(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5434925号
(P5434925)

(45)発行日　平成26年3月5日(2014.3.5)　(24)登録日　平成25年12月20日(2013.12.20)

(51)Int.Cl.　　F I
G09C 1/00 (2006.01)　　G09C 1/00 660D
H04L 9/08 (2006.01)　　H04L 9/00 601C

請求項の数 10　(全 18 頁)

(21)出願番号　特願2010-532943 (P2010-532943)
(86)(22)出願日　平成21年10月7日 (2009.10.7)
(86)国際出願番号　PCT/JP2009/067506
(87)国際公開番号　WO2010/041690
(87)国際公開日　平成22年4月15日 (2010.4.15)
審査請求日　平成24年9月7日 (2012.9.7)
(31)優先権主張番号　特願2008-260509 (P2008-260509)
(32)優先日　平成20年10月7日 (2008.10.7)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100079164
弁理士　高橋　勇
(72)発明者　古川　潤
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　久慈　渉

最終頁に続く

(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

(57)【特許請求の範囲】
【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か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か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か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第一の装置に入力する第一入力値の範囲を証明する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か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か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か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。
【発明の詳細な説明】
【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ター１０２に基づいて、2κ＋μ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]∈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（2κ+μ）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タ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ター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、2κ+μ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、2κ+μ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]∈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]∈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2κ+μ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2κ+μ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］∈ $Z/n[2]^2Z$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、γ[1]=η[12]^2、γ[2]=η[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] ∈ 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] ∈ 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] ∈ 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] ∈ 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 $\rho \in [0,1]^{|n[2]|+\mu}$、$\delta = \gamma[1]^{s[1]}\ \underline{\gamma[2]^{\rho}}$を生成する。そして、前記範囲の証明装置１２２は、

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

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

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

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

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、

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

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

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

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）。

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

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

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

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

【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、$L:Z/n[1]^2Z \rightarrow Z/n[1]Z; c \rightarrow (c\lambda\ -1) / n[1] \bmod n[1]$ 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 ∈ Z、r ∈ $Z/n[1]^{2}Z$,s,u,v ∈ 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。

