(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 4 月 15 日(15.04.2010)

PCT

(10) 国際公開番号
WO 2010/041690 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)　　*G09C 1/00* (2006.01)

(21) 国際出願番号: PCT/JP2009/067506

(22) 国際出願日: 2009 年 10 月 7 日(07.10.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-260509 2008 年 10 月 7 日(07.10.2008)　JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 古川　潤 (FURUKAWA Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号　日本電気株式会社内 Tokyo (JP).

(74) 代理人: 高橋　勇(TAKAHASHI Isamu); 〒1010031 東京都千代田区東神田１丁目１０番７号　南日本ビル７階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

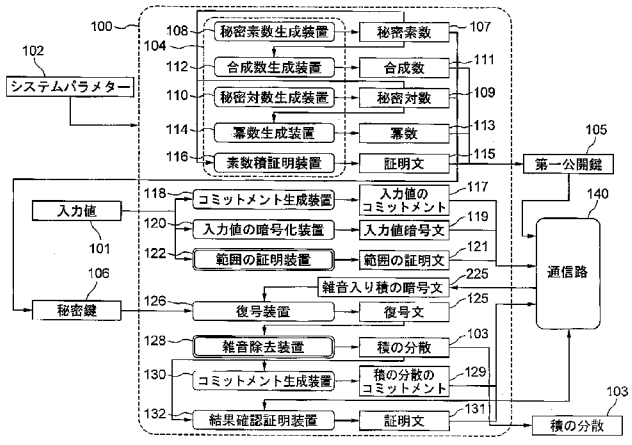
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: MULTI-PARTY VARIANCE MULTIPLICATION DEVICE, MULTI-PARTY VARIANCE MULTIPLICATION SYSTEM AND METHOD

(54) 発明の名称 : 多者分散乗算装置、多者分散乗算システム及び方法

[図1]



101 INPUT VALUE
102 SYSTEM PARAMETERS
103 VARIANCE OF THE PRODUCT
105 FIRST PUBLIC KEY
106 PRIVATE KEY
107 PRIVATE PRIME NUMBER
108 PRIVATE PRIME NUMBER GENERATION DEVICE
109 PRIVATE LOGARITHM
110 PRIVATE LOGARITHM GENERATION DEVICE
111 COMPOSITE NUMBER
112 COMPOSITE NUMBER GENERATION DEVICE
113 POWER
114 POWER GENERATION DEVICE
115 CERTIFICATE
116 PRIME NUMBER AUTHENTICATION DEVICE
117 COMMITMENT OF INPUT VALUE
118 COMMITMENT GENERATION DEVICE
119 INPUT VALUE ENCRYPTED TEXT
120 ENCRYPTION DEVICE FOR INPUT VALUE
121 CERTIFICATE OF THE RANGE
122 RANGE AUTHENTICATION DEVICE
125 DECRYPTED TEXT
126 DECRYPTION DEVICE
128 NOISE REMOVAL DEVICE
129 COMMITMENT OF VARIANCE OF THE PRODUCT
130 COMMITMENT GENERATION DEVICE
131 CERTIFICATE
132 RESULT CONFIRMATION AUTHENTICATION DEVICE
140 COMMUNICATION PATH
225 ENCRYPTED TEXT OF NOISY PRODUCT

(57) **Abstract**: Provided is a multi-party variance multiplication device for mutual communication and calculation. The device is provided with: an initial setting device for generating a first public key by using input system parameters; a commitment generation device for generating the commitment of a first input value based on the system parameters and a random number; an encryption device for generating the encrypted text of the first input value based on the system parameters, a random number, and the first public key; an authentication device for generating a certificate which authenticates the range of the first input value based on the system parameters, the random number for generating the encrypted text, the first public key, and a second public key which is already public; a decryption device in which a noisy encrypted text transmitted from a second device is decrypted and the decrypted text is generated based on the system parameters, the first public key, and a private key; and a noise removal device for generating the variance of the product by removing noise from the decrypted text.

(57) 要約:

[続葉有]

WO 2010/041690 A1

【課題】互いに通信して計算する多者分散乗算装置を提供する。 【解決手段】入力するシステムパラメターを利用することにより、第一公開鍵を生成する初期設定装置と、前記システムパラメターと乱数とに基づいて、第一入力値のコミットメントを生成するコミットメント生成装置と、前記システムパラメターと乱数と前記第一公開鍵とに基づいて、前記第一入力値の暗号文を生成する暗号化装置と、前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵及び既に公開されている第二公開鍵とに基づいて、前記第一入力値の範囲を証明する証明文を生成する証明装置と、前記システムパラメターと前記第一公開鍵と秘密鍵とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成する復号装置と、前記復号文から雑音を除去する事により積の分散を生成する雑音除去装置とを含む。

明　細　書

発明の名称 ： 多者分散乗算装置、多者分散乗算システム及び方法

技術分野

[0001] 本発明は、複数の装置に分散して所持されている二つの値の積を、これらの装置に分散して所持されるように、これら装置が互いに通信して計算する技術に関する。

背景技術

[0002] 関連する多者分散乗算装置として、非特許文献１に挙げられる方式を利用した手法がある。

以下に、非特許文献１の方法を説明する。

[0003] 非特許文献１では、二台の演算用の装置Ａ，Ｂを用いており、その一方の装置Ａにはa[1]とb[1]との値が入力されている。また、他方の装置Ｂにはa[2]とb[2]との値が入力されている。前記それぞれの装置Ａ，Ｂに入力されている値a[1]，b[1]，a[2]及びb[2]は、a[1]∈Z/2Z ，b[1] ∈Z/2Z，a[2] ∈Z/2Z ，b[2] ∈Z/2Zの関係に設定されている。

そして、前記非特許文献１での２台の装置Ａ，Ｂは相互に通信することにより、前記入力した値（二者に分散されたビット）の加算と乗算に基づいて任意の計算を分散して実行することにより、前記装置Ａはc[1] の値を、前記装置Ｂはc[2] の値をそれぞれ出力している。前記装置Ａが出力する値c[1] と、前記装置Ｂが出力する値c[2] とは、c[1]+c[2] = (a[1]+a[2])(b[1]+b[2]) を満す関係にあり、しかも、前記値c[1] と、前記値c[2] とは、c[1] ∈Z/2Z と c[2]∈Z/2Z との関係に設定されている。すなわち、非特許文献１の方法によれば、それぞれの装置Ａ，Ｂに和の形で分散されたビット (a[1]+a[2]) とビット (b[1]+b[2])との積を、再びc[1]+c[2] の様に和の形で前記２台の装置Ａ，Ｂに分散する事ができる。

[0004] 一方、ビット (a[1]+a[2]) と ビット (b[1]+b[2]) との和を、再びc[1]+c[2]の様に和の形で前記２台の装置Ａ，Ｂに分散する場合、c[1]とc[2]とが、

２台の装置Ａ，Ｂで分散して計算した結果、それぞれc[1]=a[1]+b[1]， c[2]=a[2]+b[2] となるので、ビット（a[1]+a[2]）と ビット（b[1]+b[2]）との和を、再びc[1]+c[2] の様に和の形で前記２台の装置Ａ，Ｂに分散することは容易である。

この様に非特許文献１によれば、２台の演算用の装置を用いることにより、二者に分散されたビットの値に基づいて分散した演算が可能であることから、論理回路による演算処理に、非特許文献１による分散した計算処理を適用することが可能である。また、大きな環上の演算はビット演算で記述できるため、前記環上の演算に非特許文献１による分散した計算処理を適用することが可能である。

非特許文献1：Oded Goldreich: The Foundations of Cryptography -Volume 2. pp.643-645 ISBN 0-521-83084-2 Published in US in May 2004. Publisher: Cambridge University Press

発明の概要

発明が解決しようとする課題

[0005] 上述した非特許文献１による演算方法は、二者に分散されたビットの加算と乗算に基づいて任意の計算を分散して行うことができるという利点を備えているが、前記非特許文献１による演算方法を大きな環上の演算に適用した場合、前記環上での任意の演算を分散して計算することはできず、したがって、前記環上での演算に必要な計算量が膨大となってしまうという問題がある。

[0006] 本発明の目的は、二つの演算用の装置に和の形で分散して所持されている環上の演算に用いられる二つの値の積を、これらの演算用の装置に和の形で分散して所持されるように、これら装置が互いに通信して計算する多者分散乗算装置、多者分散乗算システム及び方法を提供することにある。

課題を解決するための手段

[0007] 前記目的を達成するため、本発明に係る多者分散乗算システムは、相互通信により、対話の正当性を識別する多者分散乗算システムであって、

入力するシステムパラメターを利用することにより、第一公開鍵を生成して公開する初期設定装置を備えた第一装置と、

入力するシステムパラメターを利用することにより、第二公開鍵を生成して公開する初期設定装置を備えた第二装置とを有し、

前記第一装置は、

前記システムパラメターと乱数とに基づいて、前記第一装置に入力する第一入力値のコミットメントを生成するコミットメント生成装置と、

前記システムパラメターと乱数と前記第一公開鍵とに基づいて、前記第一入力値の暗号文を生成する暗号化装置と、

前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵及び前記第二公開鍵とに基づいて、前記第一入力値の範囲を証明する証明文を生成する証明装置と、

