(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
2022年6月30日(30.06.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/137447 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2020/048498

(22) 国際出願日： 2020年12月24日(24.12.2020)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人:三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

(72) 発明者:廣政 良(**HIROMASA, Ryo**); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

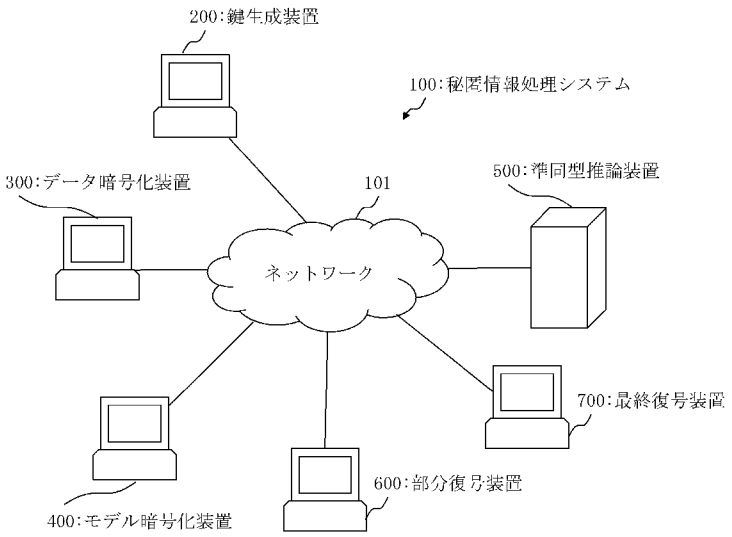
(74) 代理人: 溝井国際特許業務法人(**MIZOI INTERNATIONAL PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号３階 Kanagawa (JP).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM,

(54) **Title:** CONFIDENTIAL INFORMATION PROCESSING SYSTEM, AND CONFIDENTIAL INFORMATION PROCESSING METHOD

(54) 発明の名称： 秘匿情報処理システムおよび秘匿情報処理方法



101 Network
100 Confidential information processing system
200 Key generation device
300 Data encryption device
400 Model encryption device
500 Homomorphic inference device
600 Partial decryption device
700 Final decryption device

(57) **Abstract:** A homomorphic inference device (500) divides a model ciphertext into a ciphertext for inference and a ciphertext for calculation, generates a preliminary result ciphertext by a homomorphic computation algorithm without decrypting the ciphertext for calculation and data ciphertext, and generates an inference result ciphertext by a homomorphic computation algorithm using the preliminary result ciphertext and the ciphertext for inference without decrypting these. A partial decryption device (600) performs partial decryption on the inference result ciphertext using a secret key for models and generates a partial decryption result. A final decryption device (700) decrypts the inference result from the partial decryption result using a secret key for data.

WO 2022/137447 A1

［続葉有］

ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一　国際調査報告（条約第21条(3)）

(57) 要約：準同型推論装置（５００）は、モデル暗号文を推論用暗号文と計算用暗号文とに分割し、前記計算用暗号文とデータ暗号文とを復号せずに準同型演算アルゴリズムによって事前結果暗号文を生成し、前記事前結果暗号文と前記推論用暗号文とを復号せずに用いて準同型演算アルゴリズムによって推論結果暗号文を生成する。部分復号装置（６００）は、モデル用秘密鍵を用いて前記推論結果暗号文に対する部分復号を行って部分復号結果を生成する。最終復号装置（７００）は、データ用秘密鍵を用いて前記部分復号結果から推論結果を復号する。

明　細　書

発明の名称 ： 秘匿情報処理システムおよび秘匿情報処理方法

技術分野

[0001] 本開示は、秘匿情報処理に関するものである。

背景技術

[0002] 準同型暗号は、データを暗号化したまま演算できる暗号技術である。

昨今、クラウドサービスの利用が広まりつつあるが、クラッキングの懸念およびクラウドの信頼性の懸念から、クラウド上ではデータを暗号化して保管することが考えられる。

また、準同型暗号は、暗号化されているデータに対して、復号することなく演算を施すことができる。

そのため、準同型暗号は、安全性を損なうことなくクラウドサービスの利用を可能とする。

[0003] ニューラルネットワークは、画像および動画の認識に有用な技術であり、入力層と（複数の）中間層と出力層との３種類の層からなる。

入力層は、入力データを受け付けるための層である。

中間層は、入力データまたは他の中間層の計算結果に対して特定の計算を行うための層である。

出力層は、中間層の最終の計算結果を出力するための層である。

[0004] 近年、高い推論精度を達成するニューラルネットワークが盛んに研究されている。そのようなニューラルネットワークは非常に多数の中間層を持ち、その推論処理には多大な計算量を要する。

そのため、計算能力の低い端末では、このようなニューラルネットワークの推論処理を実行することが困難である。

そこで、高い計算能力を持ったクラウドに推論処理を委託することが考えられる。

[0005] 監視カメラの映像などのプライベートなデータがニューラルネットワーク

の入力データになる場合、入力データをクラウドから秘匿したまま、ニューラルネットワークの推論処理を行わなければならない。

その場合、準同型暗号を用いて入力データを暗号化したままニューラルネットワークによる推論処理を行うことで、データ提供者のプライバシーを保ちつつクラウドへ推論処理を委託することができる。

[0006] しかし、ニューラルネットワークの中間層の計算を定義する推論モデルデータが暗号化されなければ、推論モデルデータのパラメータ情報および推論モデルデータを生成するための学習に利用した学習データに関する情報が漏洩する可能性がある。

[0007] また、入力データ提供者が推論モデル提供者の推論モデルデータを利用してクラウド上で推論処理を行うサービスには次のような要件がある。

入力データ提供者と推論モデル提供者が入力データと推論モデルデータを共に秘匿したままクラウドに推論処理を委託することを想定する。その場合、入力データが入力データ提供者の暗号化鍵で暗号化されていて、且つ、推論モデルデータが推論モデル提供者の暗号化鍵で暗号化されている必要がある。

[0008] 特許文献１は、入力データと推論モデルデータを共に暗号化したままでの畳み込みニューラルネットワークの推論処理を開示している。

先行技術文献

非特許文献

[0009] 非特許文献1：H. Chen, W. Dai, M. Kim, Y. Song. “Efficient Multi-key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference”. In ACM CCS, page 395-412, 2019.

発明の概要

発明が解決しようとする課題

[0010] 非特許文献１の方法は、複数鍵準同型暗号と呼ばれる暗号技術を利用することで、入力データが入力データ提供者の暗号化鍵で暗号化されたまま、且つ、推論モデルデータが推論モデル提供者の暗号化鍵で暗号化されたまま、推論処理を実現する。

複数鍵準同型暗号は、準同型暗号方式の一種であり、異なる暗号化鍵で暗号化されている複数の暗号文を復号することなく複数の暗号文に対して演算を施すことができる。

[0011] 但し、非特許文献１の方法によって実現される推論処理は、畳み込みニューラルネットワークの推論処理である。

[0012] 本開示は、入力データと推論モデルデータとを共に暗号化したままで再帰的ニューラルネットワークの推論処理を実現できるようにすることを目的とする。

課題を解決するための手段

[0013] 本開示の秘匿情報処理システムは、

第１行列と第２行列を連結して得らえる推論モデルデータを暗号化して得られるモデル暗号文を、前記第１行列の暗号文に相当する推論用暗号文と、前記第２行列の暗号文に相当する計算用暗号文と、に分割するモデル分割部と、

前記計算用暗号文と、入力データを暗号化して得られるデータ暗号文と、を復号せずに、準同型演算アルゴリズムによって、前記第１行列と前記入力データを表すベクトルの積の暗号文に相当する事前結果暗号文を生成する事前計算部と、

前記事前結果暗号文と前記推論用暗号文とを復号せずに用いて、準同型演算アルゴリズムによって、前記入力データに対する推論結果の暗号文である推論結果暗号文を生成する準同型推論部と、

前記モデル暗号文のための秘密鍵であるモデル用秘密鍵を用いて、前記推論結果暗号文に対する部分復号を行って、部分復号結果を生成する部分復号

部と、

前記データ暗号文のための秘密鍵であるデータ用秘密鍵を用いて、前記部分復号結果から前記入力データに対する前記推論結果を復号する最終復号部と、を備える。

発明の効果

[0014] 本開示によれば、入力データと推論モデルデータとを共に暗号化したままで再帰的ニューラルネットワークの推論処理を実現することができる。

図面の簡単な説明

[0015] [図1]実施の形態１における秘匿情報処理システム１００の構成図。

[図2]実施の形態１における鍵生成装置２００の構成図。

[図3]実施の形態１におけるデータ暗号化装置３００の構成図。

[図4]実施の形態１におけるモデル暗号化装置４００の構成図。

[図5]実施の形態１における準同型推論装置５００の構成図。

[図6]実施の形態１における部分復号装置６００の構成図。

[図7]実施の形態１における最終復号装置７００の構成図。

[図8]実施の形態１におけるデータ用鍵ペアの管理の手順を示すフローチャート。

[図9]実施の形態１におけるモデル用鍵ペアの管理の手順を示すフローチャート。

[図10]実施の形態１における事前計算の手順を示すフローチャート。

[図11]実施の形態１における準同型推論の手順を示すフローチャート。

[図12]実施の形態１における推論結果暗号文の復号の手順を示すフローチャート。

[図13]実施の形態１における秘匿情報処理システム１００の各装置のハードウェア構成を説明するための図。

発明を実施するための形態

[0016] 実施の形態および図面において、同じ要素または対応する要素には同じ符号を付している。説明した要素と同じ符号が付された要素の説明は適宜に省

略または簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。

[0017] 実施の形態１．

秘匿情報処理システム１００について、図１から図１３に基づいて説明する。

[0018] ＊＊＊構成の説明＊＊＊

図１に基づいて、秘匿情報処理システム１００の構成を説明する。

秘匿情報処理システム１００は、鍵生成装置２００と、データ暗号化装置３００と、モデル暗号化装置４００と、準同型推論装置５００と、部分復号装置６００と、最終復号装置７００と、を備える。これらの装置は、ネットワーク１０１に接続され、ネットワーク１０１を介して互いに通信する。ネットワーク１０１の具体例はインターネットである。

[0019] 図２に基づいて、鍵生成装置２００の構成を説明する。

鍵生成装置２００は、プロセッサ２０１とメモリ２０２と補助記憶装置２０３と通信装置２０４と入出力インタフェース２０５といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0020] プロセッサ２０１は、演算処理を行うＩＣであり、他のハードウェアを制御する。例えば、プロセッサ２０１は、ＣＰＵ、ＤＳＰまたはＧＰＵである。

ＩＣは、Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔの略称である。

ＣＰＵは、Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略称である。

ＤＳＰは、Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒの略称である。

ＧＰＵは、Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略称である。

[0021] メモリ２０２は揮発性または不揮発性の記憶装置である。メモリ２０２は

、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ２０２はＲＡＭである。メモリ２０２に記憶されたデータは必要に応じて補助記憶装置２０３に保存される。

ＲＡＭは、Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙの略称である。

[0022] 補助記憶装置２０３は不揮発性の記憶装置である。例えば、補助記憶装置２０３は、ＲＯＭ、ＨＤＤまたはフラッシュメモリである。補助記憶装置２０３に記憶されたデータは必要に応じてメモリ２０２にロードされる。

ＲＯＭは、Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙの略称である。

ＨＤＤは、Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅの略称である。

[0023] 通信装置２０４はレシーバ及びトランスミッタである。例えば、通信装置２０４は通信チップまたはＮＩＣである。鍵生成装置２００の通信は通信装置２０４を用いて行われる。

ＮＩＣは、Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄの略称である。

[0024] 入出力インタフェース２０５は、入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース２０５はＵＳＢ端子であり、入力装置はキーボードおよびマウスであり、出力装置はディスプレイである。鍵生成装置２００の入出力は入出力インタフェース２０５を用いて行われる。

ＵＳＢは、Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓの略称である。

[0025] 鍵生成装置２００は、受付部２１０と鍵生成部２２０と出力部２３０といった要素を備える。これらの要素はソフトウェアで実現される。

[0026] 補助記憶装置２０３には、受付部２１０と鍵生成部２２０と出力部２３０としてコンピュータを機能させるための鍵生成プログラムが記憶されている。鍵生成プログラムは、メモリ２０２にロードされて、プロセッサ２０１によって実行される。

補助記憶装置２０３には、さらに、ＯＳが記憶されている。ＯＳの少なくとも一部は、メモリ２０２にロードされて、プロセッサ２０１によって実行

される。

プロセッサ２０１は、ＯＳを実行しながら、鍵生成プログラムを実行する。

ＯＳは、Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍの略称である。

[0027] 鍵生成プログラムの入出力データは記憶部２９０に記憶される。

メモリ２０２は記憶部２９０として機能する。但し、補助記憶装置２０３、プロセッサ２０１内のレジスタおよびプロセッサ２０１内のキャッシュメモリなどの他の記憶装置が、メモリ２０２の代わりに、又は、メモリ２０２と共に、記憶部２９０として機能してもよい。

[0028] 鍵生成装置２００は、プロセッサ２０１を代替する複数のプロセッサを備えてもよい。

[0029] 鍵生成プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0030] 図３に基づいて、データ暗号化装置３００の構成を説明する。

