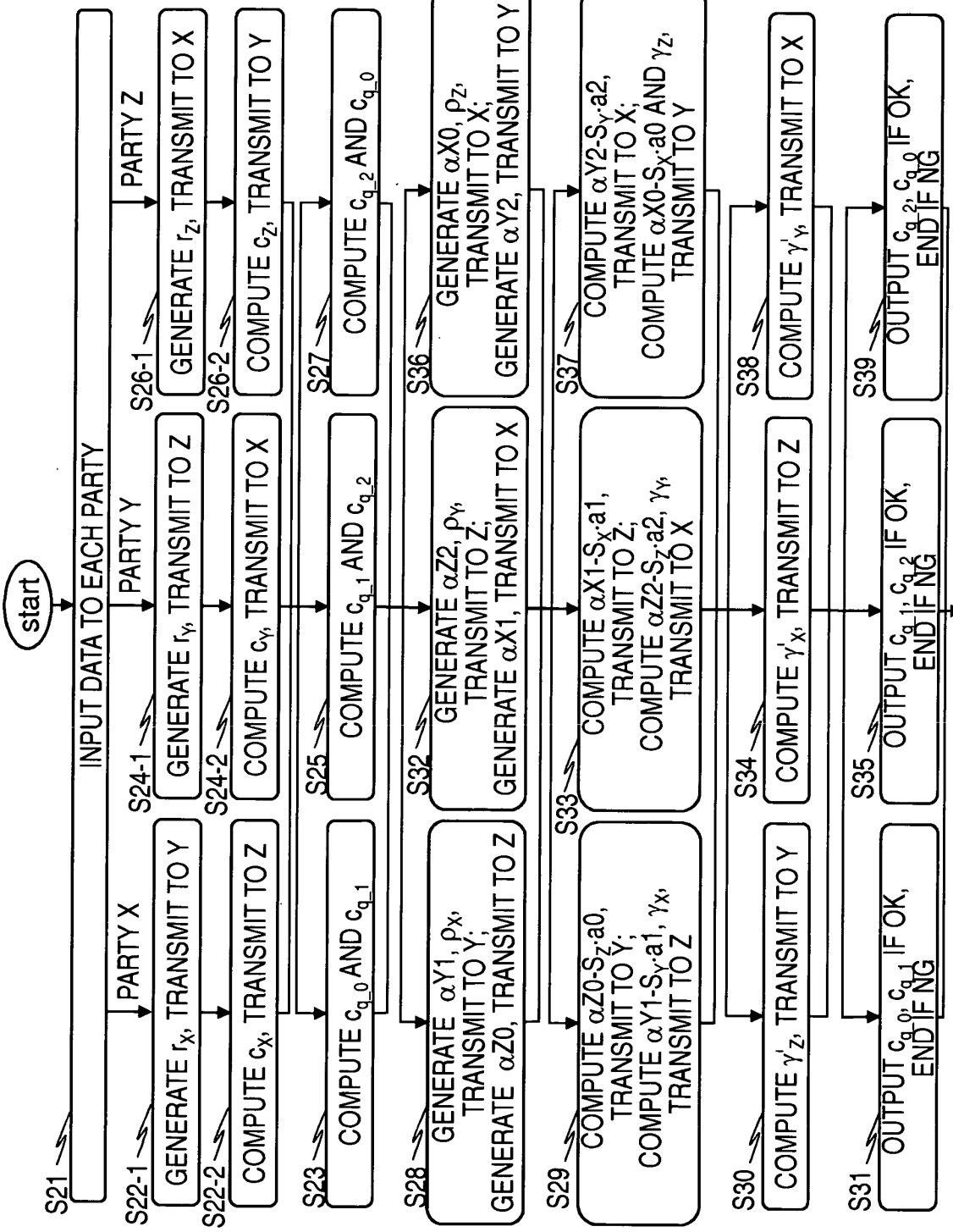
start
S21
INPUT DATA TO EACH PARTY
PARTY X
PARTY Y
PARTY Z
S22-1
GENERATE r_X, TRANSMIT TO Y
S24-1
GENERATE r_Y, TRANSMIT TO Z
S26-1
GENERATE r_Z, TRANSMIT TO X
S22-2
COMPUTE c_X, TRANSMIT TO Z
S24-2
COMPUTE c_Y, TRANSMIT TO X
S26-2
COMPUTE c_Z, TRANSMIT TO Y
S23
COMPUTE c_{q_0} AND c_{q_1}
S25
COMPUTE c_{q_1} AND c_{q_2}
S27
COMPUTE c_{q_2} AND c_{q_0}
S28
GENERATE $\alpha Y1, \rho_X$, TRANSMIT TO Y; GENERATE $\alpha Z0$, TRANSMIT TO Z
S32
GENERATE $\alpha Z2, \rho_Y$, TRANSMIT TO Z; GENERATE $\alpha X1$, TRANSMIT TO X
S36
GENERATE $\alpha X0, \rho_Z$, TRANSMIT TO X; GENERATE $\alpha Y2$, TRANSMIT TO Y
S29
COMPUTE $\alpha Z0\text{-}S_Z\cdot a0$, TRANSMIT TO Y; COMPUTE $\alpha Y1\text{-}S_Y\cdot a1, \gamma_X$, TRANSMIT TO Z
S33
COMPUTE $\alpha X1\text{-}S_X\cdot a1$, TRANSMIT TO Z; COMPUTE $\alpha Z2\text{-}S_Z\cdot a2, \gamma_Y$, TRANSMIT TO X
S37
COMPUTE $\alpha Y2\text{-}S_Y\cdot a2$, TRANSMIT TO X; COMPUTE $\alpha X0\text{-}S_X\cdot a0$ AND γ_Z, TRANSMIT TO Y
S30
COMPUTE γ'_Z, TRANSMIT TO Y
S34
COMPUTE γ'_X, TRANSMIT TO Z
S38
COMPUTE γ'_Y, TRANSMIT TO X
S31
OUTPUT c_{q_0}, c_{q_1} IF OK, END IF NG
S35
OUTPUT c_{q_1}, c_{q_2} IF OK, END IF NG
S39
OUTPUT c_{q_2}, c_{q_0} IF OK, END IF NG
end