前記システムパラメターと前記第一公開鍵と自己が保有する秘密鍵とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成する復号装置と、

前記復号文から雑音を除去する事により積の分散を生成する雑音除去装置とを含み、

前記第二装置は、

前記システムパラメターと乱数とに基づいて、前記第二装置に入力する第二入力値のコミットメントを生成するコミットメント生成装置と、

前記システムパラメターと前記第一公開鍵と前記第二公開鍵と前記証明文とに基づいて、前記第一入力値の暗号文の平文が前記範囲にあることを検証する検証装置と、

自己が保有する積の分散を生成する分散生成装置と、

前記第一入力値の暗号文と前記第二入力値と前記積の分散とに基づいて、前記第一入力値の暗号文の平文と前記第二入力値との積に雑音を足したデータの暗号文を前記雑音入り積の暗号文として生成する暗号文生成装置とを含む事を特徴とする。

[0008] また、本発明の第二の多者分散乗算装置は、入力手段、出力手段、計算手段、通信手段、とを備える多者分散乗算装置であって、

システムパラメターが入力され、第二公開鍵を出力する装置である初期設定装置と、

システムパラメター、入力値、と第二乱数から入力値のコミットメントを生成するコミットメント生成装置と、

入力値暗号文と範囲の証明文を受信する装置と、

システムパラメター、前記入力値暗号文、第一公開鍵、第二公開鍵、と範囲の証明文とから、前記入力値暗号文の平文が一定の範囲にあることを検証する範囲の検証装置と、

前記入力値暗号文と前記入力値とから、前記入力値暗号文の平文と前記入力値の積に雑音を足したデータの暗号文である雑音入り積の暗号文を生成する、雑音入り積の暗号文生成装置と、

からなる事を特徴とする。

[0009] また、本発明に係る多者分散乗算方法は、第一装置と第二装置との相互通信により、前記装置間での対話の正当性を識別する多者分散乗算方法であって、

前記第一装置に入力するシステムパラメターを利用することにより、前記第一装置から第一公開鍵を公開すると共に、前記第二装置に入力するシステムパラメターを利用することにより、前記第二装置から第二公開鍵を公開し、

前記システムパラメターと乱数とに基づいて、前記第一装置に入力する第一入力値のコミットメントを生成する処理と、

前記システムパラメターと乱数と前記第一公開鍵とに基づいて、前記第一入力値の暗号文を生成する処理と、

前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵及び前記第二公開鍵とに基づいて、前記第一入力値の範囲を証明する証明文を生成する処理と、

前記システムパラメターと前記第一公開鍵と自己が保有する秘密鍵とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成する処理と、

前記復号文から雑音を除去する事により積の分散を生成する処理と、

前記システムパラメターと乱数とに基づいて、前記第二装置に入力する第二入力値のコミットメントを生成する処理と、

前記システムパラメターと前記第一公開鍵と前記第二公開鍵と前記証明文とに基づいて、前記第一入力値の暗号文の平文が前記範囲にあることを検証する処理と、

自己が保有する積の分散を生成する処理と、

前記第一入力値の暗号文と前記第二入力値と前記積の分散とに基づいて、前記第一入力値の暗号文の平文と前記第二入力値との積に雑音を足したデータの暗号文を前記雑音入り積の暗号文として生成する処理とを実行する事を特徴とする。

発明の効果

[0010] 本発明によれば、二つの装置に和の形で分散して所持されているある環上の二つの値の積を、これらの装置に和の形で分散して所持されるように、これら装置が互いに通信して計算する事ができる。

図面の簡単な説明

[0011] [図1]本発明の実施の形態に係る第一装置の構成を示す図である。

[図2]本発明の実施の形態に係る第二装置の構成を示す図である。

[図3]本発明の実施の形態に係る第一装置の処理の流れを示す図である。

[図4]本発明の実施の形態に係る第二装置の処理の流れを示す図である。

発明を実施するための最良の形態

[0012] 以下、本発明の実施形態を図に基づいて詳細に説明する。

[0013] 図１及び図２に示す本発明の実施形態に係る多者分散乗算システムは、その一例として秘匿通信等における暗号処理に適用したものである。先ず、以下に説明する本発明の実施形態に係る多者分散乗算システムにおいて用いる

各記号について説明する。κ，μを正の整数である安全変数、pを長さκビットの正の整数、Gを位数pの巡回群、g，hをGの生成元とする。log ghは、hのgに関する離散対数であり、この値は誰も知らないものとする。Hashは任意の文字列から長さκビットの文字列への暗号学的ハッシュ関数とする。κ，μ，p，Gの記号、g，h，Hashの記号をシステムパラメーターと呼ぶ。

[0014] 図１及び図２に係る本発明の実施形態に係る多者分散乗算システムは、通信路１４０を介して相互に通信可能な図１に示す第一装置１００及び図２に示す第二装置２００を有している。

[0015] 図１に示す前記第一装置１００は、初期設定装置１０４を有している。また、図１に示す前記第一装置１００は、コミットメント生成装置１１８と、暗号化装置１２０及び範囲の証明装置１２２と、復号装置１２６と、雑音除去装置１２８と、コミットメント生成装置１３０及び結果確認証明装置１３２を有している。

[0016] 前記初期設定装置１０４は、前記第一装置１００に入力する前記システムパラメーターに基づいて第一公開鍵１０５を通信路１４０上に公開するものであり、前記初期設定装置１０４は、秘密素数生成装置１０８と、合成数生成装置１１２と、秘密対数生成装置１１０と、冪数生成装置１１４と、素数積証明装置１１６とを有している。

[0017] 前記秘密素数生成装置１０８は、第一装置１００に入力する前記システムパラメーター１０２に基づいて、$2\kappa+\mu$より大きい二つのセーフ素数である秘密素数１０７をランダムに生成するものである。前記二つのセーフ素数である秘密素数１０７を、p[1]とq[1]として表記する。また、前記秘密対数生成装置１１０は、第一装置１００に入力する前記システムパラメーター１０２に基づいて、秘密対数１０９をランダムに生成するものである。前記秘密対数１０９をx[1]として表記する。また、前記秘密対数x[1]は、$x[1]\in Z/pZ$の関係をもつ。

[0018] 前記合成数生成装置１１２は、前記秘密素数生成装置１０８が生成した秘密素数p[1]及びq[1]（１０７）に基づいて、合成数１１１を生成するもので

ある。前記合成数１１１をn[1]として表記する。また、前記合成数n[1]は、n[1]=p[1]q[1]の関係をもつ。前記p[1]q[1]は、前記p[1]と前記q[1]との積であることを示している。

[0019] 前記冪数生成装置１１４は、前記秘密対数生成装置１１０が生成した秘密対数x[1]（１０９）に基づいて、冪数１１３を生成するものである。前記冪数１１３をy[1]として表記する。前記冪数y[1]は、$y[1]=g^{x[1]}$の関係にもつ。

[0020] 前記素数積証明装置１１６は、前記秘密素数生成装置１０８が生成する前記秘密素数p[1]，q[1]に基づいて証明文１１５を生成するものである。前記証明文１１５は、前記合成数n[1]が（$2\kappa+\mu$）より大きい二つのセーフ素数である秘密素数p[1]とq[1]との積p[1]q[1]であることを示すものである。

[0021] 前記初期設定装置１０４は、前記合成数生成装置１１２が生成した合成数n[1]と、前記冪数生成装置１１４が生成した冪数y[1]と、前記素数積証明装置１１６が証明した証明文１１５とに加えて、e[1]の情報を付加することにより、これらを第一公開鍵１０５として通信路１４０上に公開する。したがって、前記第一公開鍵１０５は、合成数n[1]，冪数y[1]，証明文１１５及び前記e[1]から構成されている。

[0022] 以上説明した構成が第一公開鍵１０５を通信路１４０上に公開するためのものである。次に、前記第一公開鍵１０５を用いて入力値１０１の平文を暗号化する構成について説明する。

[0023] 前記コミットメント生成装置１１８は、前記システムパラメターと乱数とに基づいて、前記第一装置１００に入力する入力値１０１のコミットメント１１７を生成するものである。前記コミットメント１１７をc[1]として表記する。前記コミットメントc[1]は、$c[1]=g^{s[1]}h^{u[1]}$の関係をもつ。前記$g^{s[1]}h^{u[1]}$は、$g^{s[1]}$と$h^{u[1]}$との積であることを示している。前記s[1]は入力値１０１を示し、前記u[1]は後述する乱数を示している。

[0024] 前記暗号化装置１２０は、前記システムパラメターと、ランダムに選んだ第三乱数r[1]と、前記第一公開鍵１０５とを用いて、入力値１０１を暗号化し、その入力値暗号文１１９を通信路１４０に通して第二装置２００に送信