データ暗号化装置３００は、プロセッサ３０１とメモリ３０２と補助記憶装置３０３と通信装置３０４と入出力インタフェース３０５といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。これらのハードウェアは、鍵生成装置２００のハードウェアに対応する。

[0031] データ暗号化装置３００は、受付部３１０と公開鍵保管部３２０とデータ暗号化部３３０と出力部３４０といった要素を備える。これらの要素はソフトウェアで実現される。

[0032] 補助記憶装置３０３には、受付部３１０と公開鍵保管部３２０とデータ暗号化部３３０と出力部３４０としてコンピュータを機能させるためのデータ暗号化プログラムが記憶されている。データ暗号化プログラムは、メモリ３０２にロードされて、プロセッサ３０１によって実行される。

[0033] データ暗号化プログラムの入出力データは記憶部３９０に記憶される。

メモリ３０２は記憶部３９０として機能する。但し、データ暗号化装置３

００の他の記憶装置が、メモリ３０２の代わりに、又は、メモリ３０２と共に、記憶部３９０として機能してもよい。

[0034] データ暗号化装置３００は、プロセッサ３０１を代替する複数のプロセッサを備えてもよい。

[0035] データ暗号化プログラムは、不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0036] 図４に基づいて、モデル暗号化装置４００の構成を説明する。

モデル暗号化装置４００は、プロセッサ４０１とメモリ４０２と補助記憶装置４０３と通信装置４０４と入出力インタフェース４０５といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。これらのハードウェアは、鍵生成装置２００のハードウェアに対応する。

[0037] モデル暗号化装置４００は、受付部４１０公開鍵保管部４２０とモデル暗号化部４３０と出力部４４０といった要素を備える。これらの要素はソフトウェアで実現される。

[0038] 補助記憶装置４０３には、受付部４１０と公開鍵保管部４２０とモデル暗号化部４３０と出力部４４０としてコンピュータを機能させるためのモデル暗号化プログラムが記憶されている。モデル暗号化プログラムは、メモリ４０２にロードされて、プロセッサ４０１によって実行される。

[0039] モデル暗号化プログラムの入出力データは記憶部４９０に記憶される。

メモリ４０２は記憶部４９０として機能する。但し、モデル暗号化装置４００の他の記憶装置が、メモリ４０２の代わりに、又は、メモリ４０２と共に、記憶部４９０として機能してもよい。

[0040] モデル暗号化装置４００は、プロセッサ４０１を代替する複数のプロセッサを備えてもよい。

[0041] モデル暗号化プログラムは、不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0042] 図５に基づいて、準同型推論装置５００の構成を説明する。

準同型推論装置５００は、プロセッサ５０１とメモリ５０２と補助記憶装置５０３と通信装置５０４と入出力インタフェース５０５といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。これらのハードウェアは、鍵生成装置２００のハードウェアに対応する。

[0043] 準同型推論装置５００は、受付部５１０と公開鍵保管部５２１と暗号文保管部５２２とモデル分割部５３０と事前計算部５４１と事前結果保管部５４２と準同型推論部５５１と暗号文保管部５５２と出力部５６０といった要素を備える。これらの要素はソフトウェアで実現される。

[0044] 補助記憶装置５０３には、受付部５１０と公開鍵保管部５２１と暗号文保管部５２２とモデル分割部５３０と事前計算部５４１と事前結果保管部５４２と準同型推論部５５１と暗号文保管部５５２と出力部５６０としてコンピュータを機能させるための準同型推論プログラムが記憶されている。準同型推論プログラムは、メモリ５０２にロードされて、プロセッサ５０１によって実行される。

[0045] 準同型推論プログラムの入出力データは記憶部５９０に記憶される。

メモリ５０２は記憶部５９０として機能する。但し、準同型推論装置５００の他の記憶装置が、メモリ５０２の代わりに、又は、メモリ５０２と共に、記憶部５９０として機能してもよい。

[0046] 準同型推論装置５００は、プロセッサ５０１を代替する複数のプロセッサを備えてもよい。

[0047] 準同型推論プログラムは、不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0048] 図６に基づいて、部分復号装置６００の構成を説明する。

部分復号装置６００は、プロセッサ６０１とメモリ６０２と補助記憶装置６０３と通信装置６０４と入出力インタフェース６０５といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。これらのハードウェアは、鍵生成装置２００のハー

ドウェアに対応する。

[0049] 部分復号装置６００は、受付部６１０と秘密鍵保管部６２０と部分復号部６３０と出力部６４０といった要素を備える。これらの要素はソフトウェアで実現される。

[0050] 補助記憶装置６０３には、受付部６１０と秘密鍵保管部６２０と部分復号部６３０と出力部６４０としてコンピュータを機能させるための部分復号プログラムが記憶されている。部分復号プログラムは、メモリ６０２にロードされて、プロセッサ６０１によって実行される。

[0051] 部分復号プログラムの入出力データは記憶部６９０に記憶される。

メモリ６０２は記憶部６９０として機能する。但し、部分復号装置６００の他の記憶装置が、メモリ６０２の代わりに、又は、メモリ６０２と共に、記憶部６９０として機能してもよい。

[0052] 部分復号装置６００は、プロセッサ６０１を代替する複数のプロセッサを備えてもよい。

[0053] 部分復号プログラムは、不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0054] 図７に基づいて、最終復号装置７００の構成を説明する。

最終復号装置７００は、プロセッサ７０１とメモリ７０２と補助記憶装置７０３と通信装置７０４と入出力インタフェース７０５といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。これらのハードウェアは、鍵生成装置２００のハードウェアに対応する。

[0055] 最終復号装置７００は、受付部７１０と秘密鍵保管部７２０と最終復号部７３０と推論結果保管部７４０と出力部７５０といった要素を備える。これらの要素はソフトウェアで実現される。

[0056] 補助記憶装置７０３には、受付部７１０と秘密鍵保管部７２０と最終復号部７３０と推論結果保管部７４０と出力部７５０としてコンピュータを機能させるための最終復号プログラムが記憶されている。最終復号プログラムは

、メモリ７０２にロードされて、プロセッサ７０１によって実行される。

[0057] 最終復号プログラムの入出力データは記憶部７９０に記憶される。

メモリ７０２は記憶部７９０として機能する。但し、最終復号装置７００の他の記憶装置が、メモリ７０２の代わりに、又は、メモリ７０２と共に、記憶部７９０として機能してもよい。

[0058] 最終復号装置７００は、プロセッサ７０１を代替する複数のプロセッサを備えてもよい。

[0059] 最終復号プログラムは、不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0060] ＊＊＊動作の説明＊＊＊

秘匿情報処理システム１００の動作の手順は秘匿情報処理方法に相当する。また、秘匿情報処理システム１００の動作の手順は秘匿情報処理プログラムによる処理の手順に相当する。

[0061] 図８に基づいて、データ用鍵ペアの管理について説明する。

データ用鍵ペアは、後述する入力データd_tのための鍵ペアであり、データ用公開鍵とデータ用秘密鍵とで構成される。

データ用公開鍵は、入力データd_tを暗号化するための公開鍵である。

データ用秘密鍵は、データ用公開鍵に対応する秘密鍵である。データ用秘密鍵により、入力データd_tの暗号文を復号することができる。暗号文は、暗号化によって得られるデータである。

[0062] ステップＳ１０１からステップＳ１０４は、鍵生成装置２００によって実行される。

ステップＳ１０１において、受付部２１０は、パラメータλ_1を受け付ける。

パラメータλ_1は、データ用鍵ペアのための鍵生成パラメータである。例えば、パラメータλ_1は、利用者によって鍵生成装置２００に入力される。

[0063] ステップＳ１０２において、鍵生成部２２０は、パラメータλ_1を入力として鍵生成アルゴリズムを実行する。これにより、公開鍵PK_1および秘密鍵Ｓ

K_1が生成される。

公開鍵PK_1はデータ用公開鍵であり、秘密鍵SK_1はデータ用秘密鍵である。

[0064] 例えば、以下の文献（１）に記載された鍵生成アルゴリズムが使用される。

文献（１）：H. Chen, I. Chillotti, Y. Song. “Multi-key Homomorphic Encryption from TFHE”. In ASIACRYPT, pages 446-472, 2019.

[0065] ステップＳ１０３において、出力部２３０は、データ暗号化装置３００と準同型推論装置５００とのそれぞれに公開鍵PK_1を送信する。

[0066] ステップＳ１０４において、出力部２３０は、最終復号装置７００に秘密鍵SK_1を送信する。

[0067] ステップＳ１１１およびステップＳ１１２は、データ暗号化装置３００によって実行される。

ステップＳ１１１において、受付部３１０は、公開鍵PK_1を受信する。

ステップＳ１１２において、公開鍵保管部３２０は、公開鍵PK_1を記憶部２９０に保管する。

[0068] ステップＳ１２１およびステップＳ１２２は、準同型推論装置５００によって実行される。

ステップＳ１２１において、受付部５１０は、公開鍵PK_1を受信する。

ステップＳ１２２において、公開鍵保管部５２１は、公開鍵PK_1を記憶部５９０に保管する。

[0069] ステップＳ１３１およびステップＳ１３２は、最終復号装置７００によって実行される。

ステップＳ１３１において、受付部７１０は、秘密鍵SK_1を受信する。

ステップＳ１３２において、秘密鍵保管部７２０は、秘密鍵SK_1を記憶部７９０に保管する。なお、秘密鍵SK_1は外部に漏れないように厳重に保管さ

れる。

[0070] 図９に基づいて、モデル用鍵ペアの管理について説明する。

モデル用鍵ペアは、後述する推論モデルデータＭのための鍵ペアであり、モデル用公開鍵とモデル用秘密鍵とで構成される。

モデル用公開鍵は、推論モデルデータＭを暗号化するための公開鍵である。

モデル用秘密鍵は、モデル用公開鍵に対応する秘密鍵である。モデル用秘密鍵により、推論モデルデータＭの暗号文を復号することができる。

[0071] ステップＳ２０１からステップＳ２０４は、鍵生成装置２００によって実行される。

ステップＳ２０１において、受付部２１０は、パラメータλ_2を受け付ける。

パラメータλ_2は、モデル用鍵ペアのための鍵生成パラメータである。例えば、パラメータλ_2は、利用者によって鍵生成装置２００に入力される。

[0072] ステップＳ２０２において、鍵生成部２２０は、パラメータλ_2を入力として鍵生成アルゴリズムを実行する。これにより、公開鍵PK_2および秘密鍵SK_2が生成される。

公開鍵PK_2はモデル用公開鍵であり、秘密鍵SK_2はモデル用秘密鍵である。

[0073] 例えば、上記文献（１）に記載された鍵生成アルゴリズムが使用される。

[0074] ステップＳ２０３において、出力部２３０は、モデル暗号化装置４００と準同型推論装置５００とのそれぞれに公開鍵PK_2を送信する。

[0075] ステップＳ２０４において、出力部２３０は、部分復号装置６００に秘密鍵SK_2を送信する。

[0076] ステップＳ２１１およびステップＳ２１２は、モデル暗号化装置４００によって実行される。

ステップＳ２１１において、受付部４１０は、公開鍵PK_2を受信する。

ステップＳ２１２において、公開鍵保管部４２０は、公開鍵PK_2を記憶部

４９０に保管する。

[0077] ステップＳ２２１およびステップＳ２２２は、準同型推論装置５００によって実行される。

ステップＳ２２１において、受付部５１０は、公開鍵$ＰＫ_2$を受信する。

ステップＳ２２２において、公開鍵保管部５２１は、公開鍵$ＰＫ_2$を記憶部５９０に保管する。

[0078] ステップＳ２３１およびステップＳ２３２は、部分復号装置６００によって実行される。

ステップＳ２３１において、受付部６１０は、秘密鍵$ＳＫ_2$を受信する。

ステップＳ２３２において、秘密鍵保管部６２０は、秘密鍵$ＳＫ_2$を記憶部６９０に保管する。なお、秘密鍵$ＳＫ_2$は外部に漏れないように厳重に保管される。

[0079] 図１０に基づいて、推論結果の暗号文を得るための事前計算について説明する。

ステップＳ３０１からステップＳ３０３は、データ暗号化装置３００によって実行される。

ステップＳ３０１において、受付部３１０は、入力データ$ｄ_t$を受け付ける。

入力データ$ｄ_t$は、時刻ｔの入力データである。「ｔ」は１以上の整数（自然数）である。

入力データは、ｎ個の浮動小数点数から成るベクトルで表される。「ｎ」は１以上の整数である。

例えば、受付部３１０は、工場に設けられた各種センサによって時刻ｔに得られた計測値（浮動小数点数）を各種センサから収集する。収集された計測値が入力データ$ｄ_t$となる。

[0080] ステップＳ３０２において、データ暗号化部３３０は入力データ$ｄ_t$を暗号化する。具体的には、データ暗号化部３３０は、公開鍵$ＰＫ_1$を用いて入力データ$ｄ_t$に対して暗号化アルゴリズムを実行する。これにより、データ暗号文