FIG. 7

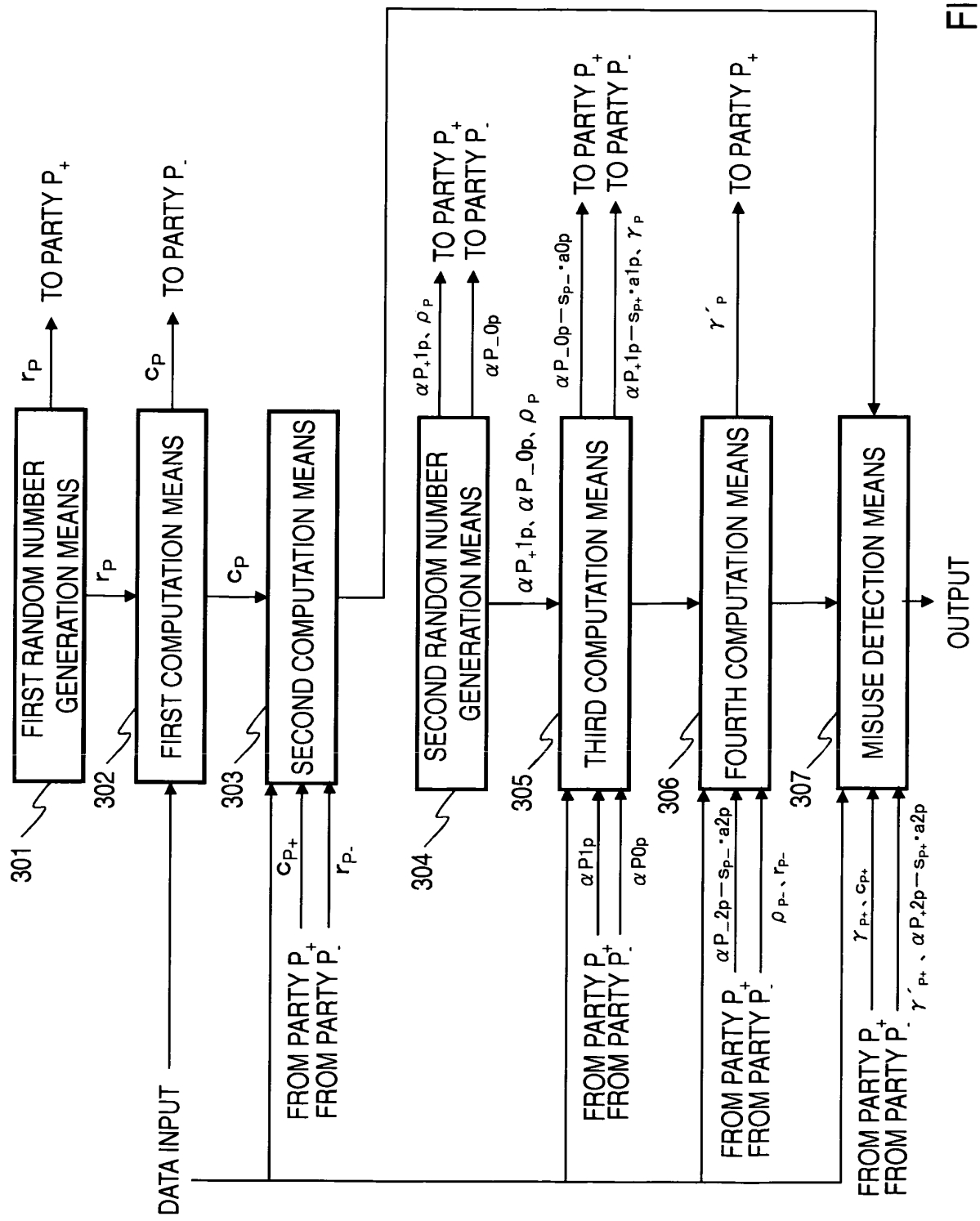
FIRST RANDOM NUMBER GENERATION MEANS
FIRST COMPUTATION MEANS
SECOND COMPUTATION MEANS
SECOND RANDOM NUMBER GENERATION MEANS
THIRD COMPUTATION MEANS
FOURTH COMPUTATION MEANS
MISUSE DETECTION MEANS
301
302
303
304
305
306
307
TO PARTY P+
TO PARTY P-
DATA INPUT
FROM PARTY P+
FROM PARTY P-
OUTPUT

FIG. 8

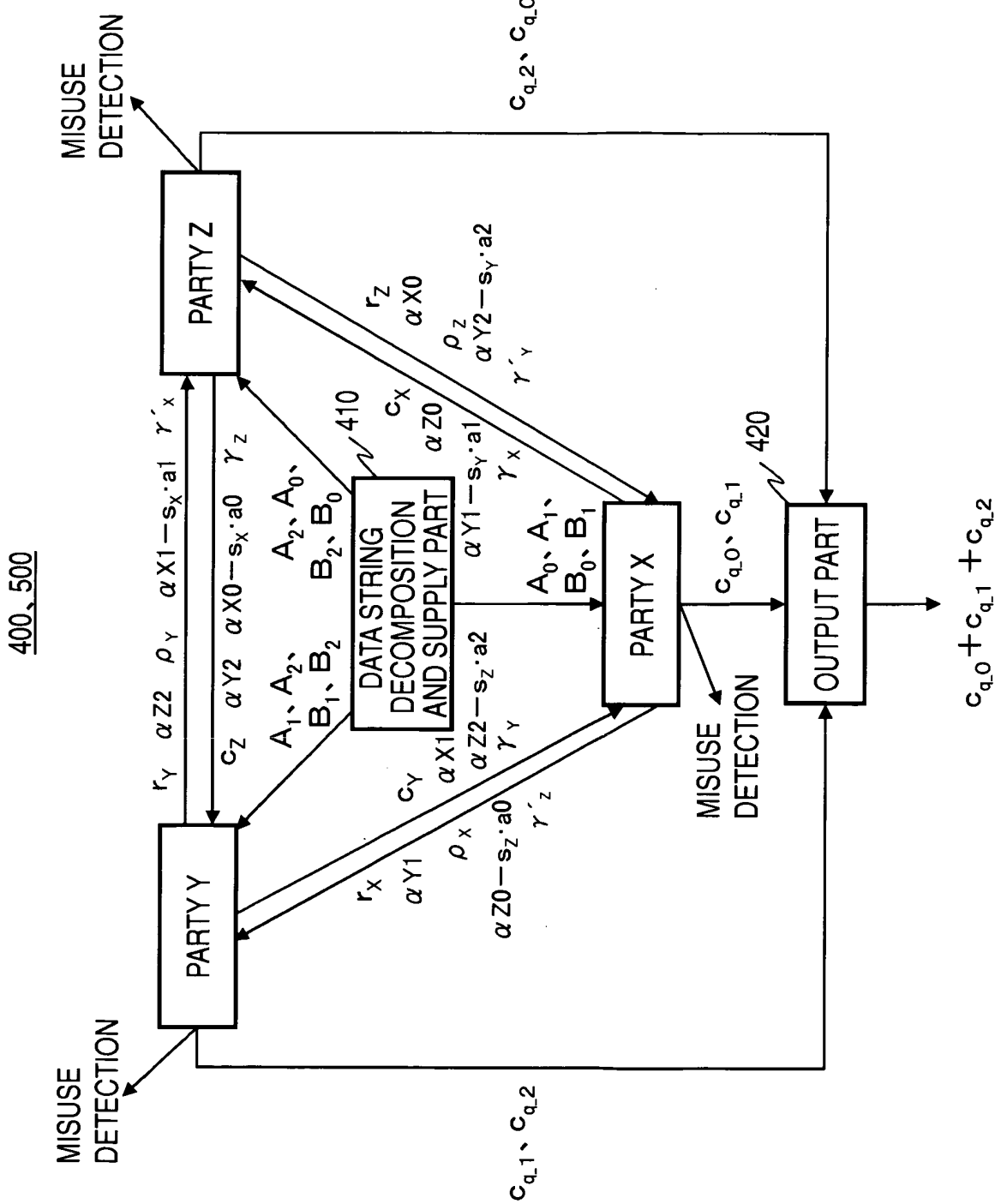
400、500
MISUSE DETECTION
PARTY Z
PARTY Y
PARTY X
DATA STRING DECOMPOSITION AND SUPPLY PART
410
420
OUTPUT PART
MISUSE DETECTION
MISUSE DETECTION
c_{q_2}、c_{q_0}
c_{q_1}、c_{q_2}
c_{q_0}、c_{q_1}
$c_{q\_0}+c_{q\_1}+c_{q\_2}$
r_Y $\alpha Z2$ ρ_Y $\alpha X1-s_X\cdot a1$ γ'_X
c_Z $\alpha Y2$ $\alpha X0-s_X\cdot a0$ γ_Z
A_1、A_2、B_1、B_2
A_2、A_0、B_2、B_0
c_X $\alpha Z0$ $\alpha Y1-s_Y\cdot a1$ γ_X
A_0、A_1、B_0、B_1
r_Z $\alpha X0$ ρ_Z $\alpha Y2-s_Y\cdot a2$ γ'_Y
c_Y $\alpha X1$ $\alpha Z2-s_Z\cdot a2$ γ_Y
r_X $\alpha Y1$ ρ_X $\alpha Z0-s_Z\cdot a0$ γ'_Z