するものである。前記入力値暗号文１１９をd=e[1]$^{s[1]}$r[1]$^{n[1]}$として表記する。前記入力値暗号文１１９は、公開鍵１０５に含まれるe[1]と、入力値s[1]と、乱数r[1]と、合成数n[1]との積として示される。

[0025] 前記範囲の証明装置１２２は、前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵１０５及び前記第二公開鍵２０５とに基づいて、前記暗号化装置１２０が作成した入力値暗号文１１９のうち暗号化された平文の大きさ（範囲）を証明する証明文１２１を作成するものである。前記入力値暗号文１１９の平文は、第一装置１００に入力する入力値１０１に相当するものであり、前記平文をs[1]として表記する。

[0026] 次に、第二装置２００で暗号化されて通信路１４０を通して第一装置１００に送信された暗号文を復号する構成について説明する。

[0027] 前記復号装置１２６は、前記システムパラメターと前記第一公開鍵１０６と自己が保有する秘密鍵１０６とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成するものである。前記復号文１２５を取得する際、前記復号装置１２６は、秘密鍵１０６を用いて前記暗号文２２５を復号する。前記秘密鍵１０６は、前記秘密素数生成装置１０８が生成する秘密素数p[1]及びq[1]と、前記秘密対数生成装置１１０が生成する秘密対数x[1]とを含んでいる。さらに、第二装置２００で暗号化された暗号文２２５には、雑音が含まれている。

[0028] 前記雑音除去装置１２８は、前記復号装置１２６が復号した復号文１２５に含まれる雑音を除去し、雑音が除去された積の分散１０３を出力するものである。

[0029] 前記コミットメント生成装置１３０は、前記雑音除去装置１２８が出力する前記積の分散１０３を入力として、前記積の分散１０３についてのコミットメント１２９を生成するものである。

[0030] 前記結果確認証明装置１３２は、第一装置１００への入力値s[1]と第二装置２００への入力値s[2]との積が、第一装置１００が保持する積の分散t[1]と第二装置２００が保持する積の分散t[2]との和となっているかを確認し、

その確認した事実を第三者に証明する証明文１３１を通信路１４０上に公開するものである。

[0031] 次に、第一装置１００と通信路１４０を介して通信を行う第二装置２００の構成について説明する。

[0032] 図２に示す前記第二装置２００は、初期設定装置２０４を有している。また、図２に示す前記第二装置２００は、コミットメント生成装置２１８と、積の分散生成装置２２４と、コミットメント生成装置２２６と、結果確認証明装置２３２と、範囲の検証装置２２２とを有している。

[0033] 前記初期設定装置２０４は、前記第二装置２００に入力する前記システムパラメーに基づいて第二公開鍵２０５を通信路１４０上に公開するものであり、前記初期設定装置２０４は、秘密素数生成装置２０８と、合成数生成装置２１２と、秘密対数生成装置２１０と、冪数生成装置２１４と、素数積証明装置２１６とを有している。

[0034] 前記秘密素数生成装置２０８は、第二装置２００に入力する前記システムパラメー１０２に基づいて、$2\kappa+\mu$より大きい二つのセーフ素数である秘密素数２０７をランダムに生成するものである。前記二つのセーフ素数である秘密素数２０７を、p[2]とq[2]として表記する。また、前記秘密対数生成装置２１０は、第二装置２００に入力する前記システムパラメー１０２に基づいて、秘密対数２０９をランダムに生成するものである。前記秘密対数２０９をx[2]として表記する。また、前記秘密対数x[2]は、$x[2]\in Z/pZ$の関係をもつ。

[0035] 前記合成数生成装置２１２は、前記秘密素数生成装置２０８が生成した秘密素数p[2]及びq[2]（２０７）に基づいて、合成数２１１を生成するものである。前記合成数２１１をn[2]として表記する。また、前記合成数n[2]は、n[2]=p[2]q[2]の関係をもつ。前記p[2]q[2]は、前記p[2]と前記q[2]との積であることを示している。

[0036] 前記冪数生成装置２１４は、前記秘密対数生成装置２１０が生成した秘密対数x[2]（２０９）に基づいて、冪数２１３を生成するものである。前記冪

数２１３をy[2]として表記する。前記冪数y[2]は、$y[2]=g^{x[2]}$の関係にもつ。

[0037] 前記素数積証明装置２１６は、前記秘密素数生成装置２０８が生成する前記秘密素数p[2]，q[2]に基づいて証明文２１５を生成するものである。前記証明文２１５は、前記合成数n[2]が（$2\kappa+\mu$）より大きい二つのセーフ素数である秘密素数p[2]とq[2]との積p[2]q[2]であることを示すものである。

[0038] 前記初期設定装置２０４は、前記合成数生成装置２１２が生成した合成数n[2]と、前記冪数生成装置２１４が生成した冪数y[2]と、前記素数積証明装置２１６が証明した証明文１１５とに加えて、η［12］及びη［22］$\in$ $Z/n[2]^2Z$の情報を付加することにより、これらを第二公開鍵２０５として通信路１４０上に公開する。したがって、前記第二公開鍵２０５は、合成数n[2]，冪数y[2]，証明文２１５、η［12］及びη［22］から構成されている。

[0039] 以上説明した構成が第二公開鍵２０５を通信路１４０上に公開するためのものである。次に、前記第二公開鍵２０５を用いて入力値２０１の平文を暗号化する構成について説明する。

[0040] 前記コミットメント生成装置２１８は、前記第二装置２００に入力する入力値２０１のコミットメント２１７を生成するものである。前記コミットメント２１７をc[2]として表記する。前記コミットメントc[2]は、$c[2]=g^{s[2]}h^{u[2]}$の関係をもつ。前記$g^{s[2]}h^{u[2]}$は、$g^{s[2]}$と$h^{u[2]}$との積であることを示している。前記s[2]は入力値２０１を示し、前記u[2]は後述する乱数を示している。

[0041] 前記範囲の検証装置２２２は、前記システムパラメターと前記第一公開鍵１０５と前記第二公開鍵２０５と前記証明文１２１とに基づいて、前記第一入力値の暗号文の平文が前記範囲にあることを検証する、言い換えるとハッシュ関数（α＝Hash）を計算することにより、第二装置２００に入力した入力値暗号文１１９のうち暗号化された平文の大きさの範囲を示す前記範囲の証明文１２１を検証するものである。

[0042] 前記積の分散生成装置２２４は、第二装置２００が保持する積の分散２０３を生成するものである。前記雑音入り積の暗号文生成装置２２６は、前記第一入力値の暗号文１１９と前記第二入力値２０１と前記積の分散２０３と

に基づいて、前記第一入力値の暗号文の平文と前記第二入力値との積に雑音を足したデータの暗号文を前記雑音入り積の暗号文として生成する、言い換えると前記積の分散生成装置２２４が生成した前記積の分散２０３及び第二装置２００に入力する入力値２０１を入力として、前記入力値２０１について暗号化処理を施し、雑音入りの積の暗号文２２５を生成し、前記積の暗号文２２５を通信路１４０に通して第一装置１００に送信するものである。

[0043] 前記コミットメント生成装置２３０は、前記積の分散生成装置２２４が出力する前記積の分散２０３を入力として、前記積の分散２０３についてのコミットメント２２９を生成するものである。

[0044] 前記結果確認証明装置２３２は、第二装置２００への入力値s[2]と第一装置１００への入力値s[1]との積が、第一装置１００が保持する積の分散t[1]と第二装置２００が保持する積の分散t[2]との和となっているかを確認し、その確認した事実を第三者に証明する証明文２３１を通信路１４０上に公開するものである。

[0045] 本発明の実施形態に係る多者分散乗算システムは、図１に示す第一装置１００が入力値s[1]（１０１）を保持し、図２に示す第二装置２００が入力値s[2]（２０１）を保持していることを前提としている。そして、本発明の実施形態に係る多者分散乗算システムは、前記前提条件の下に、通信路１４０を介して相互に通信を行い、その通信の結果、前記入力値s[1]とs[2]との積に等しい和となる積の分散t［1］（１０３），t［2］（２０３）を第一装置１００と第二装置２００とがそれぞれ保持するに至った際に、前記第一装置１００と前記第二装置２００との間で行われた通信（対話）が正当性をもつことを証明可能としたものである。なお、前記入力値s[1]とs[2]との積と分散t［1］（１０３）とt［2］（２０３）との和との関係を式で示すと、s[1]s[2]＝t［1］（１０３）＋t［2］（２０３）となる。

[0046] 以下、図１及び図２に示す本発明の実施形態に係る多者分散乗算システムの動作を図３及び図４に基づいて詳細に説明する。なお、図３は、図１に示す第一装置１００の動作を示すフローチャートであり、図４は、図２に示す

第二装置２００の動作を示すフローチャートである。

[0047] 図３及び図４に示す様に、第一装置１００の初期設定装置１０４及び第二装置２００の初期設定装置２０４は、初期設定の手続として公開鍵１０５，２０５をそれぞれ出力する。以下、公開鍵１０５，２０５をそれぞれ出力する動作を具体的に説明する。