Ｃ（d_t）が生成される。

データ暗号文Ｃ（d_t）は、暗号化された入力データd_t、すなわち、入力データd_tの暗号文である。

[0081] 例えば、上記文献（１）に記載された暗号化アルゴリズムによって、入力データd_tの各要素が暗号化される。

[0082] ステップＳ３０３において、出力部３４０は、データ暗号文Ｃ（d_t）を準同型推論装置５００に送信する。

[0083] ステップＳ３１１からステップＳ３１３は、モデル暗号化装置４００によって実行される。

ステップＳ３１１において、受付部４１０は、推論モデルデータＭを受け付ける。例えば、推論モデルデータＭは、利用者によってモデル暗号化装置４００に入力される。但し、推論モデルデータＭは、記憶部４９０に予め記憶されてもよい。

[0084] ステップＳ３１２において、モデル暗号化部４３０は推論モデルデータＭを暗号化する。具体的には、モデル暗号化部４３０は、公開鍵PK_2を用いて推論モデルデータＭに対して暗号化アルゴリズムを実行する。これにより、モデル暗号文Ｃ（Ｍ）が生成される。

モデル暗号文Ｃ（Ｍ）は、暗号化された推論モデルデータＭ、すなわち、推論モデルデータＭの暗号文である。

[0085] 例えば、上記文献（１）に記載された暗号化アルゴリズムが使用される。

[0086] 推論モデルデータＭについて説明する。

推論モデルデータＭは、推論モデル（Ｍ）のためのデータである。推論モデル（Ｍ）は、推論処理のための機械学習モデルであり、再帰的ニューラルネットワークで表される。具体的な再帰的ニューラルネットワークは「ＬＳＴＭ」である。

ＬＳＴＭは、Ｌｏｎｇ Ｓｈｏｒｔ－ｔｅｒｍ Ｍｅｍｏｒｙの略称である。

[0087] 推論モデルデータＭは、ｋ×（ｎ＋ｍ）の要素を持つ行列である。各要素

は浮動小数点数である。

「ｋ」は、１以上の整数である。

「ｎ」は、１以上の整数である（前述の通り）。

「ｍ」は、１以上の整数である。

[0088] 推論モデルデータＭに対して、Ｍ＝［Ｍ’｜｜Ｍ’’］が成り立つ。

「Ｍ’」は、ｋ×ｎの要素を持つ行列である。各要素は浮動小数点数である。

「Ｍ’’」は、ｋ×ｍの要素を持つ行列である。各要素は浮動小数点数である。

［Ｍ’｜｜Ｍ’’］は、行列Ｍ’と行列Ｍ’’を連結して得られる行列を意味する。

[0089] 推論モデルデータＭを用いた推論処理は式（１）で表される。

[0090] [数1]

$$\mathrm{M}\cdot\begin{bmatrix}\mathrm{D}_{t-1}\\ \mathrm{d}_t\end{bmatrix}=\mathrm{M}'\cdot\mathrm{D}_{t-1}+\mathrm{M}''\cdot\mathrm{d}_t \qquad (式１)$$

[0091] 「D_{t-1}」は、時刻ｔ－１における推論結果であり、ｎ個の浮動小数点数から成るベクトルで表される。

「d_t」は、時刻ｔにおける入力データであり、ｎ個の浮動小数点数から成るベクトルで表される。

「・」は、行列とベクトルの掛け算を表す。

「＋」は、ベクトル同士の足し算を表す。

[0092] ステップＳ３１３から説明を続ける。

ステップＳ３１３において、出力部４４０は、モデル暗号文Ｃ（Ｍ）を準同型推論装置５００に送信する。

[0093] ステップＳ３２１からステップＳ３２６は、準同型推論装置５００によって実行される。

ステップＳ３２１において、受付部５１０は、データ暗号文Ｃ（d_t）を受信する。

そして、暗号文保管部５２２は、データ暗号文Ｃ（d_t）を記憶部５９０に保管する。

[0094] ステップＳ３２２において、受付部５１０は、モデル暗号文Ｃ（Ｍ）を受信する。

そして、暗号文保管部５２２は、モデル暗号文Ｃ（Ｍ）を記憶部５９０に保管する。

[0095] 以下、モデル暗号文を「Ｃ（Ｍ）」または「Ｗ」で表す。

[0096] モデル暗号文Ｗは式（２）で表すことができる。

[0097] [数2]

$$W=[W'||W''] \qquad (式2)$$

[0098] 「Ｗ’」は、推論用暗号文を表す。推論用暗号文Ｗ’は、推論モデルデータＭの暗号化に用いられる暗号化アルゴリズムによって暗号化された行列Ｍ’、すなわち、行列Ｍ’の暗号文に相当する。つまり、推論用暗号文Ｗ’は、ｋ×ｎの暗号化された要素を持つ行列である。

「Ｗ’’」は、計算用暗号文を表す。計算用暗号文Ｗ’’は、推論モデルデータＭの暗号化に用いられる暗号化アルゴリズムによって暗号化された行列Ｍ’’、すなわち、行列Ｍ’’の暗号文に相当する。つまり、計算用暗号文Ｗ’’は、ｋ×ｍの暗号化された要素を持つ行列である。

[0099] ステップＳ３２４において、モデル分割部５３０は、モデル暗号文Ｗを推論用暗号文Ｗ’と計算用暗号文Ｗ’’とに分割する。

[0100] ステップＳ３２５において、事前計算部５４１は、データ暗号文Ｃ（d_t）と計算用暗号文Ｗ’’を用いて、事前計算を実行する。

具体的には、事前計算部５４１は、計算用暗号文Ｗ’’とデータ暗号文Ｃ（d_t）とを復号せずに、事前結果暗号文Ｃ（D_t’’）を生成する。

[0101] 事前結果暗号文Ｃ（D_t’’）は、行列Ｍ’’と入力データd_tを表すベク

トルとの積を暗号化して得られる暗号文に相当する。

[0102] 事前結果暗号文Ｃ（D_t''）は、準同型演算アルゴリズムによって算出される。

準同型演算アルゴリズムは、準同型暗号（特に、複数鍵準同型暗号）のアルゴリズムである。

例えば、上記文献（１）に記載された準同型演算アルゴリズムが使用される。

[0103] ステップＳ３２６において、事前結果保管部５４２は、事前結果暗号文Ｃ（D_t''）を記憶部５９０に保管する。

[0104] 図１１に基づいて、準同型推論について説明する。

ステップＳ４０１からステップＳ４０３は、準同型推論装置５００によって実行される。

ステップＳ４０１において、モデル分割部５３０は、モデル暗号文Ｗを推論用暗号文Ｗ’と計算用暗号文Ｗ’’とに分割する。

[0105] ステップＳ４０２において、準同型推論部５５１は、前回結果暗号文Ｃ（D_{t-1}）と推論用暗号文Ｗ’を用いて、中間推論処理を実行する。

前回結果暗号文Ｃ（D_{t-1}）は、前回の入力データd_{t-1}に対する暗号化された推論結果、すなわち、前回の推論結果の暗号文である。

[0106] 具体的には、準同型推論部５５１は、前回結果暗号文Ｃ（D_{t-1}）と推論用暗号文Ｗ’とを復号せずに用いて、中間結果暗号文Ｃ（D_{t-1}'）を生成する。

中間結果暗号文Ｃ（D_{t-1}'）は、行列Ｍ’と前回の入力データd_{t-1}に対する推論結果を表すベクトルとの積を暗号化して得られる暗号文に相当する。

[0107] 中間結果暗号文Ｃ（D_{t-1}'）は、準同型演算アルゴリズムによって算出される。

例えば、上記文献（１）に記載された準同型演算アルゴリズムが使用される。

[0108] ステップＳ４０３において、準同型推論部５５１は、中間結果暗号文Ｃ（D_{t-1}’）と事前結果暗号文Ｃ（D_t’’）を用いて、最終推論処理を実行する。

[0109] 具体的には、準同型推論部５５１は、中間結果暗号文Ｃ（D_{t-1}’）と事前結果暗号文Ｃ（D_t’’）とを復号せずに用いて、推論結果暗号文Ｃ（D_t）を生成する。

推論結果暗号文Ｃ（D_t）は、今回の入力データd_tに対する暗号化された推論結果、すなわち、今回の推論結果の暗号文である。

[0110] 推論結果暗号文Ｃ（D_t）は、中間結果暗号文Ｃ（D_{t-1}’）を復号して得られるベクトルと事前結果暗号文Ｃ（D_t’’）を復号して得られるベクトルとの足し算の結果を暗号化して得られる暗号文に相当する。

[0111] 推論結果暗号文Ｃ（D_t）は、準同型演算アルゴリズムによって算出される。

例えば、上記文献（１）に記載された準同型演算アルゴリズムが使用される。

[0112] ステップＳ４０４において、暗号文保管部５５２は、推論結果暗号文Ｃ（D_t）を記憶部５９０に保管する。

[0113] 図１２に基づいて、推論結果暗号文Ｃ（D_t）の復号について説明する。

ステップＳ５０１およびステップＳ５０２は、準同型推論装置５００によって実行される。

ステップＳ５０１において、出力部５６０は、推論結果暗号文Ｃ（D_t）を記憶部５９０から取得する。

ステップＳ５０２において、出力部５６０は、推論結果暗号文Ｃ（D_t）を部分復号装置６００と最終復号装置７００とのそれぞれに送信する。

[0114] ステップＳ５１１からステップＳ５１３は、部分復号装置６００によって実行される。

ステップＳ５１１において、受付部６１０は、推論結果暗号文Ｃ（D_t）を受信する。

[0115] ステップＳ５１２において、部分復号部６３０は、秘密鍵SK_2を用いて推論結果暗号文Ｃ（D_t）に対して部分復号を行う。これにより、部分復号結果Ｃ（$D_{2,t}$）が生成される。

[0116] 具体的には、部分復号部６３０は、式（３）を計算することによって、部分復号結果Ｃ（$D_{2,t}$）の各要素$d'_{2,t}$を算出する。

つまり、部分復号部６３０は、推論結果暗号文Ｃ（D_t）の要素であるベクトルと秘密鍵SK_2を表すベクトルとの内積を算出し、算出した内積と確率分布から選択される値との足し算の結果を算出する。算出される結果が部分復号結果Ｃ（$D_{2,t}$）の各要素$d'_{2,t}$となる。

[0117] [数3]

$$e \leftarrow \chi,$$

$$d'_{2,t} = \langle c, SK_2 \rangle + e \qquad \text{（式３）}$$

[0118] 「ｃ」は、推論結果暗号文Ｃ（D_t）の一つの要素を構成するベクトルを表す。推論結果暗号文Ｃ（D_t）はベクトルまたは行列である。推論結果暗号文Ｃ（D_t）を表すベクトルまたは行列は、例えば、上記文献（１）に記載された暗号方式の暗号文を要素として持つ。

「Ｘ」は、特定の確率分布を表す。例えば、確率分布Ｘは、０，１／2^{32}，・・・，（$2^{32}-1$）／2^{32}を値としてとる離散正規分布である。

「ｅ」は、確率分布Ｘに沿って選ばれた値を表す。

＜ｃ，SK_2＞は、ベクトルＣと秘密鍵SK_2を表すベクトルの内積を表す。

[0119] ステップＳ５１３において、出力部６４０は、部分復号結果Ｃ（$D_{2,t}$）を最終復号装置７００に送信する。

[0120] ステップＳ５２１からステップＳ５２４は、最終復号装置７００によって実行される。

ステップＳ５２１において、受付部７１０は、推論結果暗号文Ｃ（D_t）を

受信する。

[0121] ステップＳ５２２において、受付部７１０は、部分復号結果Ｃ（$D_{2,t}$）を受信する。

[0122] ステップＳ５２３において、最終復号部７３０は、秘密鍵SK_1を用いて、推論結果暗号文Ｃ（D_t）と部分復号結果Ｃ（$D_{2,t}$）とから、推論結果データD_tを復号する。

具体的には、最終復号部７３０は、式（４）を計算することによって、推論結果データD_tの各要素d'_tを算出する。

つまり、最終復号部７３０は、推論結果暗号文Ｃ（D_t）の要素であるベクトルと秘密鍵SK_1を表すベクトルとの内積を算出し、算出した内積と部分復号結果Ｃ（$D_{2,t}$）の要素との足し算によって得られる和を算出し、算出した和に基づいて推論結果データD_tの各要素d'_tを決定する。

[0123] [数4]

$$d'_{1,t} = \langle c, SK_1 \rangle$$

$$d'_t = \left[d'_{1,t} + d'_{2,t} \right]_{1/4} \qquad (式４)$$

[0124] ＜ｃ，SK_1＞は、ベクトルＣと秘密鍵SK_1を表すベクトルの内積を表す。

$[A]_{1/4}$は、値Ａが１／４に近ければ１を表し、値Ａが１／４に近くなければ０を表す。具体的には、$[A]_{1/4}$は、値Ａと１／４の差が閾値より小さければ１を表し、値Ａと１／４の差が閾値より大きければ０を表す。また、$[A]_{1/4}$は、値Ａが１／４の差が閾値と等しければ１または０を表す。