FIG. 9

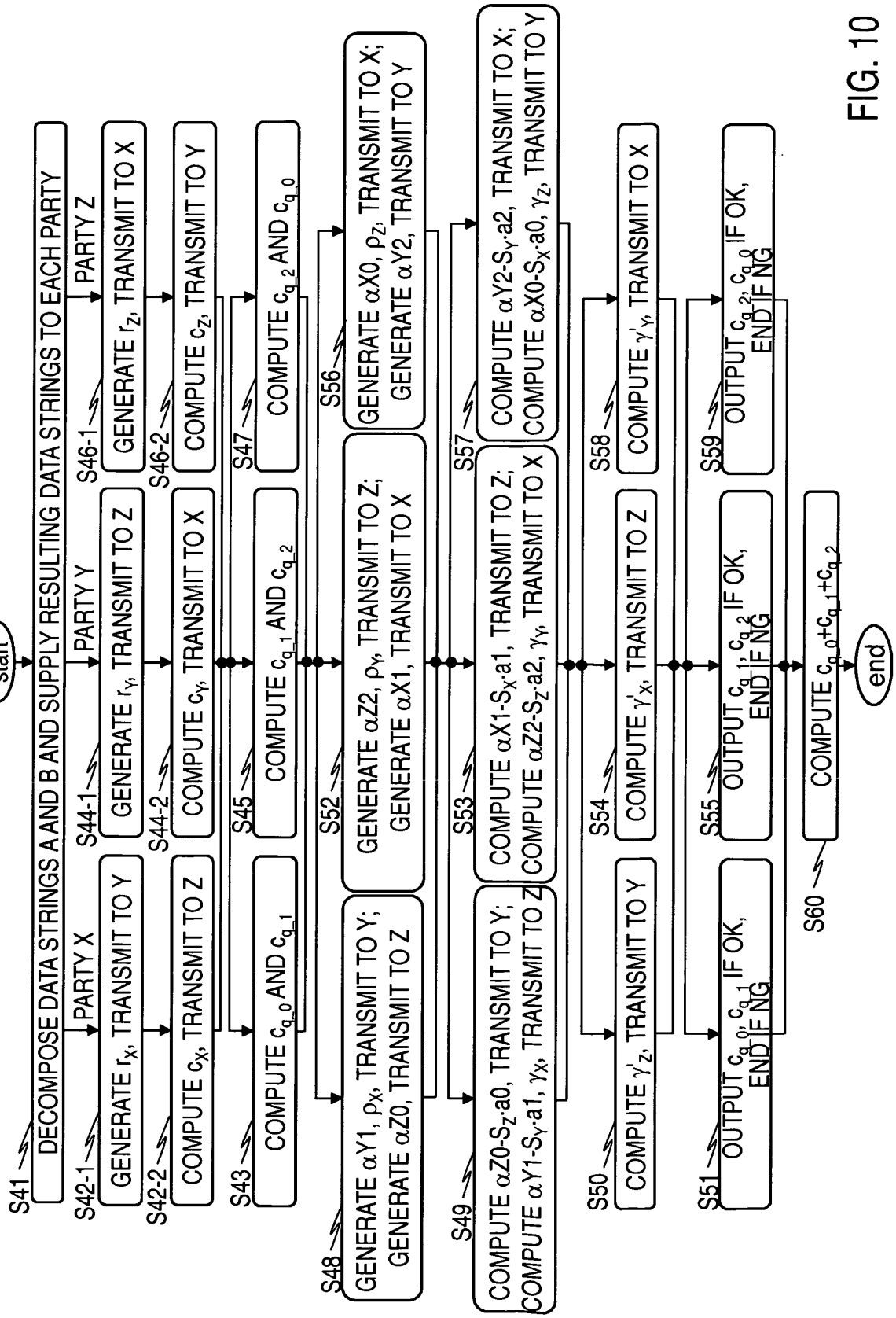
start
S41
DECOMPOSE DATA STRINGS A AND B AND SUPPLY RESULTING DATA STRINGS TO EACH PARTY
PARTY X
PARTY Y
PARTY Z
S42-1
GENERATE r_X, TRANSMIT TO Y
S44-1
GENERATE r_Y, TRANSMIT TO Z
S46-1
GENERATE r_Z, TRANSMIT TO X
S42-2
COMPUTE c_X, TRANSMIT TO Z
S44-2
COMPUTE c_Y, TRANSMIT TO X
S46-2
COMPUTE c_Z, TRANSMIT TO Y
S43
COMPUTE c_{q_0} AND c_{q_1}
S45
COMPUTE c_{q_1} AND c_{q_2}
S47
COMPUTE c_{q_2} AND c_{q_0}
S48
GENERATE $\alpha Y1$, ρ_X, TRANSMIT TO Y; GENERATE $\alpha Z0$, TRANSMIT TO Z
S52
GENERATE $\alpha Z2$, ρ_Y, TRANSMIT TO Z; GENERATE $\alpha X1$, TRANSMIT TO X
S56
GENERATE $\alpha X0$, ρ_Z, TRANSMIT TO X; GENERATE $\alpha Y2$, TRANSMIT TO Y
S49
COMPUTE $\alpha Z0$-S_Z·a0, TRANSMIT TO Y; COMPUTE $\alpha Y1$-S_Y·a1, γ_X, TRANSMIT TO Z
S53
COMPUTE $\alpha X1$-S_X·a1, TRANSMIT TO Z; COMPUTE $\alpha Z2$-S_Z·a2, γ_Y, TRANSMIT TO X
S57
COMPUTE $\alpha Y2$-S_Y·a2, TRANSMIT TO X; COMPUTE $\alpha X0$-S_X·a0, γ_Z, TRANSMIT TO Y
S50
COMPUTE γ'_Z, TRANSMIT TO Y
S54
COMPUTE γ'_X, TRANSMIT TO Z
S58
COMPUTE γ'_Y, TRANSMIT TO X
S51
OUTPUT c_{q_0}, c_{q_1} IF OK, END IF NG
S55
OUTPUT c_{q_1}, c_{q_2} IF OK, END IF NG
S59
OUTPUT c_{q_2}, c_{q_0} IF OK, END IF NG
S60
COMPUTE c_{q_0}+c_{q_1}+c_{q_2}
end