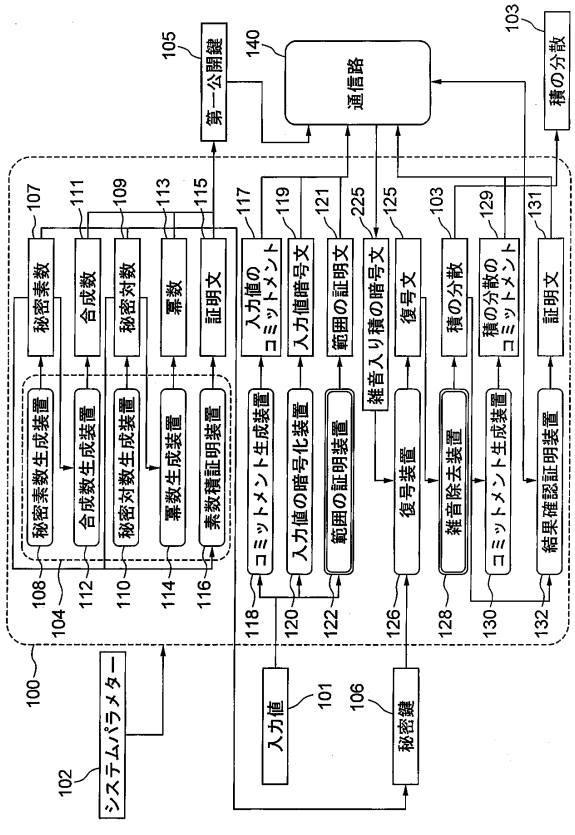
【符号の説明】

【００９４】

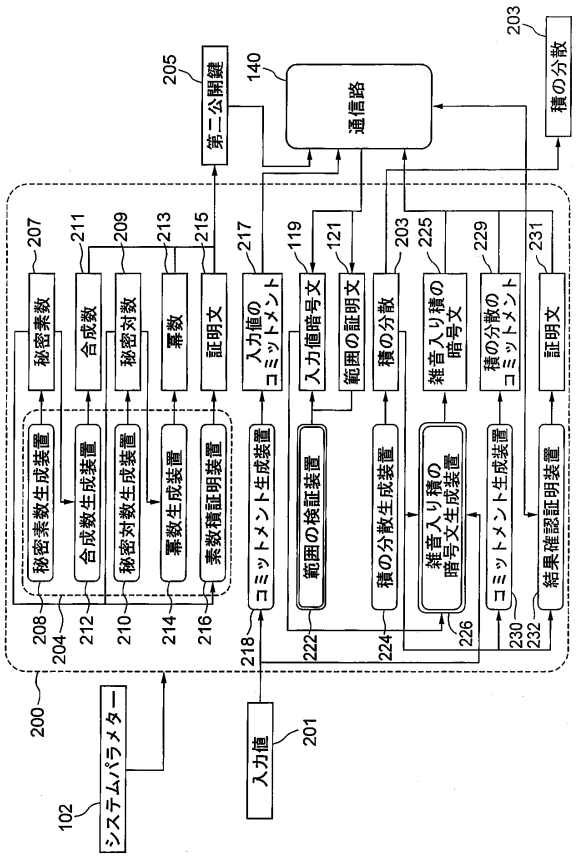
１００　第一装置
１０４　初期設定装置
１０８　秘密素数生成装置
１１０　秘密対数生成装置
１１２　合成数生成装置
１１４　冪数生成装置
１１６　素数積証明装置
１１８　コミットメント生成装置
１２０　入力値の暗号化装置
１２２　範囲の証明装置
１２６　復号装置
１２８　雑音除去装置
１３０　コミットメント生成装置
１３２　結果確認証明装置
１４０　通信路
２００　第二装置
２０４　初期設定装置
２０８　秘密素数生成装置
２１０　秘密対数生成装置
２１２　合成数生成装置
２１４　冪数生成装置
２１６　素数積証明装置

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

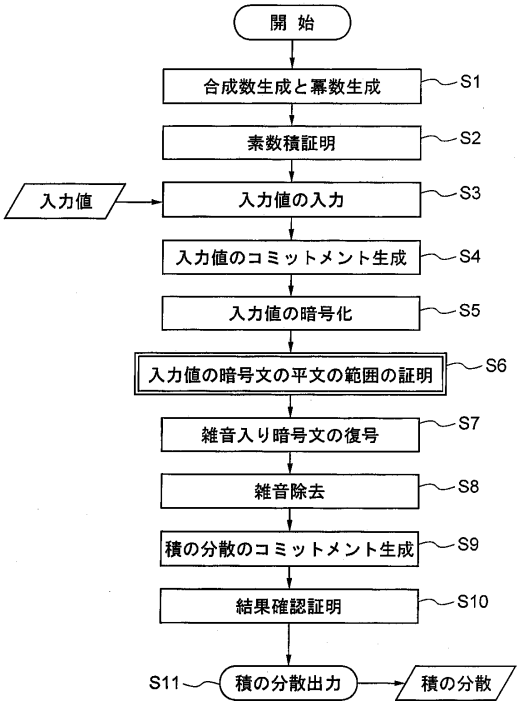
【図１】



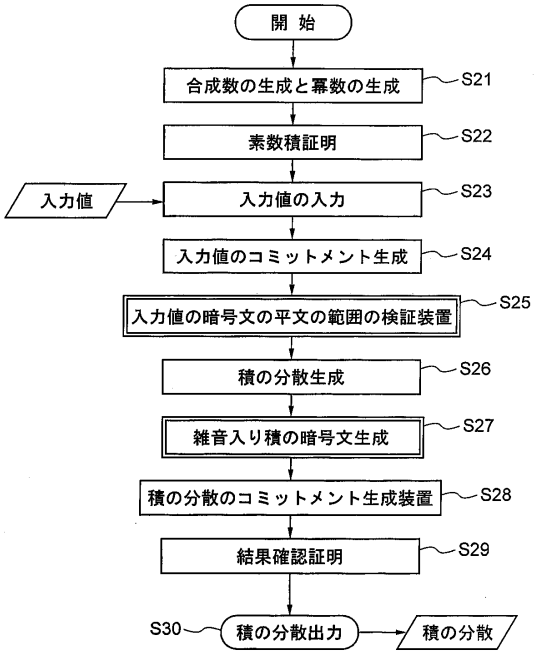
【図２】



【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

フロントページの続き

(56)参考文献　特開２０００－２１６７７４（ＪＰ，Ａ）
国際公開第２００７／０１８３１１（WO，Ａ１）
国際公開第９９／０６２２２１（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／０８