[0125] ステップＳ５２４において、推論結果保管部７４０は、推論結果データD_tを記憶部７９０に保管する。

また、出力部７５０は、推論結果データD_tを出力する。例えば、出力部７

５０は、推論結果データD_tをディスプレイに表示する。

[0126] ＊＊＊実施の形態１の効果＊＊＊

秘匿情報処理システム１００は、入力データを暗号化したまま、再帰的ニューラルネットワークによる推論処理を実行できる。そのため、秘匿情報処理システム１００により、データ提供者のプライバシーを保護したまま、推論処理をクラウドに委託することができる。

[0127] 秘匿情報処理システム１００は、推論モデルデータを暗号化したまま、再帰的ニューラルネットワークによる推論処理を実行できる。そのため、秘匿情報処理システム１００により、モデル提供者のプライバシーを保護したまま、推論処理をクラウドに委託することができる。

[0128] 秘匿情報処理システム１００は、再帰的ニューラルネットワークにおける時刻ｔの推論処理を実行する前に、時刻ｔの推論処理において時刻ｔ－１の推論結果データに依存しない処理（事前処理）を実行することができる。

入力データと推論モデルデータとを暗号化したまま推論処理を実行するためには、複数鍵準同型暗号の性質により、暗号文拡大処理を行う必要がある。複数鍵準同型暗号は、上記文献（１）に記載された準同型暗号方式である。暗号文拡大処理は、例えば、秘密鍵SK_1で復号できる暗号文を秘密鍵SK_1と秘密鍵SK_2の両方を用いることで復号できる暗号文に変換する処理である。

暗号文拡大処理を事前計算処理として実行することで、実際の推論処理時に暗号文拡大処理などによる計算オーバヘッドを削減することができる。つまり、入力データと推論モデルデータを暗号化したままでの再帰的ニューラルネットワークの推論処理を効率的に実現できる。

[0129] ＊＊＊実施の形態１の補足＊＊＊

秘匿情報処理システム１００に備わる複数の装置のうち２つ以上の装置を１つの装置にまとめてもよい。例えば、データ暗号化装置３００とモデル暗号化装置４００を１つの装置にまとめてもよいし、部分復号装置６００と最終復号装置７００を１つの装置にまとめてもよい。

装置間のデータの送受信は、データの郵送または利用者によるデータの入出力に置き換えてもよい。

[0130] 図１３に基づいて、鍵生成装置２００のハードウェア構成を説明する。

鍵生成装置２００は処理回路２０９を備える。

処理回路２０９は、鍵生成装置２００の要素を実現するハードウェアである。

処理回路２０９は、専用のハードウェアであってもよいし、メモリ２０２に格納されるプログラムを実行するプロセッサ２０１であってもよい。

[0131] 処理回路２０９が専用のハードウェアである場合、処理回路２０９は、例えば、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。

ＡＳＩＣは、Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔの略称である。

ＦＰＧＡは、Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙの略称である。

[0132] 鍵生成装置２００は、処理回路２０９を代替する複数の処理回路を備えてもよい。

[0133] 処理回路２０９において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0134] このように、鍵生成装置２００の機能はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0135] データ暗号化装置３００、モデル暗号化装置４００、準同型推論装置５００、部分復号装置６００および最終復号装置７００のハードウェア構成は、鍵生成装置２００のハードウェア構成と同様である。

[0136] 実施の形態１は、好ましい形態の例示であり、本開示の技術的範囲を制限することを意図するものではない。実施の形態１は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。

[0137] 秘匿情報処理システム１００の各装置の要素である「部」は、「処理」、「工程」、「回路」または「サーキットリ」と読み替えてもよい。

符号の説明

[0138] １００ 秘匿情報処理システム、１０１ ネットワーク、２００ 鍵生成装置、２０１ プロセッサ、２０２ メモリ、２０３ 補助記憶装置、２０４ 通信装置、２０５ 入出力インタフェース、２０９ 処理回路、２１０ 受付部、２２０ 鍵生成部、２３０ 出力部、２９０ 記憶部、３００ データ暗号化装置、３０１ プロセッサ、３０２ メモリ、３０３ 補助記憶装置、３０４ 通信装置、３０５ 入出力インタフェース、３１０ 受付部、３２０ 公開鍵保管部、３３０ データ暗号化部、３４０ 出力部、３９０ 記憶部、４００ モデル暗号化装置、４０１ プロセッサ、４０２ メモリ、４０３ 補助記憶装置、４０４ 通信装置、４０５ 入出力インタフェース、４１０ 受付部、４２０ 公開鍵保管部、４３０ モデル暗号化部、４４０ 出力部、４９０ 記憶部、５００ 準同型推論装置、５０１ プロセッサ、５０２ メモリ、５０３ 補助記憶装置、５０４ 通信装置、５０５ 入出力インタフェース、５１０ 受付部、５２１ 公開鍵保管部、５２２ 暗号文保管部、５３０ モデル分割部、５４１ 事前計算部、５４２ 事前結果保管部、５５１ 準同型推論部、５５２ 暗号文保管部、５６０ 出力部、５９０ 記憶部、６００ 部分復号装置、６０１ プロセッサ、６０２ メモリ、６０３ 補助記憶装置、６０４ 通信装置、６０５ 入出力インタフェース、６１０ 受付部、６２０ 秘密鍵保管部、６３０ 部分復号部、６４０ 出力部、６９０ 記憶部、７００ 最終復号装置、７０１ プロセッサ、７０２ メモリ、７０３ 補助記憶装置、７０４ 通信装置、７０５ 入出力インタフェース、７１０ 受付部、７２０ 秘密鍵保管部、７３０ 最終復号部、７４０ 推論結果保管部、７５０ 出力部、７９０ 記憶部。

請求の範囲

[請求項1] 第１行列と第２行列を連結して得らえる推論モデルデータを暗号化して得られるモデル暗号文を、前記第１行列の暗号文に相当する推論用暗号文と、前記第２行列の暗号文に相当する計算用暗号文と、に分割するモデル分割部と、

前記計算用暗号文と、入力データを暗号化して得られるデータ暗号文と、を復号せずに、準同型演算アルゴリズムによって、前記第１行列と前記入力データを表すベクトルの積の暗号文に相当する事前結果暗号文を生成する事前計算部と、

前記事前結果暗号文と前記推論用暗号文とを復号せずに用いて、準同型演算アルゴリズムによって、前記入力データに対する推論結果の暗号文である推論結果暗号文を生成する準同型推論部と、

前記モデル暗号文のための秘密鍵であるモデル用秘密鍵を用いて、前記推論結果暗号文に対して部分復号を行って、部分復号結果を生成する部分復号部と、

前記データ暗号文のための秘密鍵であるデータ用秘密鍵を用いて、前記部分復号結果から前記入力データに対する前記推論結果を復号する最終復号部と、

を備える秘匿情報処理システム。

[請求項2] 前記準同型推論部は、前記事前結果暗号文と、前記推論用暗号文と、前回の入力データに対する推論結果の暗号文である前回結果暗号文と、を復号せずに用いて、前記推論結果暗号文を生成する

請求項１に記載の秘匿情報処理システム。

[請求項3] 前記準同型推論部は、

前記推論用暗号文と前記前回結果暗号文とを復号せずに用いて、準同型演算アルゴリズムによって、前記第１行列と前記前回の入力データに対する前記推論結果を表すベクトルの積の暗号文に相当する中間結果暗号文を生成し、

前記中間結果暗号文と前記事前結果暗号文とを復号せずに用いて、準同型演算アルゴリズムによって、前記中間結果暗号文を復号して得られるベクトルと前記事前結果暗号文を復号して得られるベクトルとの足し算の結果の暗号文を前記推論結果暗号文として生成する
請求項２に記載の秘匿情報処理システム。

[請求項4] 前記部分復号部は、前記推論結果暗号文の要素であるベクトルと前記モデル用秘密鍵を表すベクトルとの内積と、確率分布から選択される値との足し算の結果を、前記部分復号結果の要素として算出する
請求項１から請求項３のいずれか１項に記載の秘匿情報処理システム。

[請求項5] 前記最終復号部は、前記データ用秘密鍵を用いて、前記推論結果暗号文と前記部分復号結果とから、前記入力データに対する前記推論結果を復号する
請求項１から請求項４のいずれか１項に記載の秘匿情報処理システム。

[請求項6] 前記最終復号部は、前記推論結果暗号文の要素であるベクトルと前記データ用秘密鍵を表すベクトルとの内積と、前記部分復号結果の要素との足し算によって得られる和に基づいて、前記推論結果の要素を決定する
請求項５に記載の秘匿情報処理システム。

[請求項7] 前記最終復号部は、前記和と１／４の差に基づいて前記推論結果の前記要素を決定する
請求項６に記載の秘匿情報処理システム。

[請求項8] 前記最終復号部は、前記差が閾値より小さい場合に前記推論結果の前記要素を１に決定し、前記差が前記閾値より大きい場合に前記推論結果の前記要素を０に決定する
請求項７に記載の秘匿情報処理システム。

[請求項9] 前記モデル分割部と前記事前計算部と前記準同型推論部とを備える

準同型推論装置と、

前記部分復号部を備える部分復号装置と、

前記最終復号部を備える最終復号装置７００と、を備える

請求項１から請求項８のいずれか１項に記載の秘匿情報処理システム。

[請求項10] 前記入力データのための公開鍵であるデータ用公開鍵を用いて前記入力データを暗号化して前記データ暗号文を生成するデータ暗号化部と、

前記推論モデルデータのための公開鍵であるモデル用公開鍵を用いて前記推論モデルデータを暗号化して前記モデル暗号文を生成するモデル暗号化部と、を備える

請求項１から請求項９のいずれか１項に記載の秘匿情報処理システム。

[請求項11] 前記データ暗号化部を備えるデータ暗号化装置と、

前記モデル暗号化部を備えるモデル暗号化装置と、を備える

請求項１０に記載の秘匿情報処理システム。

[請求項12] 前記データ用公開鍵と前記データ用秘密鍵の組と、前記モデル用公開鍵と前記モデル用秘密鍵の組と、を生成する鍵生成部を備える

請求項１０または請求項１１に記載の秘匿情報処理システム。

[請求項13] 前記鍵生成部を備える鍵生成装置を備える

請求項１２に記載の秘匿情報処理システム。

[請求項14] モデル分割部が、第１行列と第２行列を連結して得らえる推論モデルデータを暗号化して得られるモデル暗号文を、前記第１行列の暗号文に相当する推論用暗号文と、前記第２行列の暗号文に相当する計算用暗号文と、に分割し、

事前計算部が、前記計算用暗号文と、入力データを暗号化して得られるデータ暗号文と、を復号せずに、準同型演算アルゴリズムによって、前記第１行列と前記入力データを表すベクトルの積の暗号文に相

当する事前結果暗号文を生成し、

準同型推論部が、前記事前結果暗号文と、前記推論用暗号文と、前回の入力データに対する推論結果の暗号文である前回結果暗号文と、を復号せずに用いて、準同型演算アルゴリズムによって、前記入力データに対する推論結果の暗号文である推論結果暗号文を生成し、

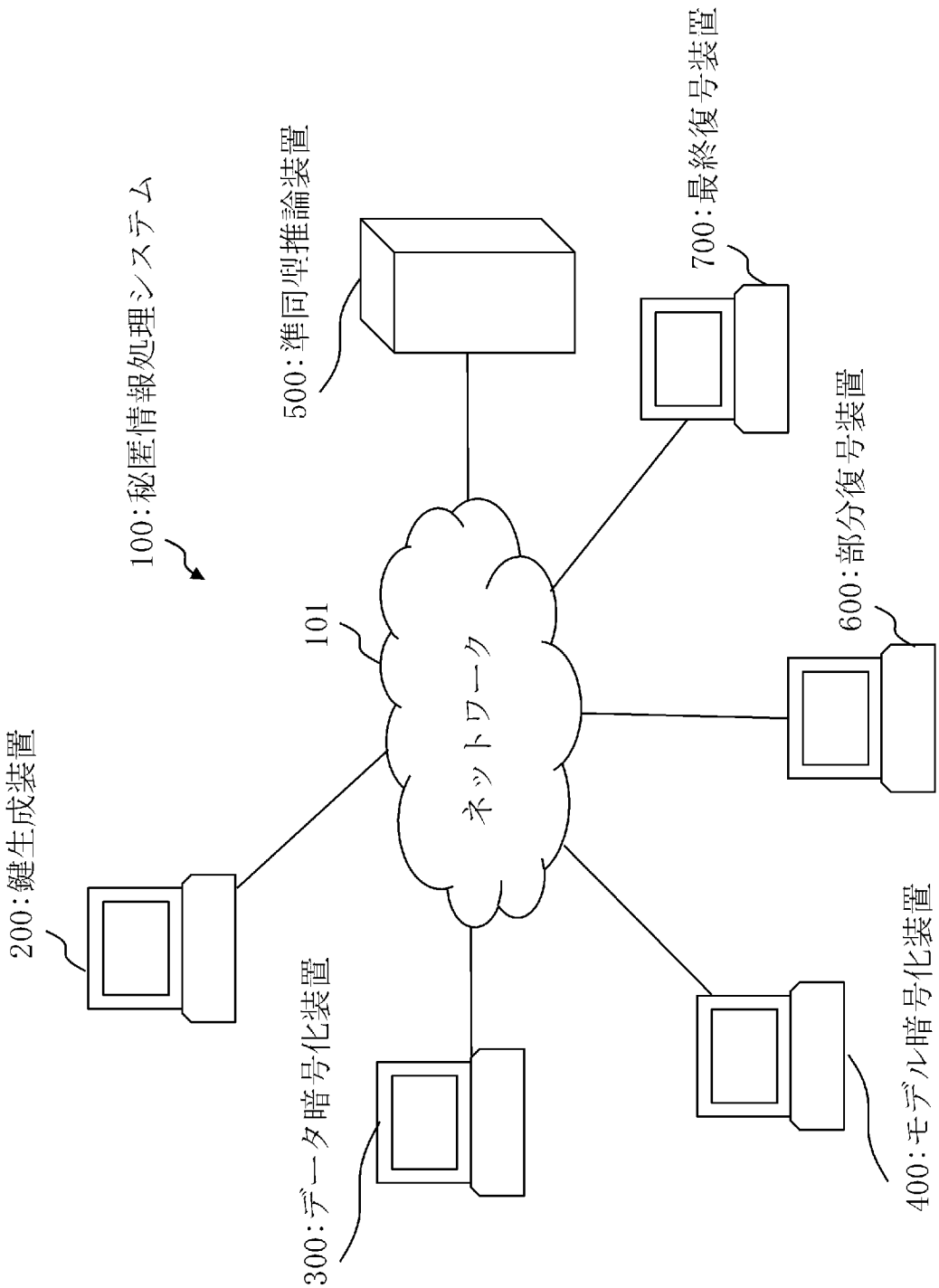
部分復号部が、前記モデル暗号文のための秘密鍵であるモデル用秘密鍵を用いて、前記推論結果暗号文に対する部分復号を行って、部分復号結果を生成し、