FIG. 10

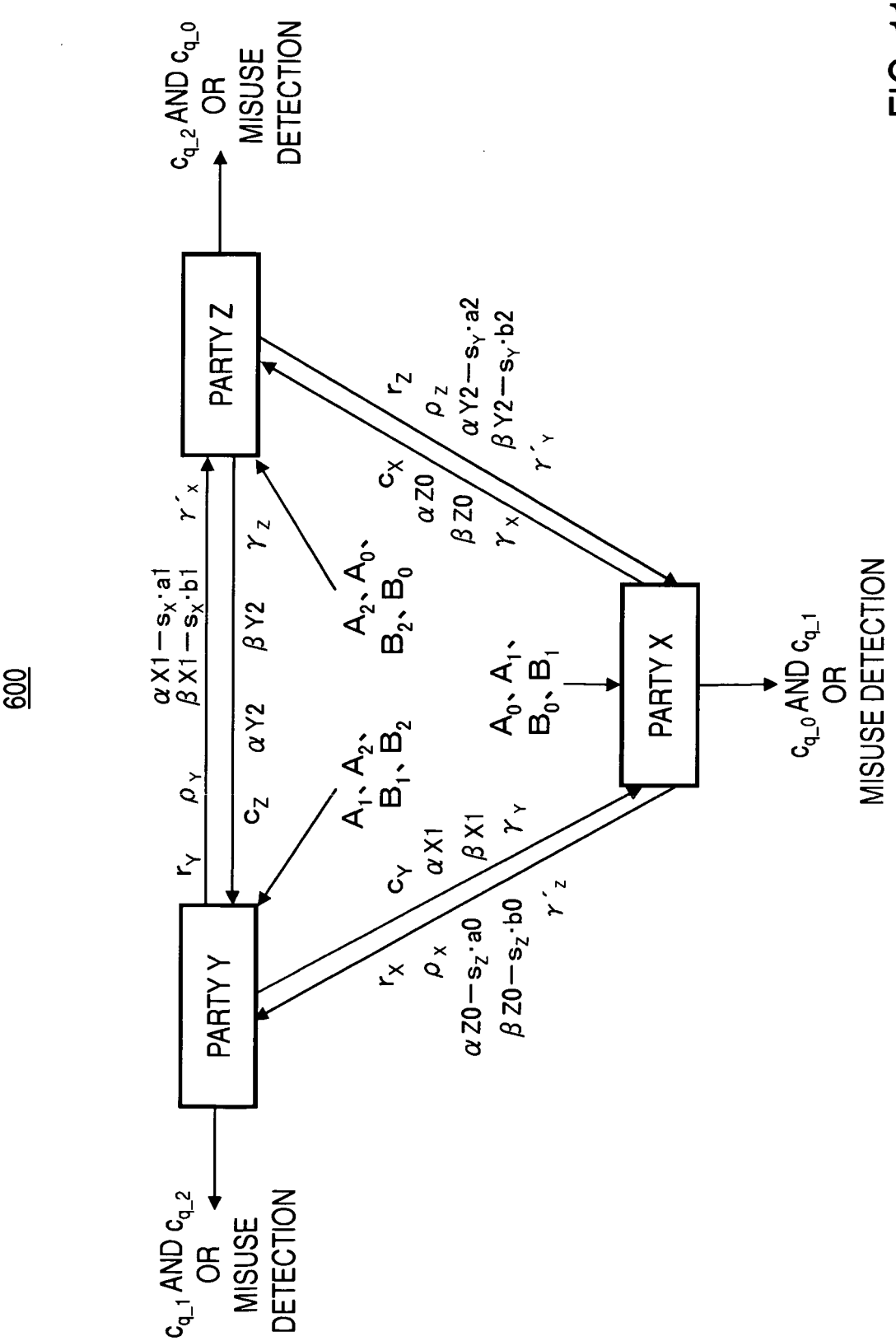
600
PARTY Z
PARTY Y
PARTY X
c_{q_2} AND c_{q_0} OR MISUSE DETECTION
c_{q_1} AND c_{q_2} OR MISUSE DETECTION
c_{q_0} AND c_{q_1} OR MISUSE DETECTION
$\alpha X1 - s_X \cdot a1$
$\beta X1 - s_X \cdot b1$
r_Y
ρ_Y
γ'_X
γ_Z
c_Z
$\alpha Y2$
$\beta Y2$
A_2, A_0, B_2, B_0
A_1, A_2, B_1, B_2
c_X
$\alpha Z0$
$\beta Z0$
γ_X
r_Z
ρ_Z
$\alpha Y2 - s_Y \cdot a2$
$\beta Y2 - s_Y \cdot b2$
γ'_Y
A_0, A_1, B_0, B_1
c_Y
$\alpha X1$
$\beta X1$
γ_Y
r_X
ρ_X
$\alpha Z0 - s_Z \cdot a0$
$\beta Z0 - s_Z \cdot b0$
γ'_Z