[0048] 第一装置１００と第二装置２００には、システムパラメター１０２が入力される。

[0049] 第一装置１００の秘密素数生成装置１０８は、システムパラメター１０２に基づいて、$2\kappa+\mu$より大きい二つのセーフ素数である秘密素数p[1]，q[1]（１０７）をランダムに生成する。同様に第二装置２００の秘密素数生成装置２０８は、システムパラメター１０２に基づいて、$2\kappa+\mu$より大きい二つのセーフ素数である秘密素数p[2]，q[2]（２０７）をランダムに生成する。

[0050] 第一装置１００の秘密対数生成装置１１０は、システムパラメター１０２に基づいて、秘密対数x[1]（１０９）をランダムに生成する。前記秘密対数x[1]は、$x[1]\in Z/pZ$の関係を持っている。

第二装置２００秘密対数生成装置２１０は、システムパラメター１０２に基づいて、秘密対数x[2]（２０９）をランダムに生成する。前記秘密対数x[2]は、$x[2]\in Z/pZ$の関係を持っている。

[0051] 第一装置１００の合成数生成装置１１４は、前記秘密素数生成装置１０８が生成した秘密素数p[1]q[1]（１０７）に基づいて合成数n[1]（１１１）を生成する。前記合成数n[1]は、n[1]=p[1]q[1]の関係をもつ。

第二装置２００の合成数生成装置２１４は、前記秘密素数生成装置２０８が生成した秘密素数p[2]q[2]（２０７）に基づいて合成数n[2]（２１１）を生成する。前記合成数n[2]は、n[2]=p[2]q[2]の関係をもつ。

[0052] 第一装置１００の冪数生成装置１１４は、前記秘密対数生成装置１１０が生成した秘密対数x[1]（１０９）に基づいて、冪数y[1]（１１３）を生成する。前記冪数y[1]は、$y[1]=g^{x[1]}$の関係をもつ。

第二装置２００の冪数生成装置２１４は、前記秘密対数生成装置２１０が

生成した秘密対数x[2]（２０９）に基づいて、冪数y[2]（２１３）を生成する。前記冪数y[2]は、$y[2]=g^{x[2]}$の関係をもつ。

[0053] 以上説明した前記秘密素数生成装置１０８，２０８、前記合成数生成装置１１２，２１２、前記秘密対数生成装置１１０，２１０、前記冪数生成装置１１４，２１４による処理は、図３のステップＳ１及び図４のステップＳ２１において実行する。

[0054] また、第一装置１００の素数積証明装置１１６は、前記秘密素数生成装置１０８が生成した秘密素数p[1]，q[1]に基づいて、前記合成数n[1]が$2\kappa+\mu$より大きい二つのセーフ素数（p[1]，q[1]）の積であることを証明する証明文１１５を生成する。

第二装置２００の素数積証明装置２１６は、前記秘密素数生成装置２０８が生成した秘密素数p[2]，q[2]に基づいて、前記合成数n[2]が$2\kappa+\mu$より大きい二つのセーフ素数（p[2]，q[2]）の積であることを証明する証明文２１５を生成する。

以上説明した前記素数積証明装置１１６，２１６による処理は、図３のステップＳ２，図４のステップＳ２２において実行する。

[0055] 次に、第一装置１００は、前記秘密素数１０７，前記合成数１１１，前記秘密対数１０９，前記冪数１１３及び前記証明文１１５をそれぞれ生成した際に、前記合成数n[1]（１１１）と、前記冪数y[1]（１１３）と、前記証明文１１５とに加えて、e[1]の情報を付加することにより、これらを第一公開鍵１０５として通信路１４０上に公開する。

[0056] 同様に前記初期設定装置２０４は、前記秘密素数２０７，前記合成数２１１，前記秘密対数２０９，前記冪数２１３及び前記証明文２１５をそれぞれ生成した際に、前記合成数n[2]（２０７）と、前記冪数y[2]（２１３）と、前記証明文２１５とに加えて、η［12］及びη［22］$\in Z/n[2]^2Z$の情報を付加することにより、これらを第二公開鍵２０５として通信路１４０上に公開する。

[0057] 以下、$\gamma[1]=\eta[12]^2$、$\gamma[2]=\eta[22]^2$とする。第一装置１００の出力する第

一公開鍵１０５には、n[1]、y[1]、証明文、e[1]が含まれている。第二装置２００の出力する第二公開鍵２０５には、n[2]、y[2]、証明文、η[12]、η[22]が含まれている。また、第一装置１００は、p[1]，q[1]，x[1]を含む秘密鍵１０６を保有しているが、第二装置２００は、第一装置１００とは異なり、秘密鍵を保有していない。

[0058] 以上説明した処理は、前記入力値s[1]，s[2]を用いていない処理であるため、以上の過程で生成した、秘密素数１０７，２０１、合成数１１１，２１１、秘密対数１０９，２０９、冪数１１３，２１３、証明文１１５，２１５の情報は、入力値s[1]，s[2]が変更になった際にも、何度でも利用することができる。

[0059] 以上説明した前記初期設定装置１０４，２０４による初期設定が終了した際に（図３のステップＳ３，Ｓ２３）、コミットメントの処理を実行する（図３のステップＳ４，図４のステップＳ２４）。具体的に説明する。

[0060] 第一装置１００のコミットメント生成装置１１８には、入力値１０１として、s[1] $\in$ Z/pZ の入力値s[1]が入力し、第二装置２００のコミットメント生成装置２１８には、入力値２０１として、s[2] $\in$ Z/pZ が入力する。

[0061] 第一装置１００のコミットメント生成装置１１８は、第一乱数 u[1] $\in$ Z/pZ を生成し、その乱数u[1]に基づいて、前記入力値s[1]のコミットメント（c[1]）１１７を生成する（図３のステップＳ４）。前記コミットメント１１７は、$c[1]=g^{s[1]}\ h^{u[1]}$の関係をもつ。

同様に第二装置２００のコミットメント生成装置２１８は、第二乱数 u[2] $\in$ Z/pZ を生成し、その乱数u[2]に基づいて、前記入力値s[2]のコミットメント（c[2]）２１７を生成する。前記コミットメント２１７は、$c[2]=g^{s[2]}\ h^{u[2]}$の関係をもつ。

[0062] これにより、前記コミットメント生成装置１１８から、入力値のコミットメント（$c[1]=g^{s[1]}\ h^{u[1]}$）１１７が通信路１４０上に公開される。同様に前記コミットメント生成装置２１８から、入力値のコミットメント（$c[2]=g^{s[2]}\ h^{u[2]}$）２１７が通信路１４０上に公開される。

[0063] 以上説明した図３のステップＳ４及び図４のステップＳ２４までの処理が実行された後、積の分散t[1]（１０３）、t[2]（２０３）を計算する処理を行う。因みに、第一装置１００と第二装置２００とが正当に通信を行う場合、前記入力値s[1]とs[2]との積と、分散t［1］（１０３）とt［2］（２０３）との和との関係は、s[1]s[2]＝t［1］（１０３）＋t［2］（２０３）を満たすこととなる。具体的に説明する。

[0064] 第一装置１００の暗号化装置１２０は、入力値１０１が入力すると、ランダムに第三乱数r[1] ∈ Z/n[1]^{2}Zを選び、その乱数r[1]を用いて入力値１０１を暗号化する。前記入力値１０１を暗号化した暗号文１１９をdとして表記すると、d = e[1]$^{s[1]}$ r[1]$^{n[1]}$の関係をもつ。

[0065] 第一装置１００の証明装置２２２は、前記暗号文（d）１１９に含まれる平文（入力値s[1]（１０１））の大きさ（範囲）を示す証明文１２１を生成する（図３のステップＳ６）。前記証明装置２２２は、前記証明文１２１を通信路１４０上に公開する。

[0066] 前記暗号化装置１２０が前記入力値の暗号文１１９を通信路１４０に通して第二装置２００に送信すると、第二装置は、範囲の証明文１２１を検証装置２２２を用いて検証する。具体的に説明する。

[0067] 第一装置１００の前記範囲の証明装置１２２は、ランダムに $\rho \in [0,1]^{|n[2]|+\mu}$、$\delta = \gamma[1]^{s[1]}\ \gamma[2]\rho$ を生成する。そして、前記範囲の証明装置１２２は、

$\delta = \gamma[1]^{s}\ \gamma[2]\rho$

$-2^{2}\kappa + \mu+1 < s < 2^{2}\kappa+\mu+1$

$d = e[1]^{s}\ r^{n[1]}$

$c[1] = g^{s}\ h^{u}$

を満すs、$\rho \in Z$、$r \in Z/n[1]^2Z$、$u \in Z/pZ$ の知識を統計的零知識で証明する証明文を次のように生成する。

[0068] すなわち、前記範囲の証明装置１２２は、

$0 \leqq s' < 2^{2}\kappa+\mu$、$\rho' \in [0,1]^{|n[2]|+\kappa+2\mu}$、$r' \in Z/n[1]^2Z$、$u' \in Z$