最終復号部が、前記データ暗号文のための秘密鍵であるデータ用秘密鍵を用いて、前記部分復号結果から前記入力データに対する前記推論結果を復号する

秘匿情報処理方法。

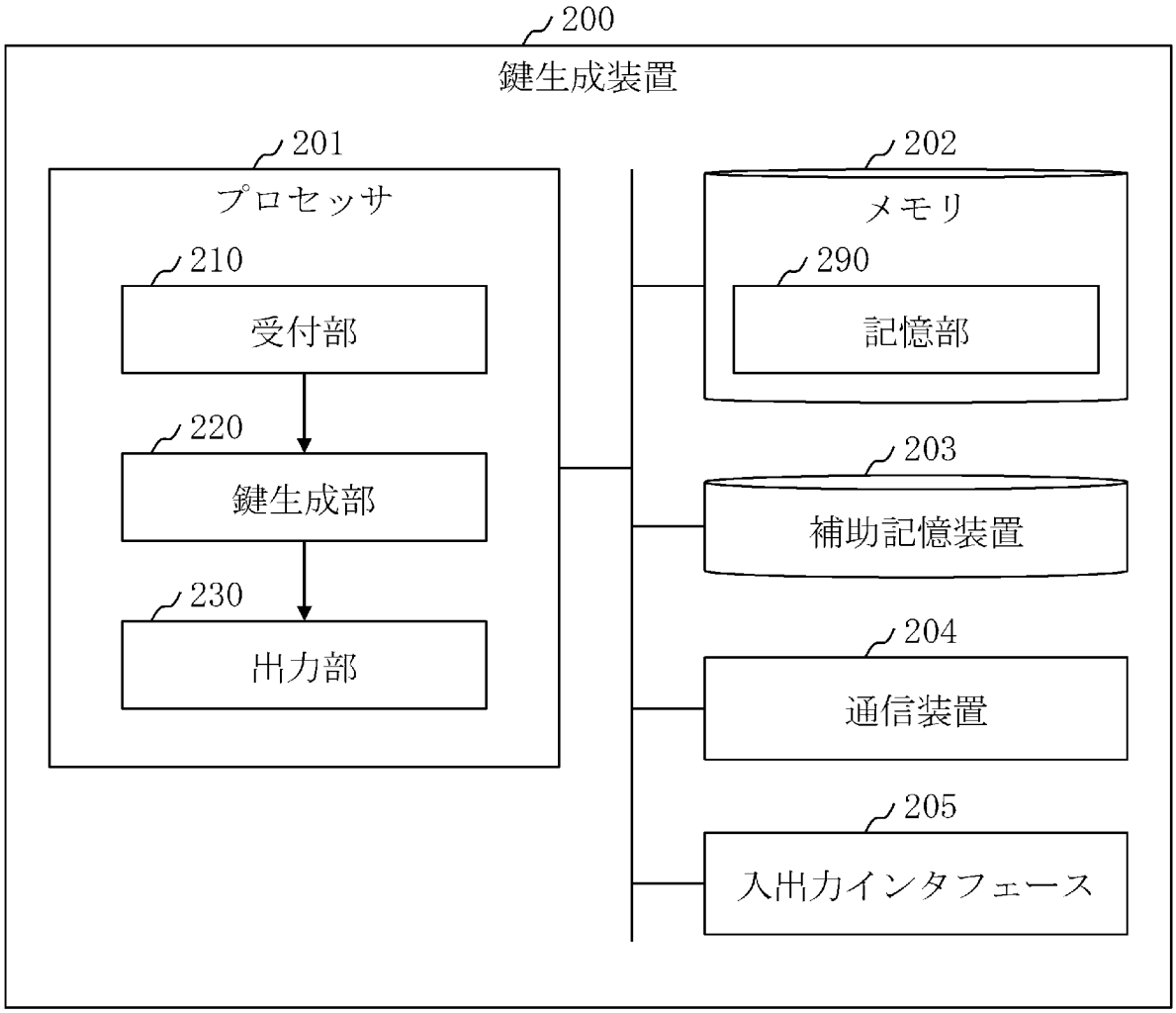
[図1]

図1


100:秘匿情報処理システム
101
ネットワーク
200:鍵生成装置
300:データ暗号化装置
400:モデル暗号化装置
500:準同型推論装置
600:部分復号装置
700:最終復号装置

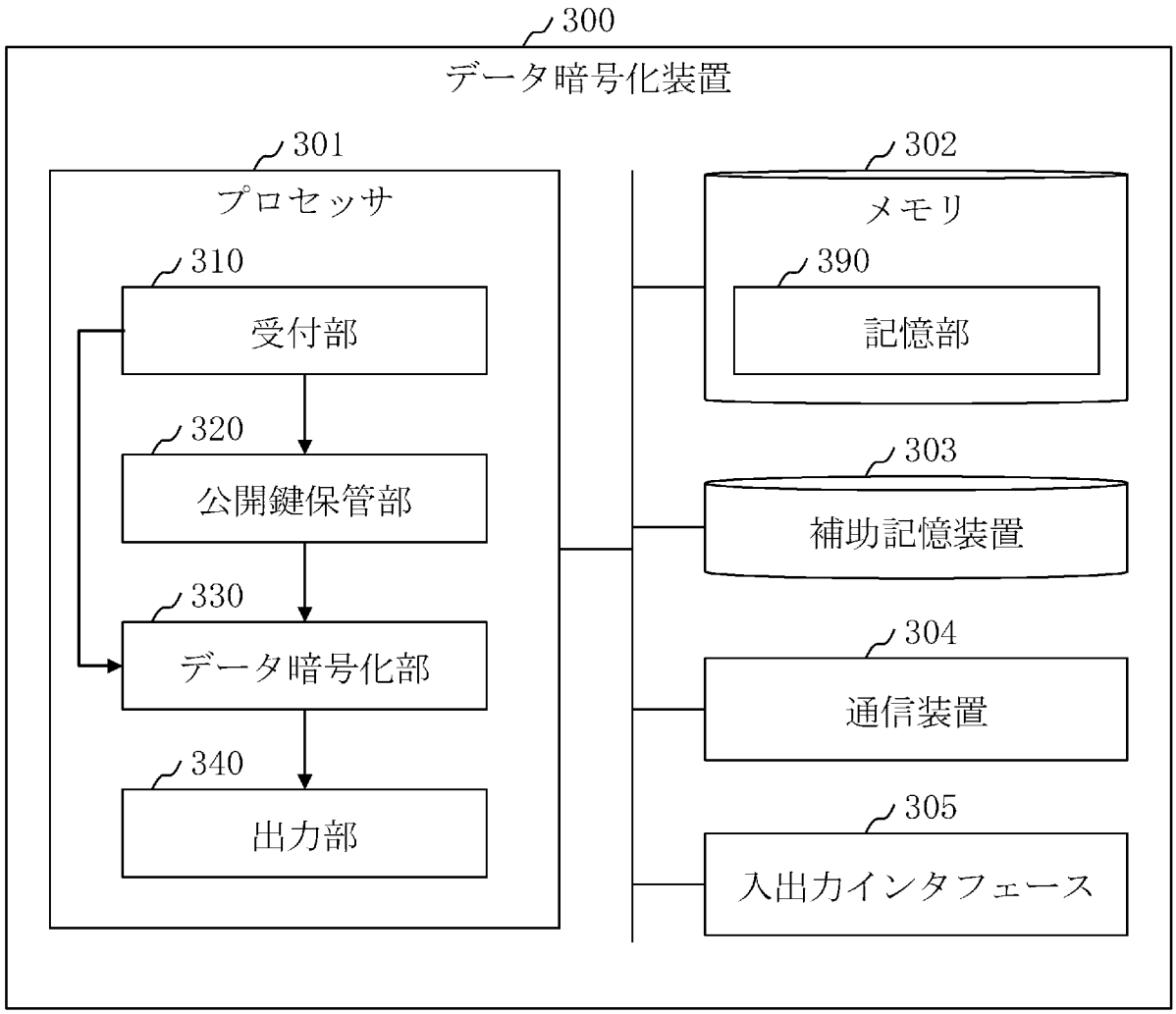
[図2]

図2


200
鍵生成装置
201
プロセッサ
210
受付部
220
鍵生成部
230
出力部
202
メモリ
290
記憶部
203
補助記憶装置
204
通信装置
205
入出力インタフェース

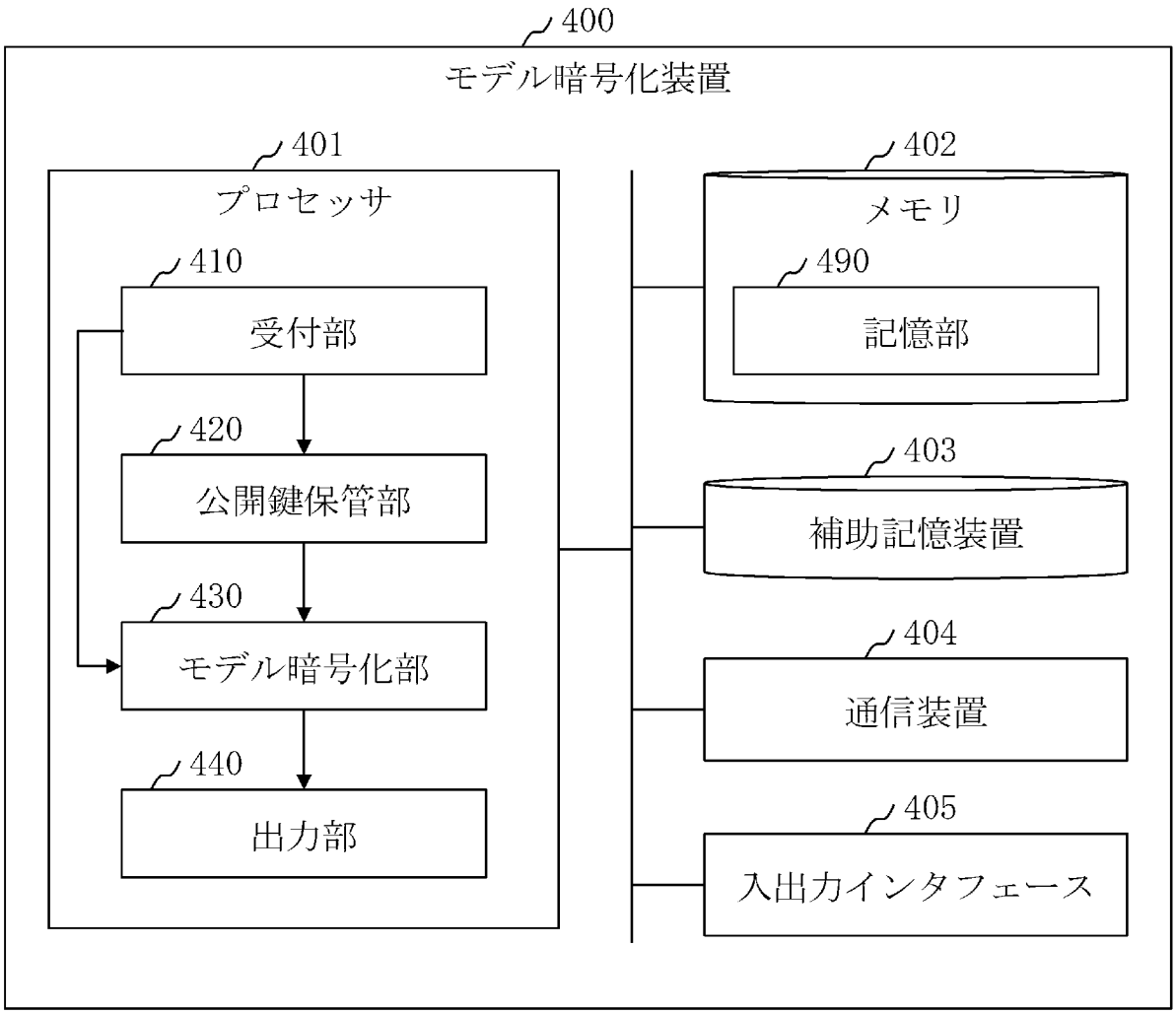
[図3]