FIG. 11

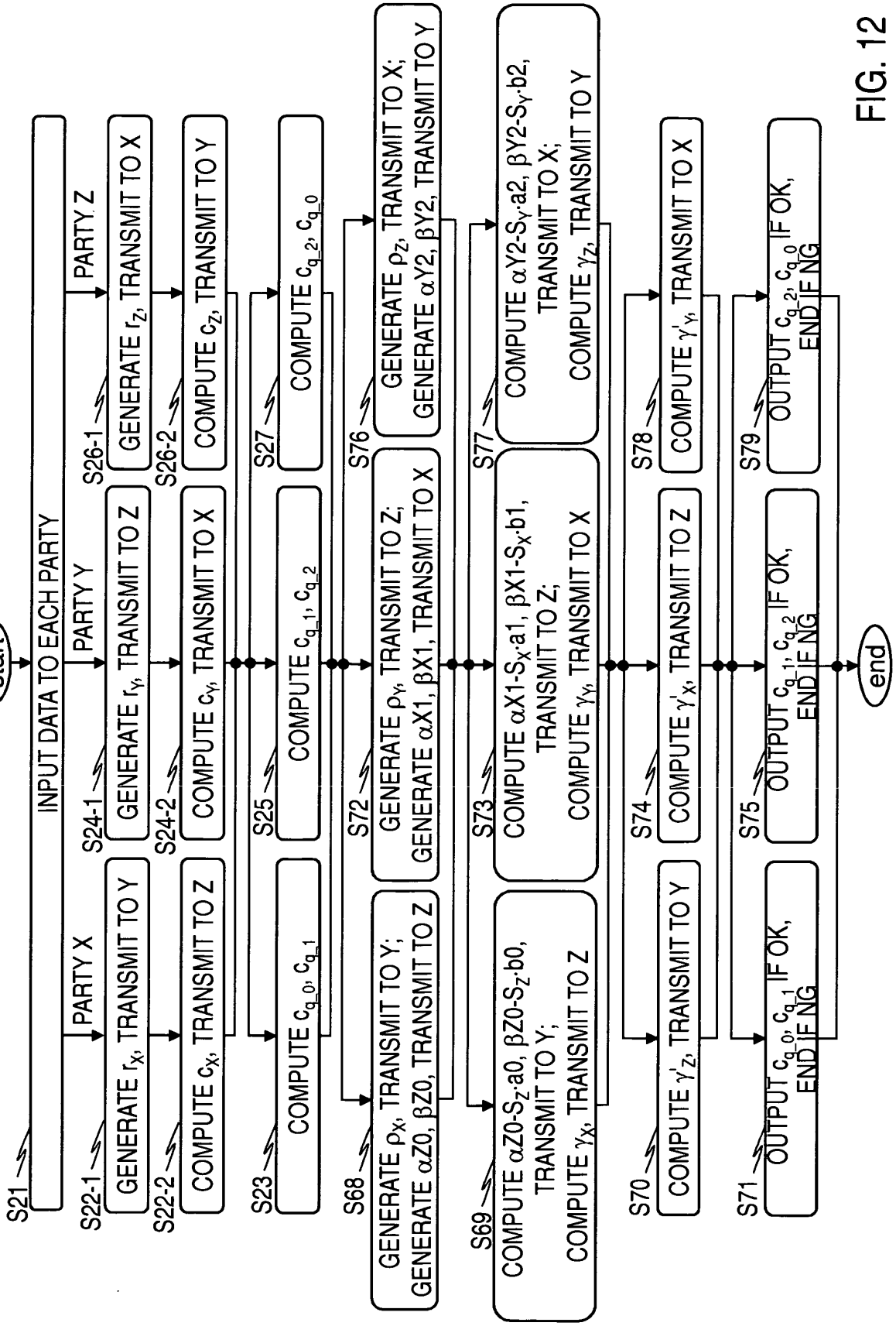
start
INPUT DATA TO EACH PARTY
PARTY X
PARTY Y
PARTY Z
S21
S22-1
GENERATE r_X, TRANSMIT TO Y
S22-2
COMPUTE c_X, TRANSMIT TO Z
S23
COMPUTE c_{q_0}, c_{q_1}
S24-1
GENERATE r_Y, TRANSMIT TO Z
S24-2
COMPUTE c_Y, TRANSMIT TO X
S25
COMPUTE c_{q_1}, c_{q_2}
S26-1
GENERATE r_Z, TRANSMIT TO X
S26-2
COMPUTE c_Z, TRANSMIT TO Y
S27
COMPUTE c_{q_2}, c_{q_0}
S68
GENERATE ρ_X, TRANSMIT TO Y;
GENERATE $\alpha Z0$, $\beta Z0$, TRANSMIT TO Z
S69
COMPUTE $\alpha Z0$-S_Z·a0, $\beta Z0$-S_Z·b0,
TRANSMIT TO Y;
COMPUTE γ_X, TRANSMIT TO Z
S70
COMPUTE γ'_Z, TRANSMIT TO Y
S71
OUTPUT c_{q_0}, c_{q_1} IF OK,
END IF NG
S72
GENERATE ρ_Y, TRANSMIT TO Z;
GENERATE $\alpha X1$, $\beta X1$, TRANSMIT TO X
S73
COMPUTE $\alpha X1$-S_X·a1, $\beta X1$-S_X·b1,
TRANSMIT TO Z;
COMPUTE γ_Y, TRANSMIT TO X
S74
COMPUTE γ'_X, TRANSMIT TO Z
S75
OUTPUT c_{q_1}, c_{q_2} IF OK,
END IF NG
S76
GENERATE ρ_Z, TRANSMIT TO X;
GENERATE $\alpha Y2$, $\beta Y2$, TRANSMIT TO Y
S77
COMPUTE $\alpha Y2$-S_Y·a2, $\beta Y2$-S_Y·b2,
TRANSMIT TO X;
COMPUTE γ_Z, TRANSMIT TO Y
S78
COMPUTE γ'_Y, TRANSMIT TO X
S79
OUTPUT c_{q_2}, c_{q_0} IF OK,
END IF NG
end

FIG. 12

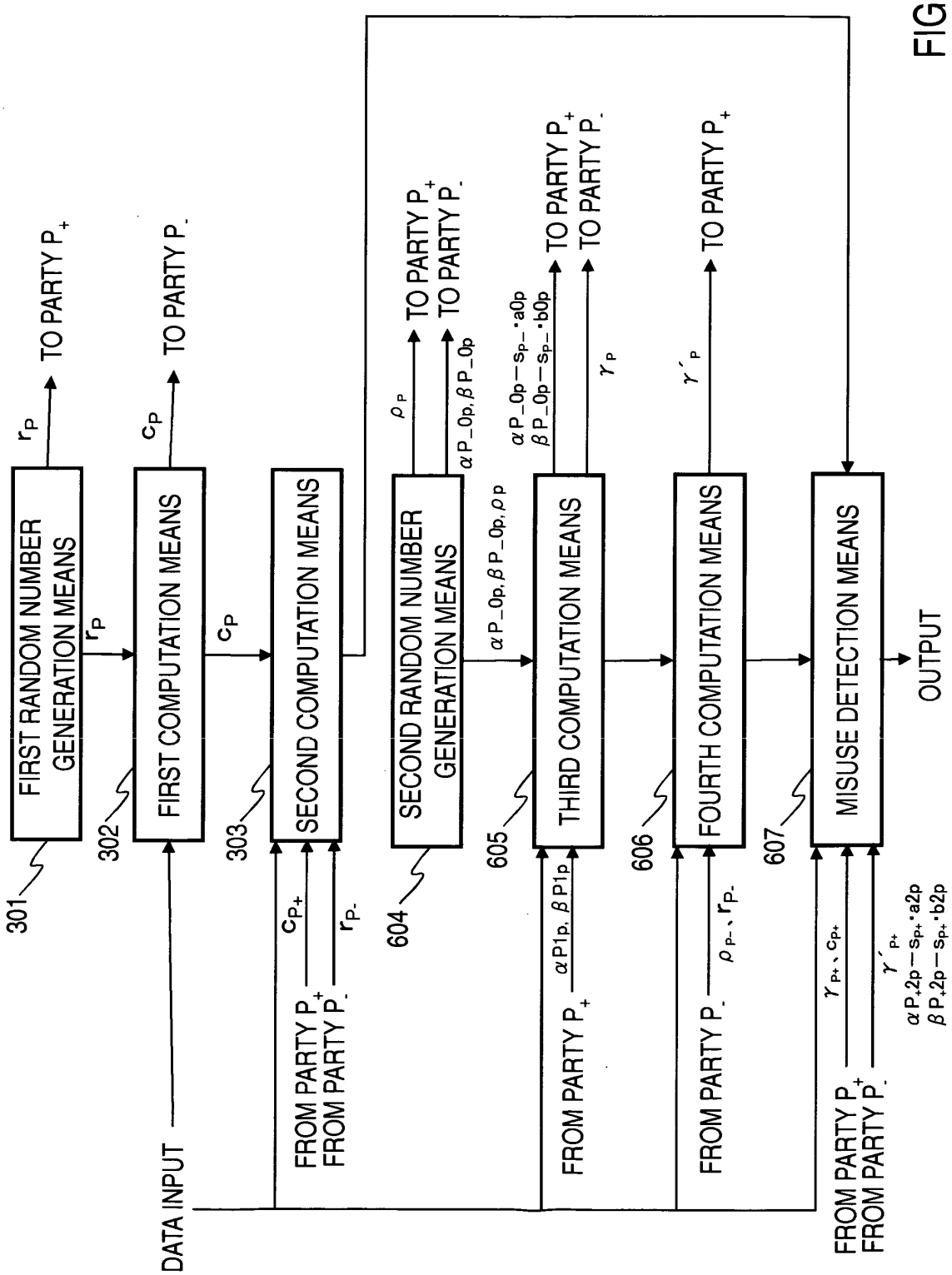
FIRST RANDOM NUMBER GENERATION MEANS
FIRST COMPUTATION MEANS
SECOND COMPUTATION MEANS
SECOND RANDOM NUMBER GENERATION MEANS
THIRD COMPUTATION MEANS
FOURTH COMPUTATION MEANS
MISUSE DETECTION MEANS
DATA INPUT
OUTPUT
TO PARTY P+
TO PARTY P-
FROM PARTY P+
FROM PARTY P-
301
302
303
604
605
606
607