/pZ をランダムに選び、

$\delta' = \gamma[1]^{s'} \gamma[2]^{\rho'}$

$d' = e[1]^{s'} r'^{n[1]}$

$c' = g^{s'} h^{u'}$

を生成し、

$\alpha = \mathrm{Hash}(\kappa, \mu, p, g, h, n\_1, n[2], e[1], \delta, d, c[1], \delta', d', c')$

を生成する。

さらに、前記範囲の証明装置１２２は、

$s'' = s[1]\ c + s'$ (Z 上)

$\rho'' = \rho\ c + \rho'$ (Z 上)

$r'' = r^c r'$

$u'' = u\ c + u'$

を計算する。

[0069] そして、前記範囲の証明装置１２２は、通信路１４０を介して第二装置２００に、範囲の証明文１２１を送信する。前記証明文１２１には、($\delta, \delta', d', c', s'', \rho'', r'', u''$)が含まれている。

[0070] 第二装置２００が前記暗号文１１９及び前記証明文１２１を受信した際、範囲の検証装置２２２は、

$\alpha = \mathrm{Hash}(\kappa, \mu, p, g, h, n_1, n[2], e[1], \delta, d, c[1], \delta', d', c')$を計算し、

以下の式が成り立つことを確認して、範囲の証明文１２１を検証する（図４のステップＳ２５）。

$\delta^c \delta' = \gamma[1]^{s''} \gamma[2]^{\rho''}$

$-2^{2\kappa+\mu+1} < s'' < 2^{2\kappa+\mu+1}$

$d^c d' = e[1]''^{r''^n}$

$c[1]^c c' = g^{s''} h^{u''}$

[0071] 第二装置２００の積の分散生成装置２２４は、雑音 $0 < m < 2^{2\kappa+2\mu}$、及び乱数 $r[2] \in Z/n[1]^2Z$に加えて、積の分散t[2]をランダムに選び、積の分散（２０３）$t[2] \in Z/pZ$を生成する（図４のステップＳ２６）。

[0072] 次に、暗号文生成装置２２６は、前記積の分散生成装置２２４が出力する、前記雑音及び前記乱数に加えて前記積の分散のデータを得ることにより、前記入力した暗号文１１９に基づいて雑音入り積の暗号文２２５を生成する（図４のステップＳ２７）。

前記暗号文生成装置２２６が生成する暗号文２２５をbとして表記すると、次の式で表される。

$b = d^{s[2]}\ e[1]^{p\,m\,-t[2]} r[2]^{n[1]}$

前記暗号文生成装置２２６は、前記暗号文２２５を通信路１４０に通して第一装置１００に送信する。

[0073] 第一装置１００の復号装置１２６は、前記暗号文２２５を受信すると、秘密鍵１０６を用いて、前記bで表記された暗号をPaillier暗号として復号し、前記暗号文２２５を復号文１２５（t'[2] ∈ Z/n[1]Z）を得る。上述した様に、前記秘密鍵１０６は、p[1], q[1], x[1]を含んでいる。

前記復号装置１２６は、

λ=lcm(p[1],q[1]$ 及び、$L:Z/n[1]^2Z → Z/n[1]Z; c → (cλ -1) / n[1] mod n[1]の復号のための式を用いて、

t'[1] =L(bλ) / L(e[1]λ）とする復号文１２５を得る（図３のステップＳ７）。

[0074] 雑音除去装置１２８は、前記復号文１２５を受信すると、前記復号文１２５から前記雑音を除去して、積の分散１０３（t[1] ∈ Z/pZ）を得る（図３のステップＳ８）。前記積の分散１０３をt[1]と表記した場合、t[1] = t'[1] mod p となる。

[0075] 上の処理により、第一装置１００と第二装置２００とが、なりすましの行為を行わずに、正当な通信を行った場合、第一装置１００が保持する積の分散１０３であるt[1]と、第二装置２００が保持する積の分散２０３であるt[2]と、第一装置１００の入力値s[1]と第二装置２００の入力値s[2]との関係は、

t[1] + t[2] = s[1] s[2] となるはずである。

[0076] 次に、前記式を満たしているか否かの処理を行う場合について説明する。

[0077] 第一装置１００のコミットメント生成装置１３０は、前記積の分散１０３を受信して、ランダムにv[1] ∈ Z/pZを生成し、積の分散のコミットメント１２９（$a[1] = g^{t[1]} h^{v[1]}$）を生成し（図３のステップＳ９）、そのコミットメント１２９を通信路１４０上に公開する。

同様に第２装置２００のコミットメント生成装置２３０は、前記積の分散２０３を受信して、ランダムにv[2] ∈ Z/pZを生成し、積の分散のコミットメント１２９（$a[2] = g^{t[2]} h^{v[2]}$）を生成し（図４のステップＳ２８）、そのコミットメント２２９を通信路１４０上に公開する。

[0078] 次に、第一装置１００と第二装置２００は、それぞれ結果確認証明装置１３２，２３２を用いて、t[1] + t[2] = s[1] s[2] を以下の手順に従って確認する。また、この事実を第三者に証明する証明文１３１，２３１を出力する。この出力は、次の手続きにおいて出力される証明文全てを合わせたものである。

[0079] y =y[1] y[2] とする。すなわち、i=1,2 に関して、第i装置は$y[i]=g^{x[i]}$なるx[i] ∈ Z/pZを知っている。第二装置の結果確認証明装置２３２はランダムにw[2] ∈ Z/pZ を選んで、

$(g'[2], y'[2]) = (g^{w[2]}, g^{s[2]} y^{w[2]})$

を計算して通信路１４０上に公開する。

そして、前記結果確認証明装置２３２は、

$(g'[2], y'[2]) = (g^{w[2]}, g^{s[2]} y^{w[2]})$

$c[2] = g^{s[2]} h^{u[2]}$

なる w[2],s[2],u[2] の知識を零知識証明する。

[0080] 第一装置の結果確認証明装置１３２は、

$(g'[1], y'[1]) = (g'[2]^{s[1]} g^{w[1]}, y'[2]^{s[1]} y^{w[1]})$

を計算して通信路１４０上に公開する。

そして、前記結果確認証明装置１３２は、

$(g'[1], y'[1]) = (g'[2]^{s[1]} g^{w[1]}, y'[2]^{s[1]} y^{w[1]})$

$c[1] = g^{s[1]} h^{u[1]}$

なる w[1],s[1],u[1] の知識を零知識証明する証明文を通信路１４０上に出力する。

なお、(g'[1],y'[1])は、$g^{s[1]s[2]}$の公開鍵(g,y)によるElGamal暗号文である。

[0081] 各i=1,2 に関して、第一装置の結果確認証明装置１３２は、z[i] ∈ Z/pZ をランダムに選んで、

$(g''[i],y''[i]) = (g^{z[i]}、g^{t[i]}y^{z[i]})$

を生成し、

$(g''[i],y''[i]) = (g^{z[i]}、g^{t[i]}y^{z[i]})$

$a[i] = g^{t[i]} h^{v[i]}$

を満す、t[i],z[i],v[i] の知識を零知識証明する証明文を出力する。

(g'',y'') = (g''[1] g''[2],y''[1]y''[2]) とする.(g'',y'') は、$g^{t[1]+t[2]}$ の公開鍵(g,y) によ るElGamal 暗号文である。

[0082] 第一装置の結果確認証明装置１３２は、ランダムにθ[1] ∈ Z/pZ を選んで、

$(g[3],y[3]) =((g''/g'[2])^{\theta[1]},(y''/y'[2])^{\theta[1]})$

を生成し、θ[1]の知識を零知識証明する証明文を通信路１４０上に出力する。

[0083] 第二装置の結果確認証明装置２３２はランダムにθ[2] ∈ Z/pZ を選んで、

$(g[4],y[4]) =(g[3]^{\theta[2]},y[3]^{\theta[2]})$

を生成し、θ[2]の知識を零知識証明する証明文を通信路１４０上に出力する。

[0084] 第一装置と第二装置は協力して、(g[4],y[4])の検証可能な復号を行い、復号結果が1であることを確認する。もし異なれば、第一装置、第二装置の何れかが不正を行っている。

[0085] 何れかのi=1,2 に関する第i装置に不正があった場合は次の方法で不正者を

特定する。

第二装置の結果確認証明装置２３２は、前記積の分散（b）１０３を正しく生成したことを証明する。すなわち、前記結果確認証明装置２３２は

$b = d^s\ e[1]^t\ r^n$

$c[2] = g^s\ h^u$

$a[2] = g^{-t}\ h^v$

$0 < t < 2^{2\kappa+\mu+1}$

を満す $t \in Z$、$r \in Z/n[1]^2Z$, $s,u,v \in Z/pZ$ の知識を零知識証明する証明文を通信路１４０上に出力する。

[0086] 上の方法で第二装置の不正が明らかにならなかった場合、第一装置が不正を働いていると見做す。

[0087] 上記の各実施の形態によれば、二つの装置に和の形で分散して所持されているある環上の二つの値の積を、これらの装置に和の形で分散して所持されるように、これら装置が互いに通信して計算する事ができる。