図3


300
データ暗号化装置
301
プロセッサ
310
受付部
320
公開鍵保管部
330
データ暗号化部
340
出力部
302
メモリ
390
記憶部
303
補助記憶装置
304
通信装置
305
入出力インタフェース

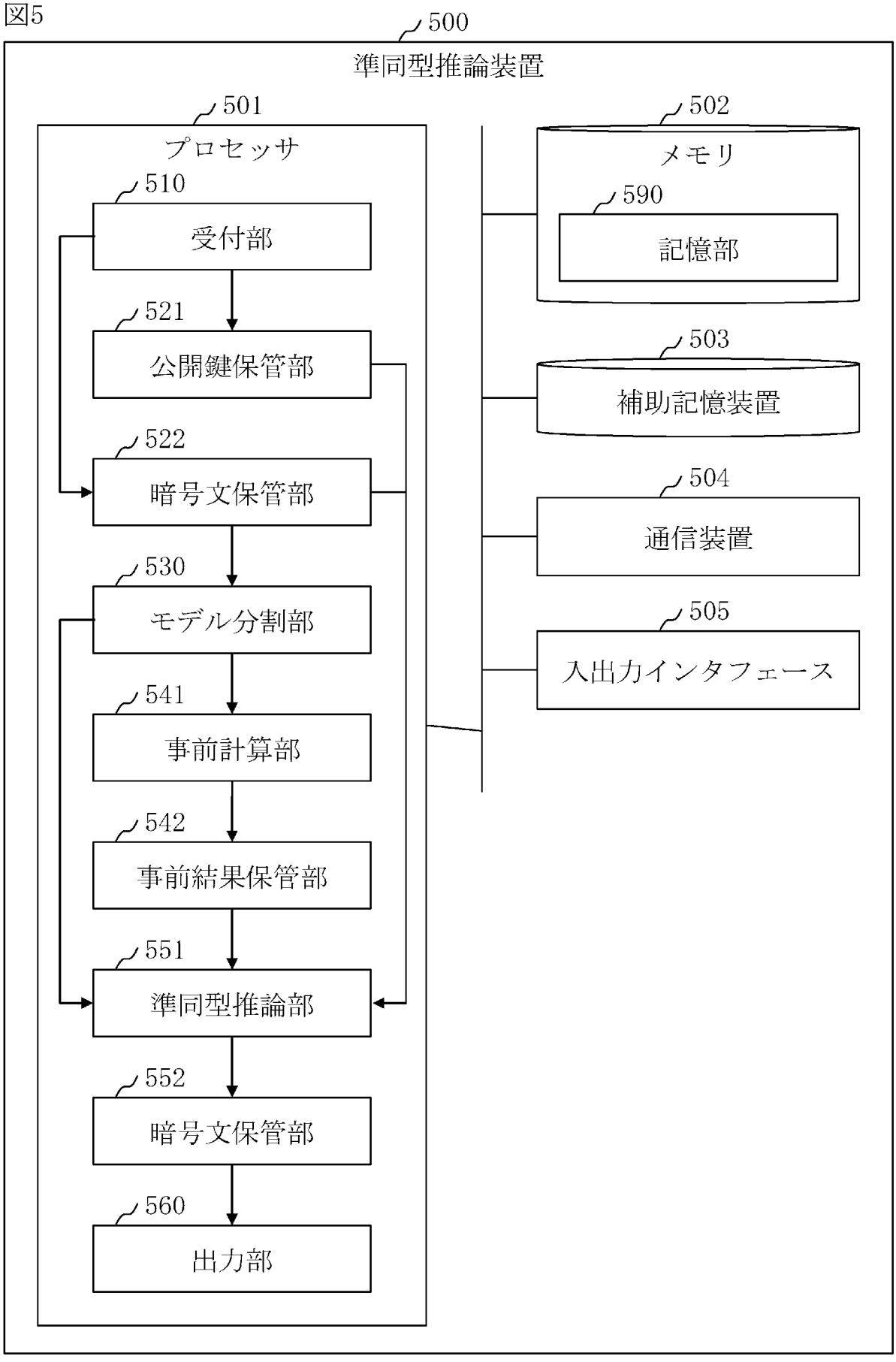
[図4]

図4


400
モデル暗号化装置
401
プロセッサ
410
受付部
420
公開鍵保管部
430
モデル暗号化部
440
出力部
402
メモリ
490
記憶部
403
補助記憶装置
404
通信装置
405
入出力インタフェース

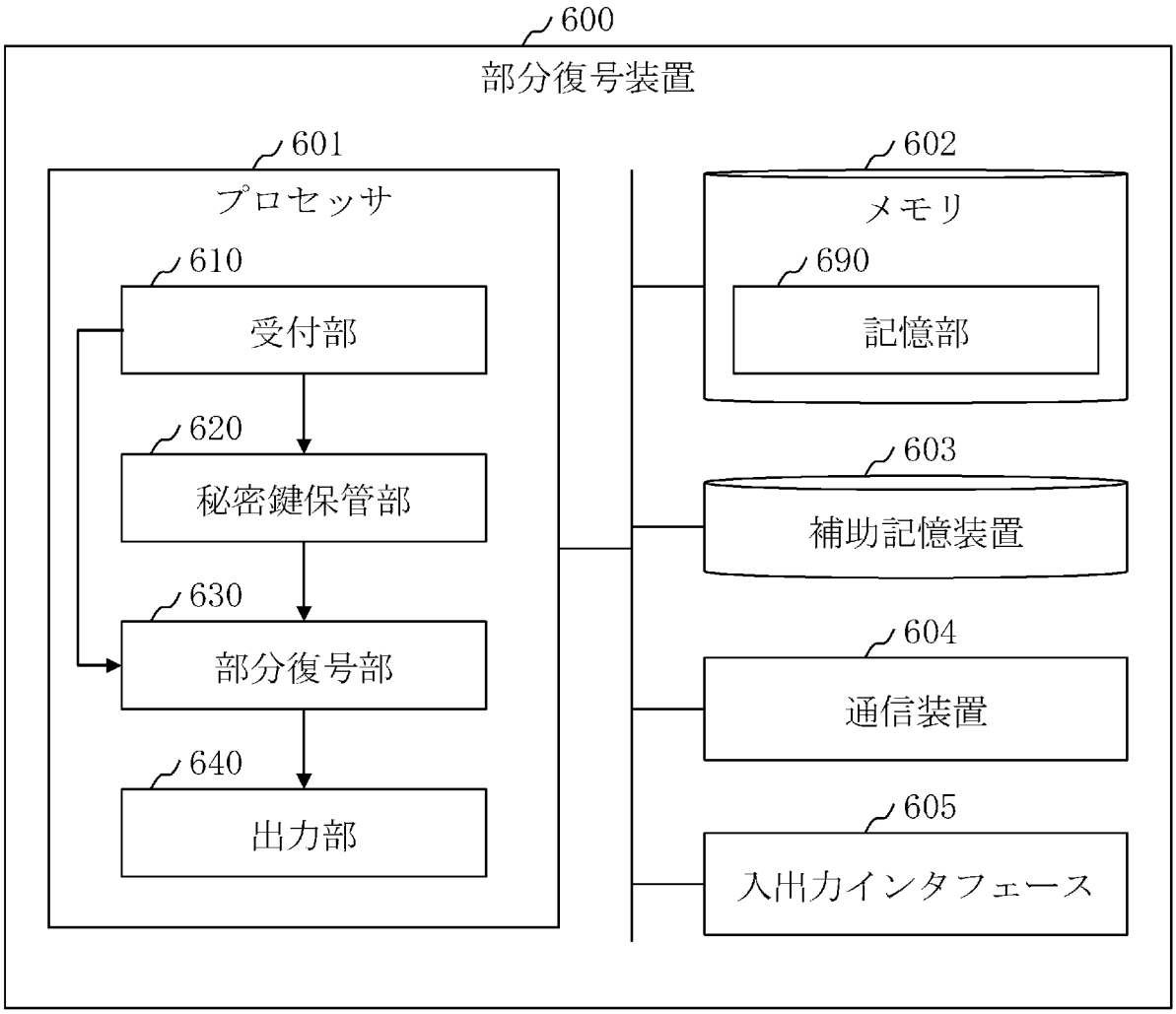
[図5]

図5


500
準同型推論装置
501
プロセッサ
510
受付部
521
公開鍵保管部
522
暗号文保管部
530
モデル分割部
541
事前計算部
542
事前結果保管部
551
準同型推論部
552
暗号文保管部
560
出力部
502
メモリ
590
記憶部
503
補助記憶装置
504
通信装置
505
入出力インタフェース

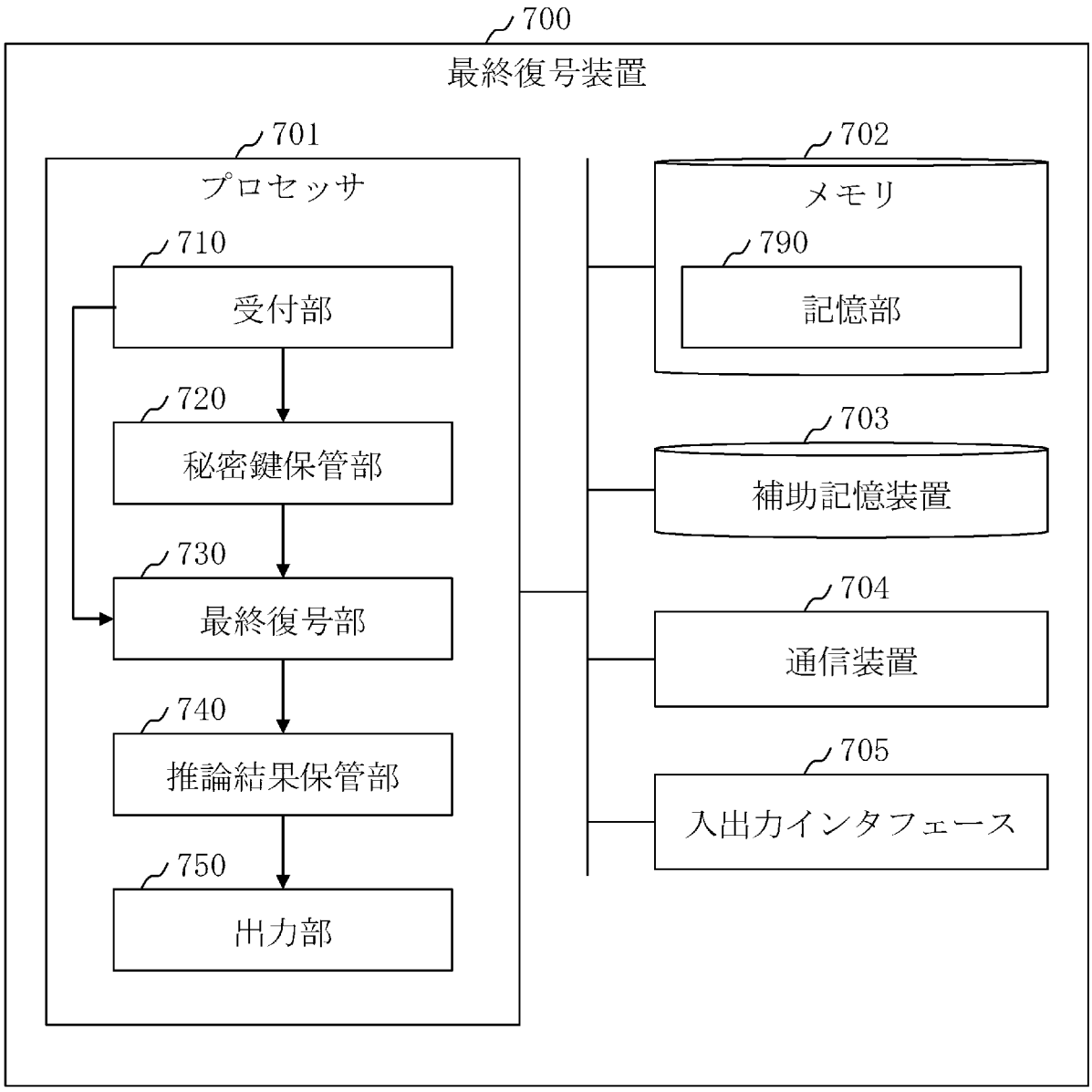
[図6]

図6


600
部分復号装置
601
プロセッサ
610
受付部
620
秘密鍵保管部
630
部分復号部
640
出力部
602
メモリ
690
記憶部
603
補助記憶装置
604
通信装置
605
入出力インタフェース