FIG.13

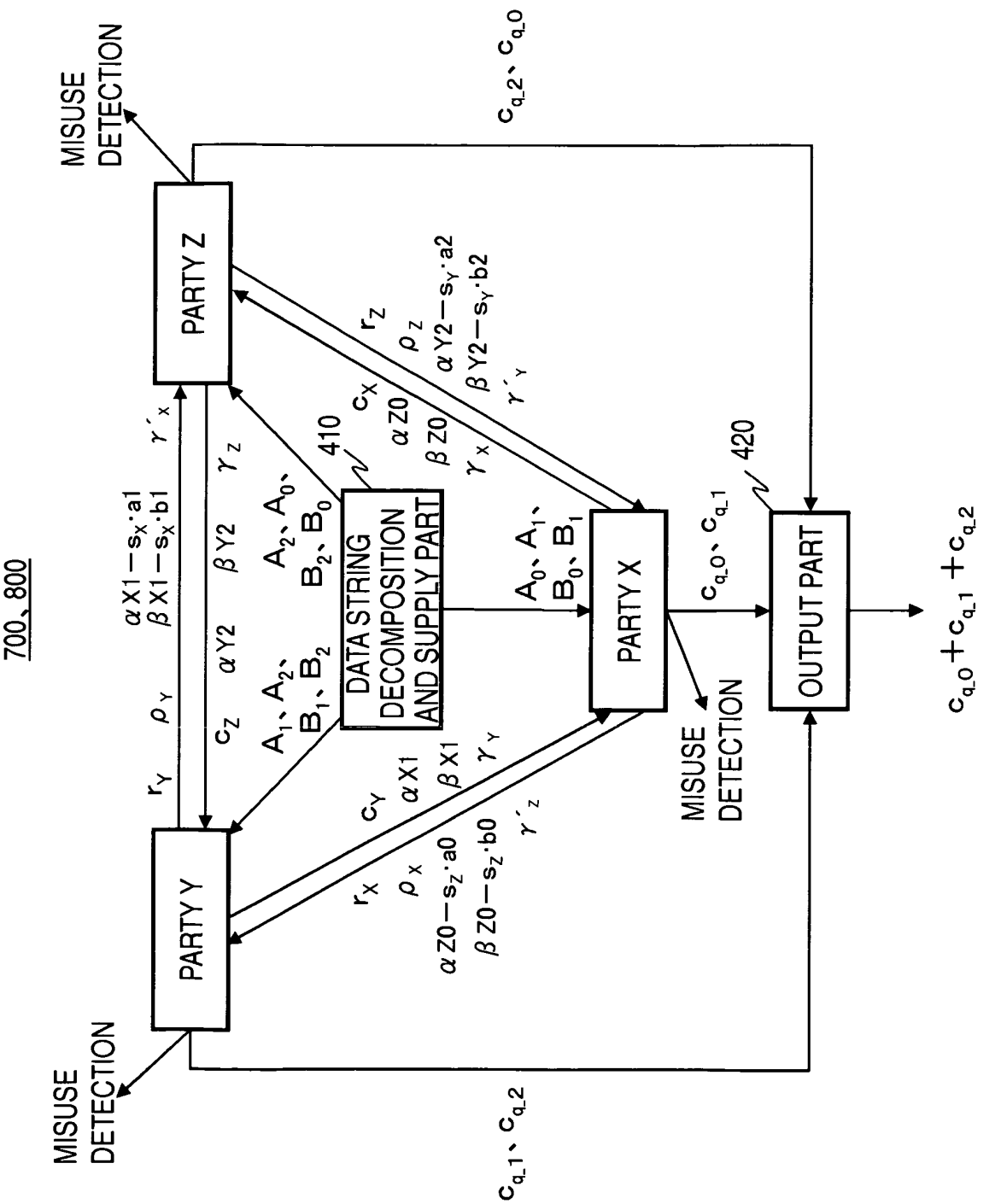
700、800
MISUSE DETECTION
PARTY Z
PARTY Y
PARTY X
DATA STRING DECOMPOSITION AND SUPPLY PART
410
420
OUTPUT PART
MISUSE DETECTION
MISUSE DETECTION
c_{q_2}、c_{q_0}
c_{q_1}、c_{q_2}
$c_{q\_0}+c_{q\_1}+c_{q\_2}$
c_{q_0}、c_{q_1}
A_0、A_1、B_0、B_1
A_1、A_2、B_1、B_2
A_2、A_0、B_2、B_0
c_X $\alpha Z0$ $\beta Z0$ r_X
c_Y $\alpha X1$ $\beta X1$ r_Y
c_Z $\alpha Y2$ $\beta Y2$ r_Z
r_X ρ_X $\alpha Z0-s_Z\cdot a0$ $\beta Z0-s_Z\cdot b0$ r'_Z
r_Y ρ_Y $\alpha X1-s_X\cdot a1$ $\beta X1-s_X\cdot b1$ r'_X
r_Z ρ_Z $\alpha Y2-s_Y\cdot a2$ $\beta Y2-s_Y\cdot b2$ r'_Y