[0088] 二つの装置に和の形で分散して所持されているある環上の二つの値の和を、これらの装置に和の形で分散して所持されるように、これら装置が互いに通信して計算する事は簡単にできることは自明であるので、本方法と合わせれば、この環上での任意の演算を分散して計算することができる。

[0089] また、本発明の計算は、各装置ではビット毎に演算するのではなく、大きな環上でまとめて計算を行っており、きわめて効率的である。

[0090] なお、環上の計算は暗号、秘密分散、符合の計算で多用される演算であるため、これらの分野で幅広く利用できる。

[0091] なお、上述する各実施の形態は、本発明の好適な実施の形態であり、本発明の要旨を逸脱しない範囲内において種々変更実施が可能である。例えば、多者分散乗算装置の機能を実現するためのプログラムを装置に読込ませて実行することにより装置の機能を実現する処理を行ってもよい。さらに、そのプログラムは、コンピュータ読み取り可能な記録媒体であるＣＤ－ＲＯＭまたは光磁気ディスクなどを介して、または伝送媒体であるインターネット、

電話回線などを介して伝送波により他のコンピュータシステムに伝送されてもよい。また、装置の機能が他の装置によりまとめて実現されたり、追加の装置により機能が分散されて実現される形態も本発明の範囲内である。

産業上の利用可能性

[0092] 本発明は、通信によって情報の遣り取りを行う際に、なりすましを阻止することができ、不正な情報通信を排除することに貢献できるものである。

[0093] この出願は２００８年１０月７日に出願された日本出願特願２００８－２６０５０９を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0094] １００ 第一装置

１０４ 初期設定装置

１０８ 秘密素数生成装置

１１０ 秘密対数生成装置

１１２ 合成数生成装置

１１４ 冪数生成装置

１１６ 素数積証明装置

１１８ コミットメント生成装置

１２０ 入力値の暗号化装置

１２２ 範囲の証明装置

１２６ 復号装置

１２８ 雑音除去装置

１３０ コミットメント生成装置

１３２ 結果確認証明装置

１４０ 通信路

２００ 第二装置

２０４ 初期設定装置

２０８ 秘密素数生成装置

２１０　秘密対数生成装置

２１２　合成数生成装置

２１４　冪数生成装置

２１６　素数積証明装置

２１８　コミットメント生成装置

２２２　範囲の検証装置

２２４　積の分散生成装置

２２６　雑音入り積の暗号文生成装置

２３０　コミットメント生成装置

２３２　結果確認証明装置

請求の範囲

[請求項1] 相互通信により、対話の正当性を識別する多者分散乗算システムであって、

入力するシステムパラメターを利用することにより、第一公開鍵を生成して公開する初期設定装置を備えた第一装置と、

入力するシステムパラメターを利用することにより、第二公開鍵を生成して公開する初期設定装置を備えた第二装置とを有し、

前記第一装置は、

前記システムパラメターと乱数とに基づいて、前記第一装置に入力する第一入力値のコミットメントを生成するコミットメント生成装置と、

前記システムパラメターと乱数と前記第一公開鍵とに基づいて、前記第一入力値の暗号文を生成する暗号化装置と、

前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵及び前記第二公開鍵とに基づいて、前記第一入力値の範囲を証明する証明文を生成する証明装置と、

前記システムパラメターと前記第一公開鍵と自己が保有する秘密鍵とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成する復号装置と、

前記復号文から雑音を除去する事により積の分散を生成する雑音除去装置とを含み、

前記第二装置は、

前記システムパラメターと乱数とに基づいて、前記第二装置に入力する第二入力値のコミットメントを生成するコミットメント生成装置と、

前記システムパラメターと前記第一公開鍵と前記第二公開鍵と前記証明文とに基づいて、前記第一入力値の暗号文の平文が前記範囲にあることを検証する検証装置と、

自己が保有する積の分散を生成する分散生成装置と、

前記第一入力値の暗号文と前記第二入力値と前記積の分散とに基づいて、前記第一入力値の暗号文の平文と前記第二入力値との積に雑音を足したデータの暗号文を前記雑音入り積の暗号文として生成する暗号文生成装置とを含む事を特徴とする多者分散乗算システム。

[請求項2] 前記第一装置は、前記第二装置との通信に不正が行われた否かを確認する結果確認証明装置を有する請求項１に記載の多者分散乗算システム。

[請求項3] 前記第二装置は、前記第一装置との通信に不正が行われた否かを確認する結果確認証明装置を有する請求項１に記載の多者分散乗算システム。

[請求項4] 第一装置と第二装置との相互通信により、前記装置間の対話の正当性を識別する多者分散乗算システムに用いる多者分散乗算装置であって、

入力するシステムパラメターを利用することにより、第一公開鍵を生成して公開する初期設定装置と、

前記システムパラメターと乱数とに基づいて、前記第一装置に入力する第一入力値のコミットメントを生成するコミットメント生成装置と、

前記システムパラメターと乱数と前記第一公開鍵とに基づいて、前記第一入力値の暗号文を生成する暗号化装置と、

前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵及び前記第二装置が公開する第二公開鍵とに基づいて、前記第一入力値の範囲を証明する証明文を生成する証明装置と、

前記システムパラメターと前記第一公開鍵と自己が保有する秘密鍵とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成する復号装置と、

前記復号文から雑音を除去する事により積の分散を生成する雑音除

去装置とを含むことを特徴とする多者分散乗算装置。

[請求項5] 前記第二装置との通信に不正が行われた否かを確認する結果確認証明装置を有する請求項４に記載の多者分散乗算装置。

[請求項6] 第一装置と第二装置との相互通信により、前記装置間の対話の正当性を識別する多者分散乗算システムに用いる多者分散乗算装置であって、

入力するシステムパラメターを利用することにより、第二公開鍵を生成して公開する初期設定装置と、

前記システムパラメターと乱数とに基づいて、前記第一装置から第二装置に入力する第二入力値のコミットメントを生成するコミットメント生成装置と、

前記システムパラメターと前記第一装置が公開する第一公開鍵と前記第二公開鍵と前記証明文とに基づいて、前記第一入力値の暗号文の平文が前記範囲にあることを検証する検証装置と、

自己が保有する積の分散を生成する分散生成装置と、

前記第一入力値の暗号文と前記第二入力値と前記積の分散とに基づいて、前記第一入力値の暗号文の平文と前記第二入力値との積に雑音を足したデータの暗号文を前記雑音入り積の暗号文として生成する暗号文生成装置とを含む事を特徴とする多者分散乗算装置。

[請求項7] 前記第二装置は、前記第一装置との通信に不正が行われた否かを確認する結果確認証明装置を有する請求項６に記載の多者分散乗算装置。

[請求項8] 第一装置と第二装置との相互通信により、前記装置間での対話の正当性を識別する多者分散乗算方法であって、

前記第一装置に入力するシステムパラメターを利用することにより、前記第一装置から第一公開鍵を公開すると共に、前記第二装置に入力するシステムパラメターを利用することにより、前記第二装置から第二公開鍵を公開し、