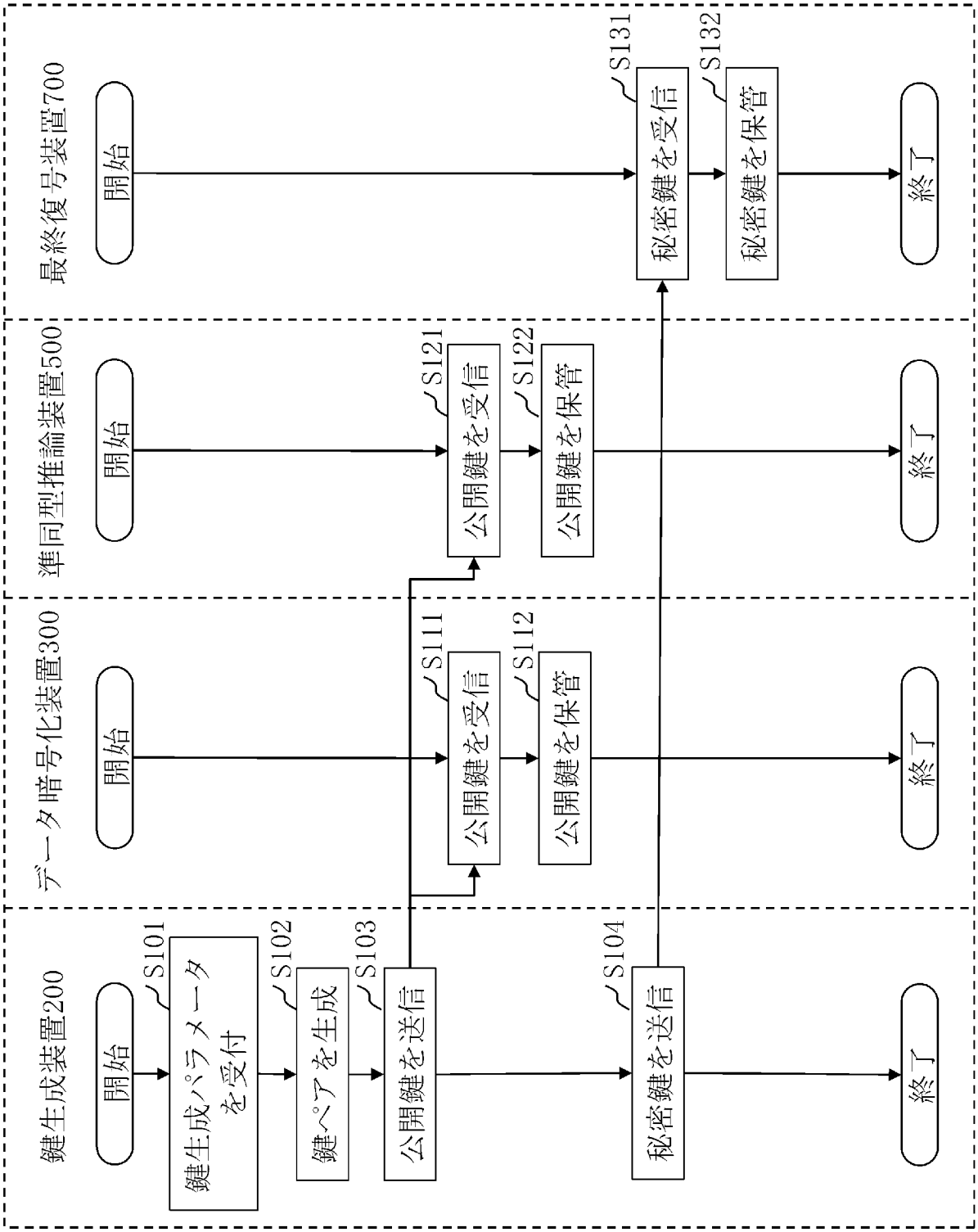
[図7]

図7


700
最終復号装置
701
プロセッサ
710
受付部
720
秘密鍵保管部
730
最終復号部
740
推論結果保管部
750
出力部
702
メモリ
790
記憶部
703
補助記憶装置
704
通信装置
705
入出力インタフェース

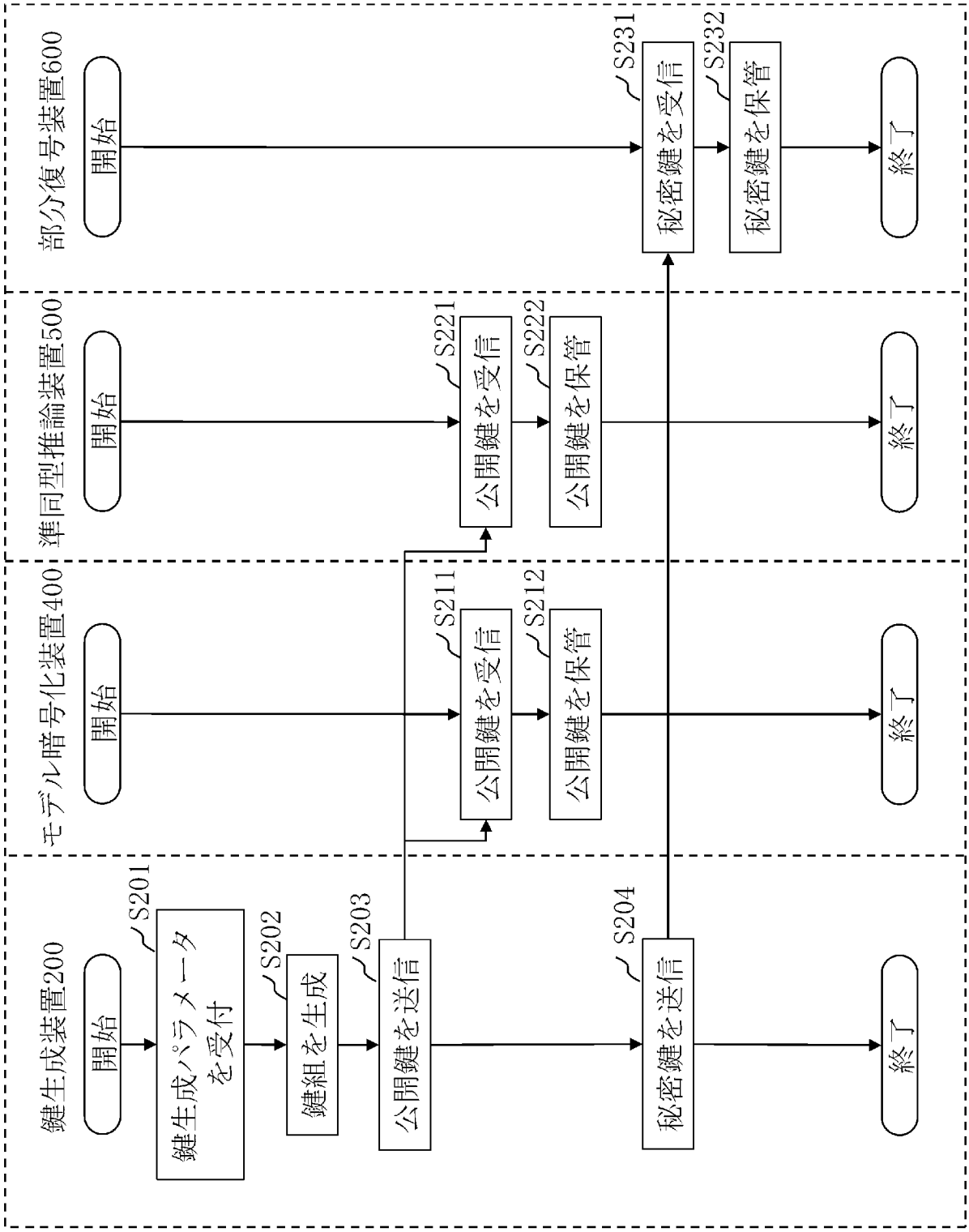
[図8]

図8


鍵生成装置200
開始
S101
鍵生成パラメータを受付
S102
鍵ペアを生成
S103
公開鍵を送信
S104
秘密鍵を送信
終了
データ暗号化装置300
開始
S111
公開鍵を受信
S112
公開鍵を保管
終了
準同型推論装置500
開始
S121
公開鍵を受信
S122
公開鍵を保管
終了
最終復号装置700
開始
S131
秘密鍵を受信
S132
秘密鍵を保管
終了

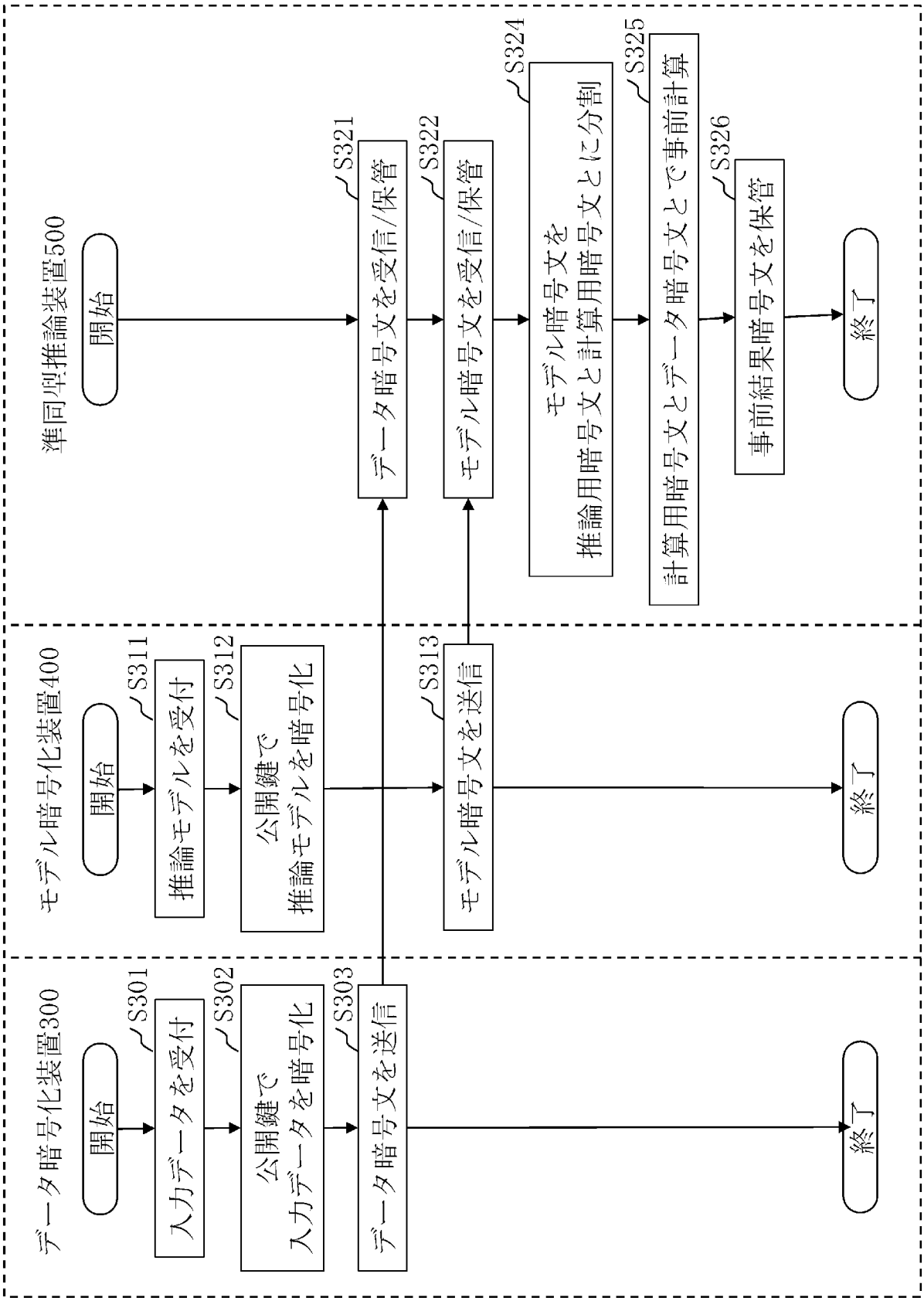
[図9]

図9


鍵生成装置200
開始
S201
鍵生成パラメータを受付
S202
鍵組を生成
S203
公開鍵を送信
S204
秘密鍵を送信
終了
モデル暗号化装置400
開始
S211
公開鍵を受信
S212
公開鍵を保管
終了
準同型推論装置500
開始
S221
公開鍵を受信
S222
公開鍵を保管
終了
部分復号装置600
開始
S231
秘密鍵を受信
S232
秘密鍵を保管
終了