FIG. 14

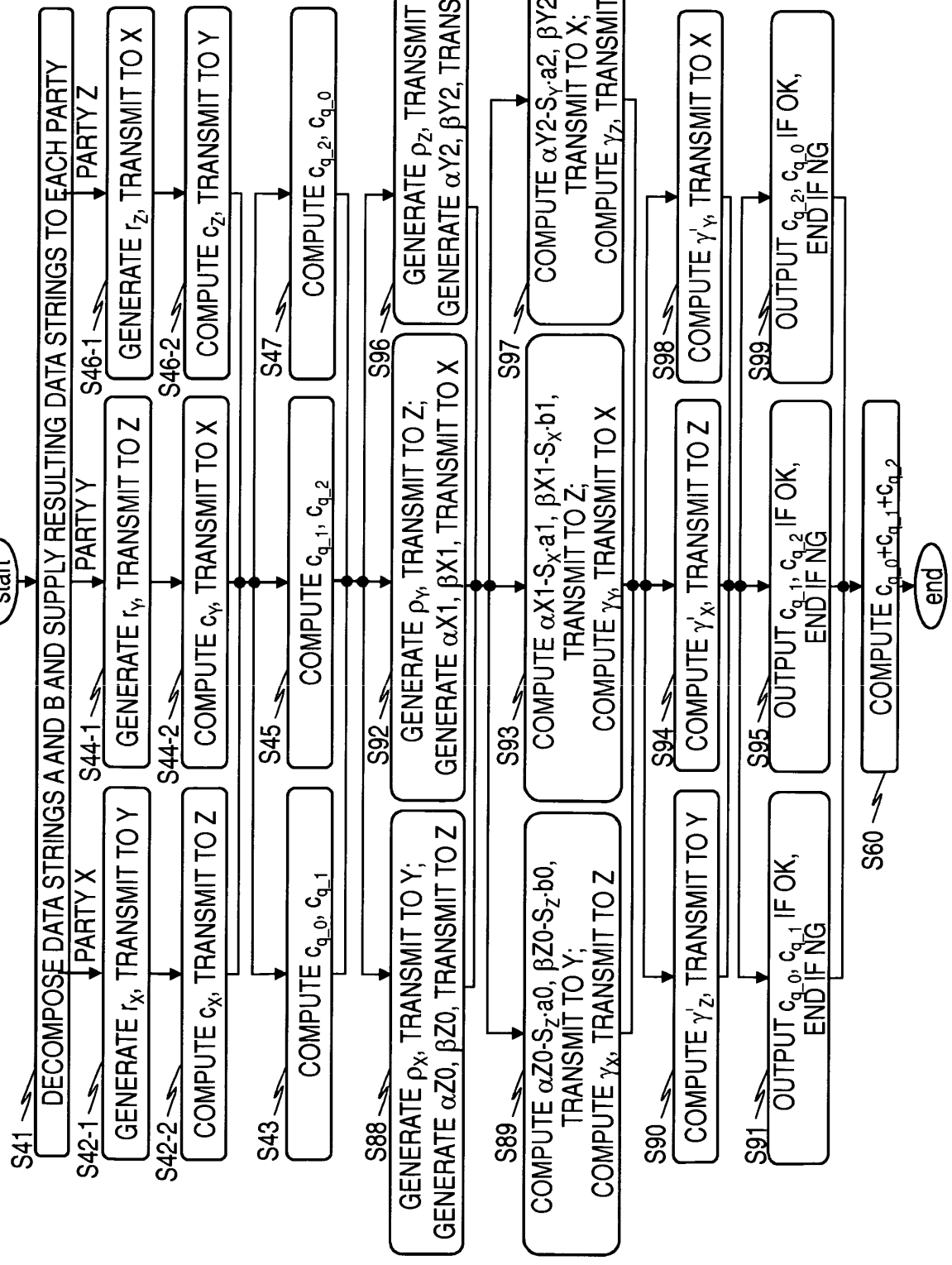
start
S41
DECOMPOSE DATA STRINGS A AND B AND SUPPLY RESULTING DATA STRINGS TO EACH PARTY
PARTY X
PARTY Y
PARTY Z
S42-1
GENERATE r_X, TRANSMIT TO Y
S44-1
GENERATE r_Y, TRANSMIT TO Z
S46-1
GENERATE r_Z, TRANSMIT TO X
S42-2
COMPUTE c_X, TRANSMIT TO Z
S44-2
COMPUTE c_Y, TRANSMIT TO X
S46-2
COMPUTE c_Z, TRANSMIT TO Y
S43
COMPUTE c_{q_0}, c_{q_1}
S45
COMPUTE c_{q_1}, c_{q_2}
S47
COMPUTE c_{q_2}, c_{q_0}
S88
GENERATE ρ_X, TRANSMIT TO Y;
GENERATE $\alpha Z0$, $\beta Z0$, TRANSMIT TO Z
S92
GENERATE ρ_Y, TRANSMIT TO Z;
GENERATE $\alpha X1$, $\beta X1$, TRANSMIT TO X
S96
GENERATE ρ_Z, TRANSMIT TO X;
GENERATE $\alpha Y2$, $\beta Y2$, TRANSMIT TO Y
S89
COMPUTE $\alpha Z0$-S_Z·a0, $\beta Z0$-S_Z·b0,
TRANSMIT TO Y;
COMPUTE γ_X, TRANSMIT TO Z
S93
COMPUTE $\alpha X1$-S_X·a1, $\beta X1$-S_X·b1,
TRANSMIT TO Z;
COMPUTE γ_Y, TRANSMIT TO X
S97
COMPUTE $\alpha Y2$-S_Y·a2, $\beta Y2$-S_Y·b2,
TRANSMIT TO X;
COMPUTE γ_Z, TRANSMIT TO Y
S90
COMPUTE γ'_Z, TRANSMIT TO Y
S94
COMPUTE γ'_X, TRANSMIT TO Z
S98
COMPUTE γ'_Y, TRANSMIT TO X
S91
OUTPUT c_{q_0}, c_{q_1} IF OK,
END IF NG
S95
OUTPUT c_{q_1}, c_{q_2} IF OK,
END IF NG
S99
OUTPUT c_{q_2}, c_{q_0} IF OK,
END IF NG
S60
COMPUTE c_{q_0}+c_{q_1}+c_{q_2}
end