前記システムパラメターと乱数とに基づいて、前記第一装置に入力

する第一入力値のコミットメントを生成する処理と、

前記システムパラメターと乱数と前記第一公開鍵とに基づいて、前記第一入力値の暗号文を生成する処理と、

前記システムパラメターと前記暗号文生成用の乱数と前記第一公開鍵及び前記第二公開鍵とに基づいて、前記第一入力値の範囲を証明する証明文を生成する処理と、

前記システムパラメターと前記第一公開鍵と自己が保有する秘密鍵とに基づいて、前記第二装置から送信される雑音入り暗号文を復号して復号文を生成する処理と、

前記復号文から雑音を除去する事により積の分散を生成する処理と、

前記システムパラメターと乱数とに基づいて、前記第二装置に入力する第二入力値のコミットメントを生成する処理と、

前記システムパラメターと前記第一公開鍵と前記第二公開鍵と前記証明文とに基づいて、前記第一入力値の暗号文の平文が前記範囲にあることを検証する処理と、

自己が保有する積の分散を生成する処理と、

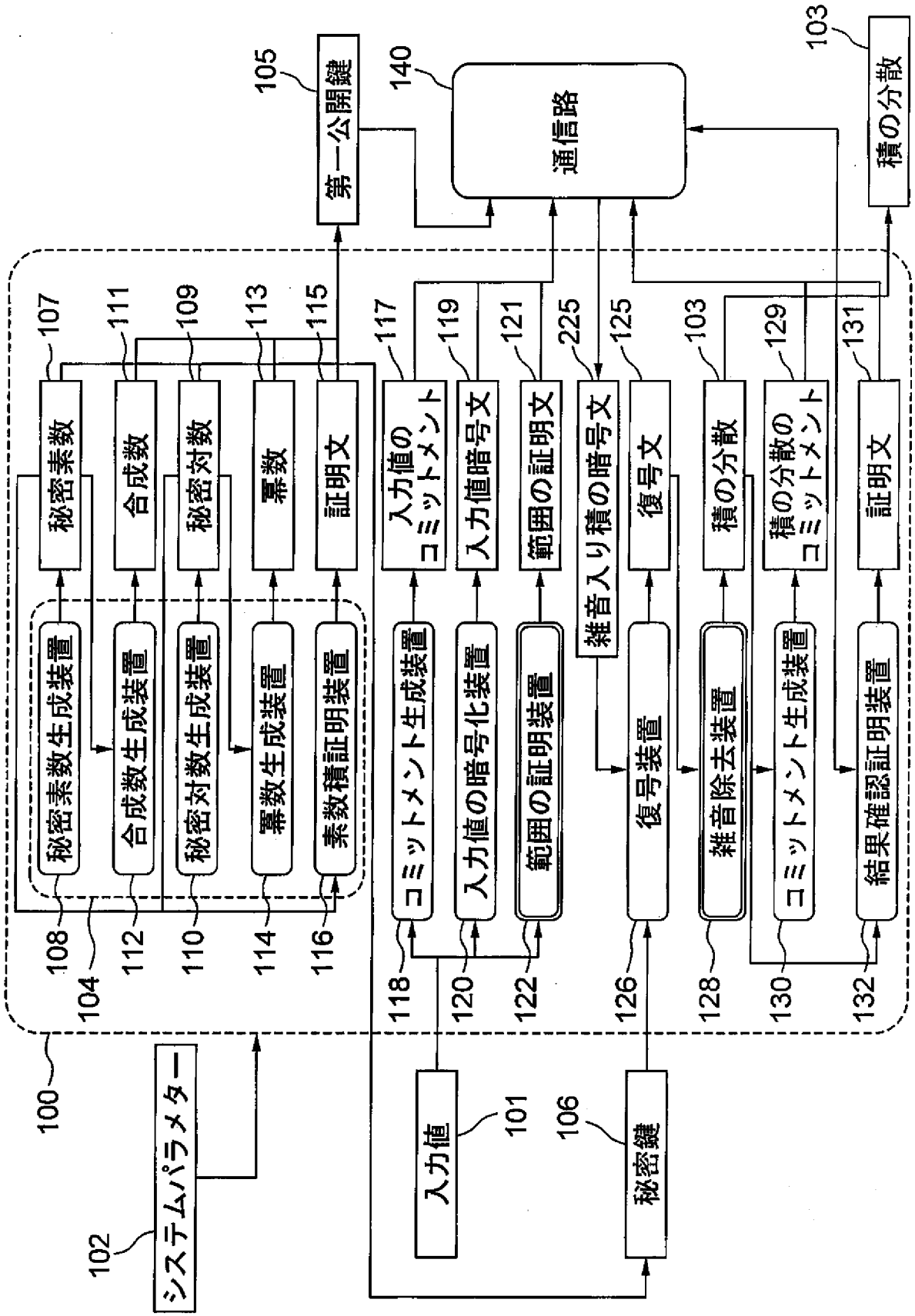
前記第一入力値の暗号文と前記第二入力値と前記積の分散とに基づいて、前記第一入力値の暗号文の平文と前記第二入力値との積に雑音を足したデータの暗号文を前記雑音入り積の暗号文として生成する処理とを実行する事を特徴とする多者分散乗算方法。

[請求項9] 前記第一装置において、前記第二装置との通信に不正が行われた否かを確認する処理を行う請求項８に記載の多者分散乗算方法。

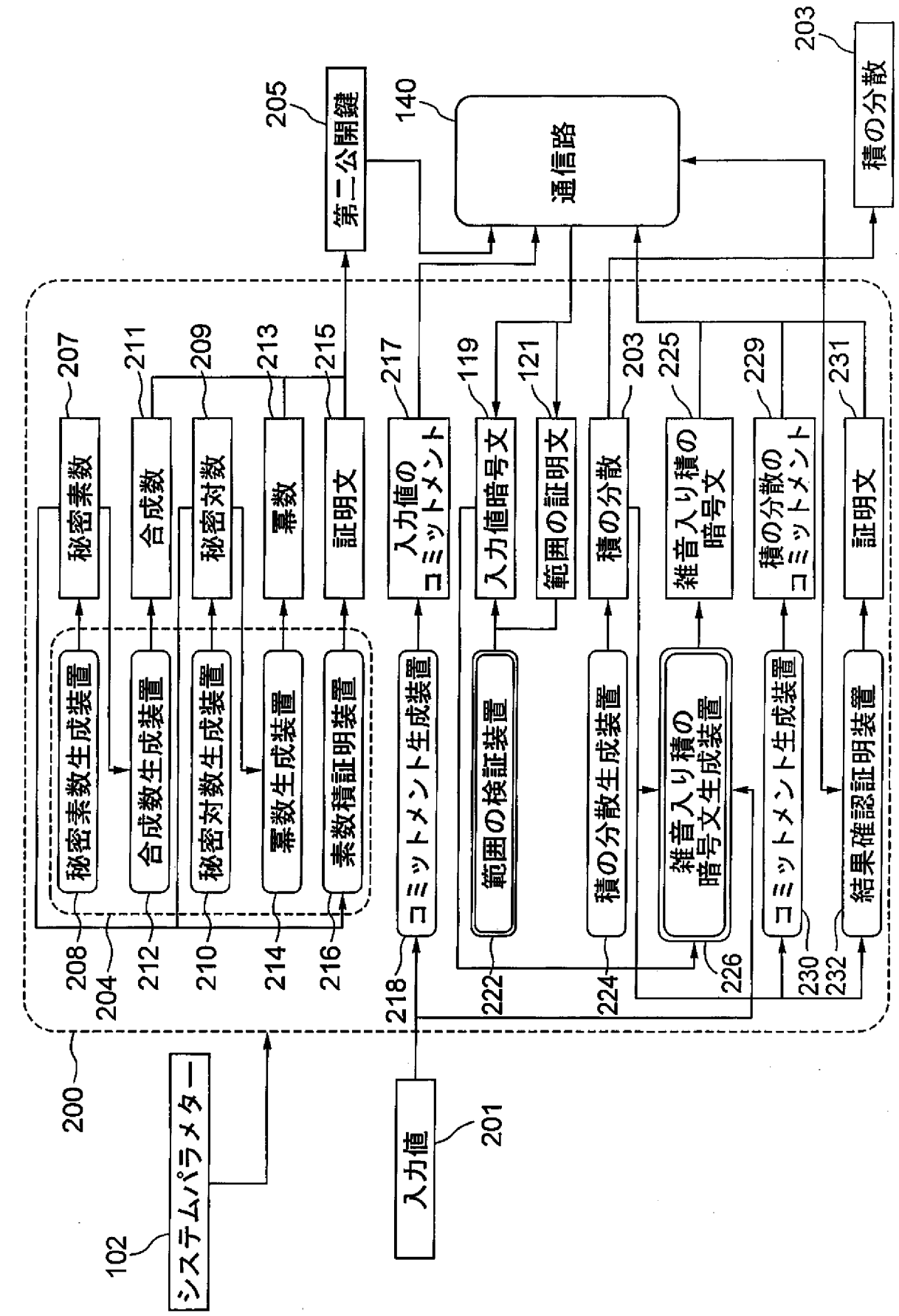
[請求項10] 前記第二装置において、前記第一装置との通信に不正が行われた否かを確認する処理を実行する請求項８に記載の多者分散乗算方法。