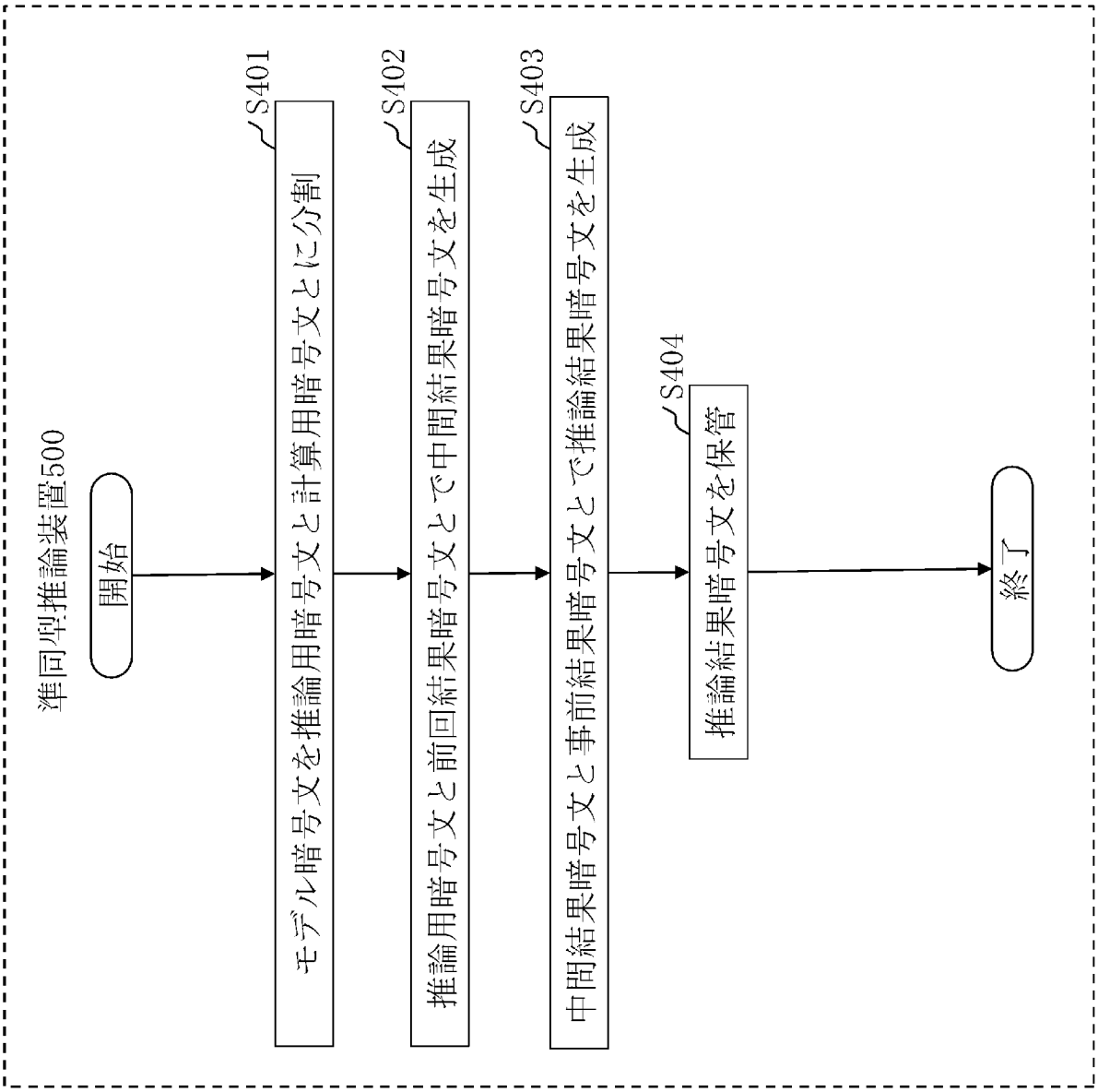
[図10]

図10


準同型推論装置500
開始
S321
データ暗号文を受信/保管
S322
モデル暗号文を受信/保管
S324
モデル暗号文を
推論用暗号文と計算用暗号文とに分割
S325
計算用暗号文とデータ暗号文とで事前計算
S326
事前結果暗号文を保管
終了
モデル暗号化装置400
開始
S311
推論モデルを受付
S312
公開鍵で
推論モデルを暗号化
S313
モデル暗号文を送信
終了
データ暗号化装置300
開始
S301
入力データを受付
S302
公開鍵で
入力データを暗号化
S303
データ暗号文を送信
終了

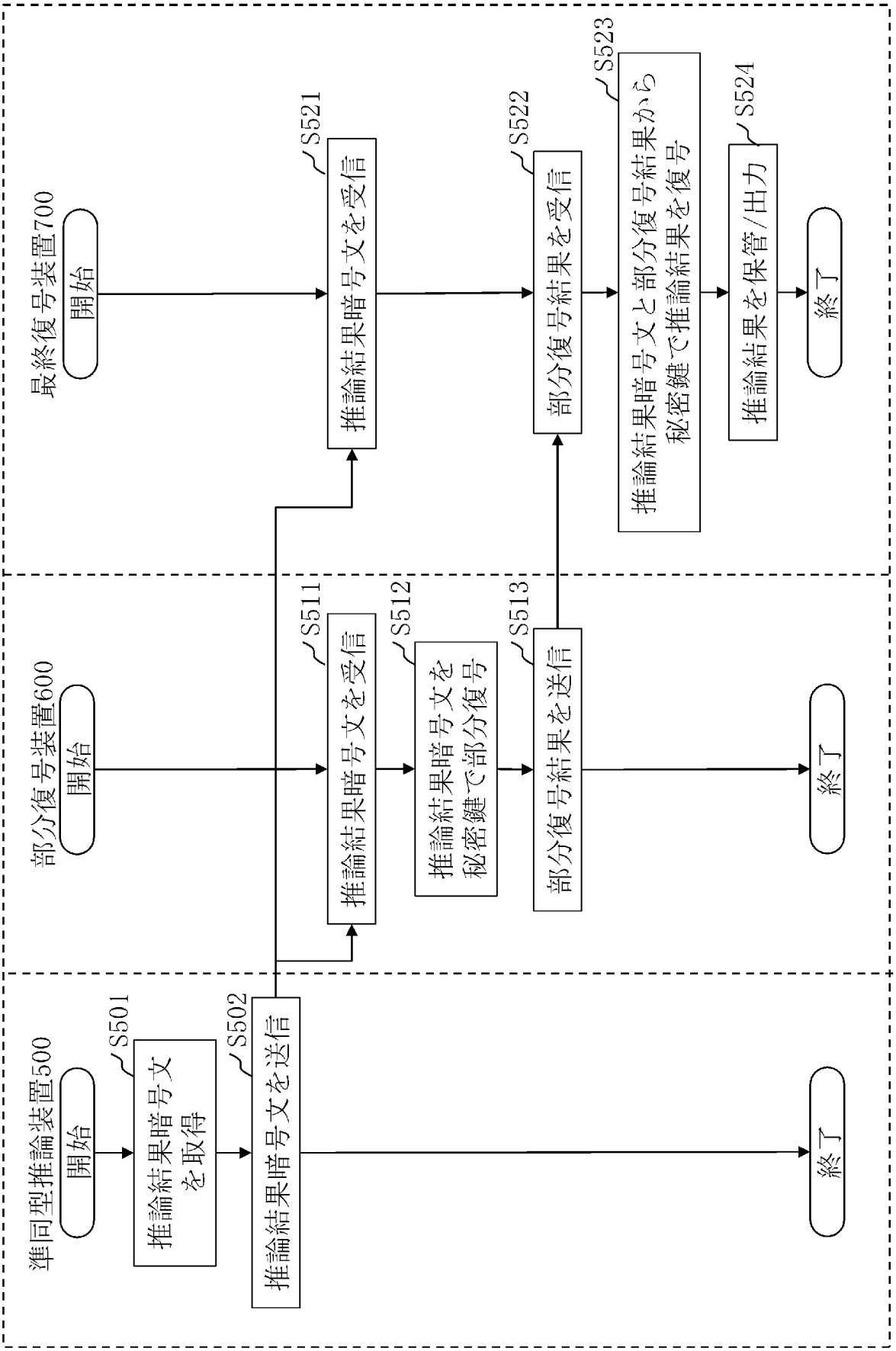
[図11]

図11


準同型推論装置500
開始
S401
モデル暗号文を推論用暗号文と計算用暗号文とに分割
S402
推論用暗号文と前回結果暗号文とで中間結果暗号文を生成
S403
中間結果暗号文と事前結果暗号文とで推論結果暗号文を生成
S404
推論結果暗号文を保管
終了

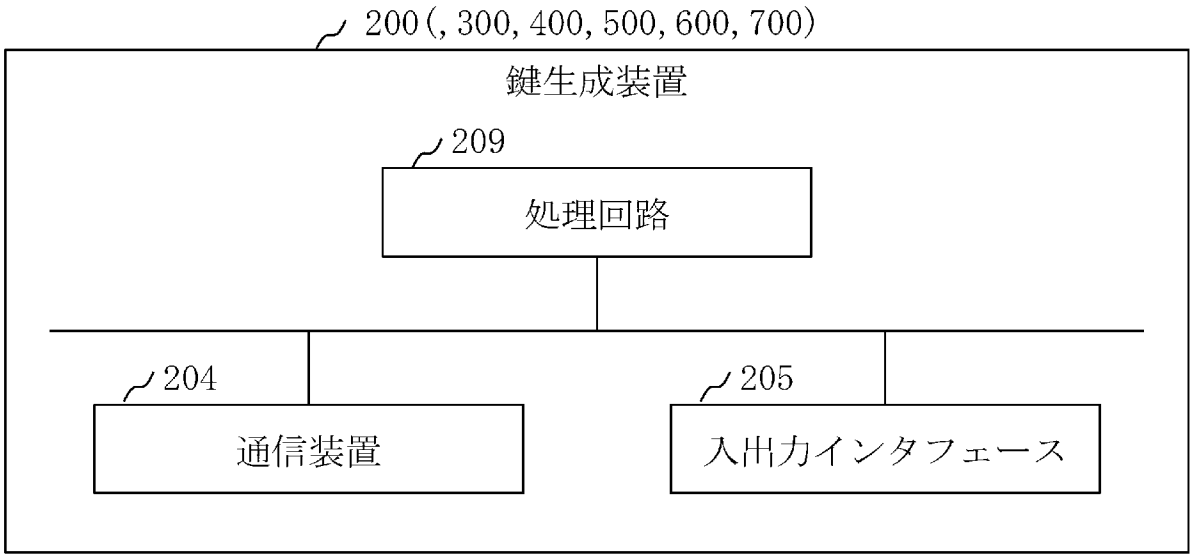
[図12]

図12


準同型推論装置500
開始
S501
推論結果暗号文を取得
S502
推論結果暗号文を送信
終了
部分復号装置600
開始
S511
推論結果暗号文を受信
S512
推論結果暗号文を秘密鍵で部分復号
S513
部分復号結果を送信
終了
最終復号装置700
開始
S521
推論結果暗号文を受信
S522
部分復号結果を受信
S523
推論結果暗号文と部分復号結果から秘密鍵で推論結果を復号
S524
推論結果を保管/出力
終了

[図13]

図13


200(, 300, 400, 500, 600, 700)
鍵生成装置
209
処理回路
204
通信装置
205
入出力インタフェース

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/048498

A. CLASSIFICATION OF SUBJECT MATTER
G09C 1/00(2006.01)i
FI: G09C1/00 620A
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)
G09C1/00

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

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 2019-113665 A (AXELL CORP.) 11 July 2019 (2019-07-11) paragraphs [0014]-[0043]	1-14
A	JP 2019-046460 A (AXELL CORP.) 22 March 2019 (2019-03-22) paragraphs [0053]-[0064], fig. 3-5	1-14
A	WO 2019/102624 A1 (MITSUBISHI ELECTRIC CORP.) 31 May 2019 (2019-05-31) paragraphs [0008]-[0050]	1-14
A	US 2016/0350648 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC.) 01 December 2016 (2016-12-01) paragraph [0073], fig. 10	1-14

☐ 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
12 March 2021 (12.03.2021)	23 March 2021 (23.03.2021)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/048498

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2019-113665 A	11 Jul. 2019	US 2019/0199511 A1 paragraphs [0024]-[0053]	
JP 2019-046460 A	22 Mar. 2019	US 2019/0065974 A1 paragraphs [0069]-[0086], fig. 3-5	
WO 2019/102624 A1	31 May 2019	(Family: none)	
US 2016/0350648 A1	01 Dec. 2016	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/048498

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G09C 1/00(2006.01)i
FI: G09C1/00 620A

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））

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	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１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 2019-113665 A (株式会社アクセル) 11.07.2019 (2019-07-11) 段落0014-0043	1-14
A	JP 2019-046460 A (株式会社アクセル) 22.03.2019 (2019-03-22) 段落0053-0064, 図3-5	1-14
A	WO 2019/102624 A1 (三菱電機株式会社) 31.05.2019 (2019-05-31) 段落0008-0050	1-14
A	US 2016/0350648 A1 (MICROSOFT TECHNOLOGY LICENSING, LLC.) 01.12.2016 (2016-12-01) 段落0073, 図10	1-14

☐ 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抵触するものではなく、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	国際調査報告の発送日
12.03.2021	23.03.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
行田　悦資 5S 6304
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/048498

引用文献	公表日	パテントファミリー文献	公表日
JP 2019-113665 A	11.07.2019	US 2019/0199511 A1 段落0024-0053	
JP 2019-046460 A	22.03.2019	US 2019/0065974 A1 段落0069-0086, 図3-5	
WO 2019/102624 A1	31.05.2019	（ファミリーなし）	
US 2016/0350648 A1	01.12.2016	（ファミリーなし）	