FIG. 15

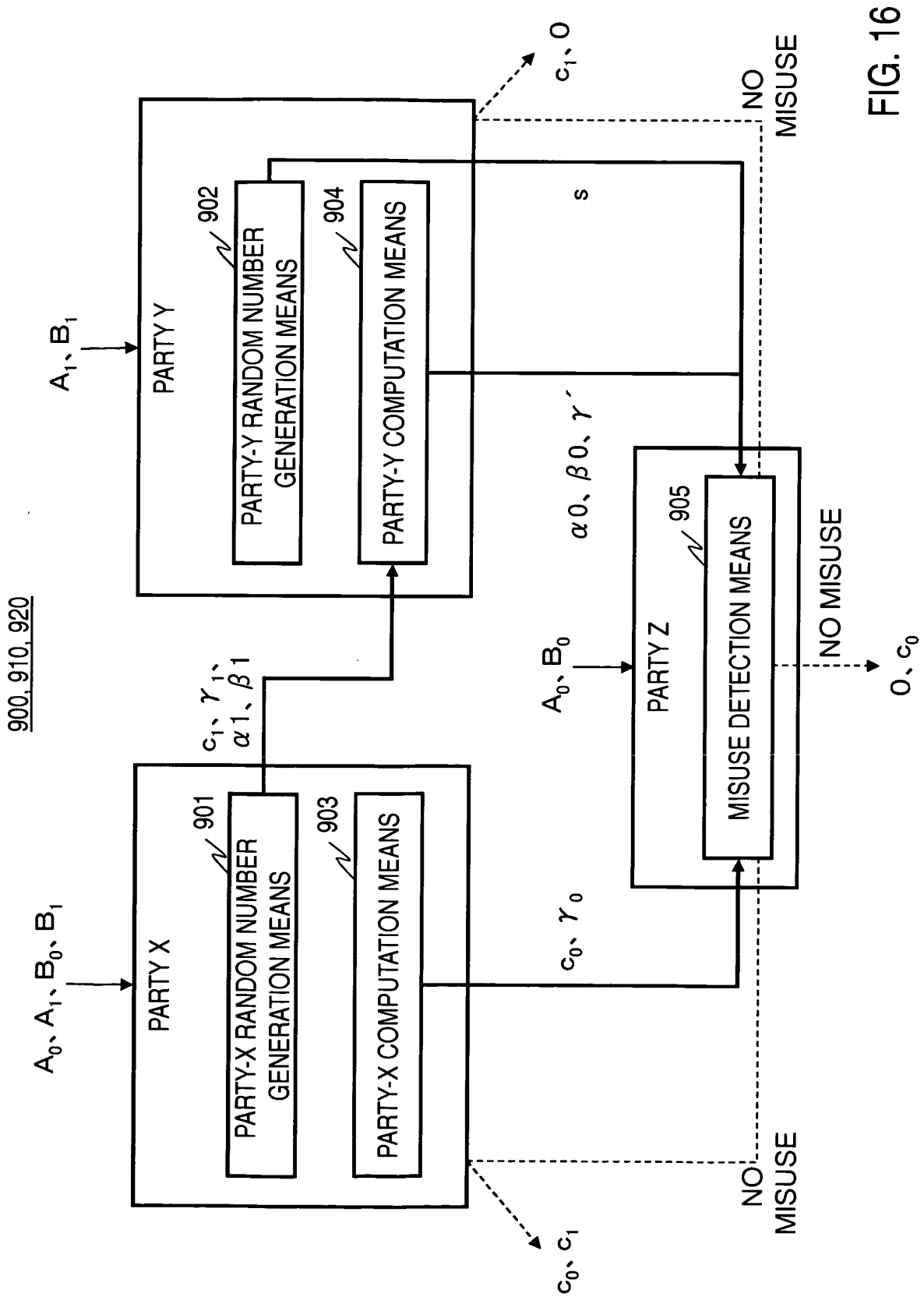
900, 910, 920
PARTY X
PARTY Y
PARTY Z
PARTY-X RANDOM NUMBER GENERATION MEANS
PARTY-Y RANDOM NUMBER GENERATION MEANS
PARTY-X COMPUTATION MEANS
PARTY-Y COMPUTATION MEANS
MISUSE DETECTION MEANS
901
902
903
904
905
A0、A1、B0、B1
A1、B1
A0、B0
c1、γ1、α1、β1
c0、γ0
α0、β0、γ'
s
c1、O
c0、c1
O、c0
NO MISUSE
NO MISUSE
NO MISUSE

FIG. 16

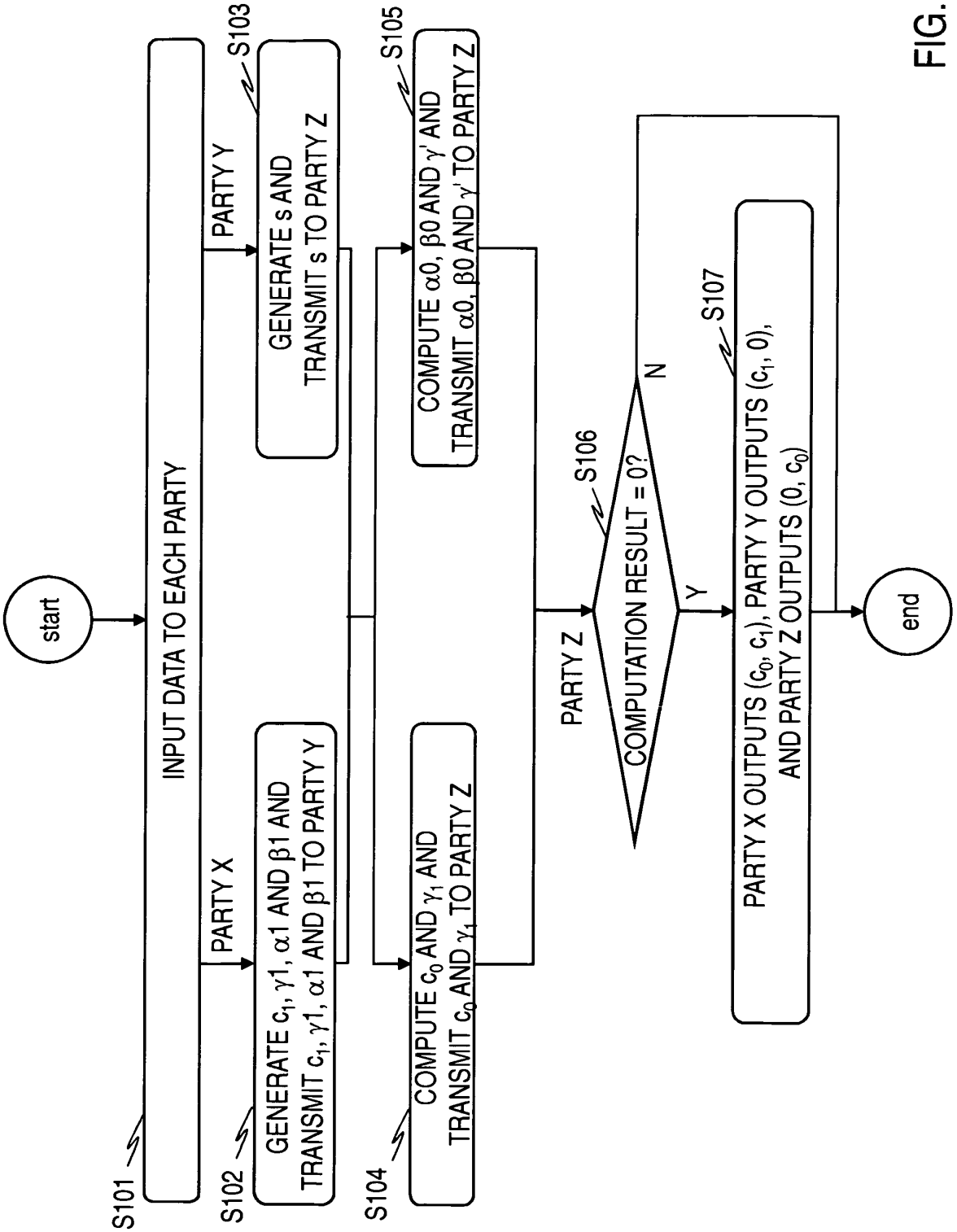
start
INPUT DATA TO EACH PARTY
S101
PARTY X
GENERATE c_1, $\gamma 1$, $\alpha 1$ AND $\beta 1$ AND TRANSMIT c_1, $\gamma 1$, $\alpha 1$ AND $\beta 1$ TO PARTY Y
S102
PARTY Y
S103
GENERATE s AND TRANSMIT s TO PARTY Z
PARTY Z
S104
COMPUTE c_0 AND γ_1 AND TRANSMIT c_0 AND γ_1 TO PARTY Z
S105
COMPUTE $\alpha 0$, $\beta 0$ AND γ' AND TRANSMIT $\alpha 0$, $\beta 0$ AND γ' TO PARTY Z
S106
COMPUTATION RESULT = 0?
N
Y
S107
PARTY X OUTPUTS (c_0, c_1), PARTY Y OUTPUTS (c_1, 0), AND PARTY Z OUTPUTS (0, c_0)
end

FIG. 17