WO 2010/041690 PCT/JP2009/067506

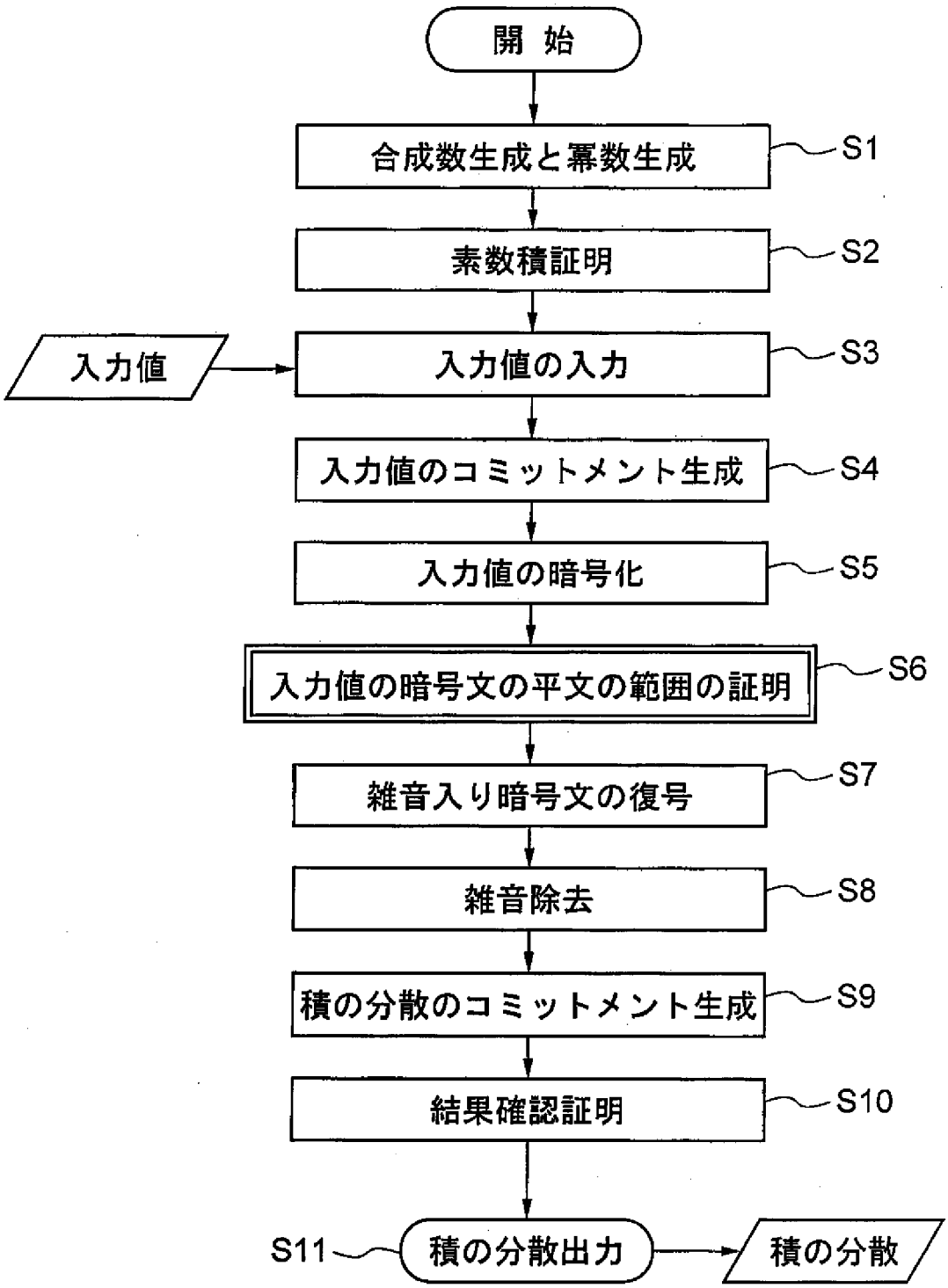
[図1]



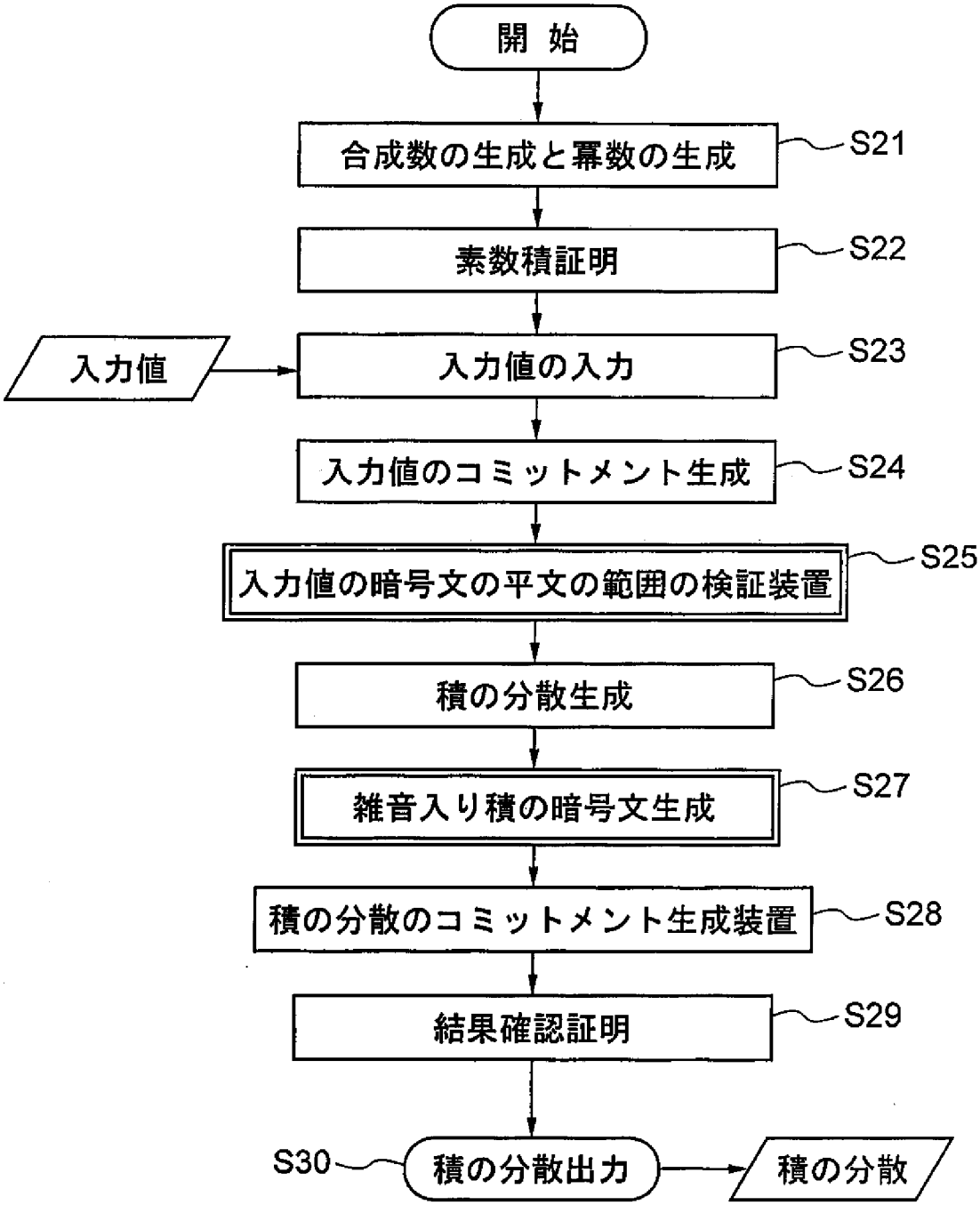
[図2]


200
システムパラメター
102
入力値
201
秘密素数生成装置
合成数生成装置
秘密対数生成装置
冪数生成装置
素数積証明装置
コミットメント生成装置
範囲の検証装置
積の分散生成装置
雑音入り積の暗号文生成装置
コミットメント生成装置
結果確認証明装置
208
204
212
210
214
216
218
222
224
226
230
232
秘密素数
合成数
秘密対数
冪数
証明文
入力値のコミットメント
入力値暗号文
範囲の証明文
積の分散
雑音入り積の暗号文
積の分散のコミットメント
証明文
207
211
209
213
215
217
119
121
203
225
229
231
第二公開鍵
205
通信路
140
積の分散
203

[図3]


開 始
合成数生成と冪数生成
S1
素数積証明
S2
入力値
入力値の入力
S3
入力値のコミットメント生成
S4
入力値の暗号化
S5
入力値の暗号文の平文の範囲の証明
S6
雑音入り暗号文の復号
S7
雑音除去
S8
積の分散のコミットメント生成
S9
結果確認証明
S10
S11
積の分散出力
積の分散

[図4]


開 始
合成数の生成と冪数の生成
S21
素数積証明
S22
入力値
入力値の入力
S23
入力値のコミットメント生成
S24
入力値の暗号文の平文の範囲の検証装置
S25
積の分散生成
S26
雑音入り積の暗号文生成
S27
積の分散のコミットメント生成装置
S28
結果確認証明
S29
S30
積の分散出力
積の分散

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/067506

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-216774 A (Nippon Telegraph And Telephone Corp.), 04 August 2000 (04.08.2000), paragraphs [0033] to [0058] (Family: none)	1-10
A	WO 2007/018311 A2 (NEC Corp.), 15 February 2007 (15.02.2007), page 16, line 25 to page 22, line 3 & EP 1921793 A2	1-10
A	WO 99/62221 A1 (CERTCO INC.), 02 December 1999 (02.12.1999), page 11, line 13 to page 40, line 32 & US 6237097 B1	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December, 2009 (15.12.09)	28 December, 2009 (28.12.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０６７５０６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2000-216774 A（日本電信電話株式会社）2000.08.04, 段落【００３３】～【００５８】（ファミリーなし）	1-10
A	WO 2007/018311 A2（日本電気株式会社）2007.02.15, 第１６頁第２５行目～第２２頁第３行目 & EP 1921793 A2	1-10
A	WO 99/62221 A1 (CERTCO INCORPORATED) 1999.12.02, 第１１頁第１３行目～第４０頁第３２行目 & US 6237097 B1	1-10

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １５．１２．２００９	国際調査報告の発送日 ２８．１２．２００９
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３８５７ 鳥居　稔 電話番号　０３－３５８１－１１０１　内線　３５４６