(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-177223
(P2020-177223A)
(43)公開日　令和2年10月29日(2020.10.29)

(51)Int.Cl.			F I		テーマコード（参考）
G09C	1/00	(2006.01)	G09C	1/00	620Z
H04L	9/08	(2006.01)	H04L	9/00	601C
G06F	21/64	(2013.01)	H04L	9/00	601F
			G06F	21/64	

審査請求 未請求　請求項の数 23　ＯＬ　（全 26 頁）

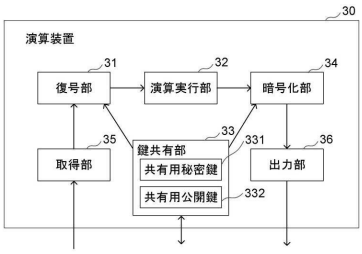
(21)出願番号　特願2020-26497(P2020-26497)
(22)出願日　令和2年2月19日(2020.2.19)
(31)優先権主張番号　特願2019-77259(P2019-77259)
(32)優先日　平成31年4月15日(2019.4.15)
(33)優先権主張国・地域又は機関
日本国(JP)

(71)出願人　398034168
株式会社アクセル
東京都千代田区外神田四丁目１４番１号
(74)代理人　110000279
特許業務法人ウィルフォート国際特許事務所
(72)発明者　星月　優佑
東京都千代田区外神田四丁目１４番１号
株式会社アクセル内

(54)【発明の名称】演算装置、演算システム、及び演算方法

(57)【要約】　（修正有）
【課題】データの漏洩を防止でき、且つ、広範な処理を実行することができるようにする。
【解決手段】演算システムにおいて、クライアント装置と、ネットワークを介して接続されるサーバにバスを介して接続される演算装置３０と、を有する。クライアント装置は、処理対象のデータを暗号鍵で暗号化させて、サーバに送信し、サーバから送信された暗号化された演算結果のデータを復号鍵で復号する。演算装置３０は、クライアント装置との間で暗号鍵及び復号鍵を外部に秘匿した状態で共有する鍵共有部３３と、クライアント装置から送信されたデータに基づく暗号鍵で暗号化されているデータを取得し、取得したデータを復号鍵で復号する復号部３１と、復号されたデータに対して所定の演算を実行する演算実行部３２と、演算結果のデータを暗号鍵で暗号化し、暗号化された演算結果のデータをサーバに出力する暗号化部３４とを備える。
【選択図】図４

図4



【特許請求の範囲】
【請求項１】
クライアント装置とネットワークを介して接続される情報処理装置にバスを介して接続される演算装置であって、
前記クライアント装置は、処理対象のデータを第１暗号鍵で暗号化させて、前記情報処理装置に送信し、前記情報処理装置から送信された暗号化された処理結果のデータを、前記第１暗号鍵に対応する第１復号鍵で復号し、
前記演算装置は、
前記クライアント装置との間で前記第１暗号鍵及び前記第１復号鍵を外部に秘匿した状態で共有する鍵共有部と、
前記クライアント装置から送信されたデータに基づく前記第１暗号鍵で暗号化されているデータを前記情報処理装置から取得する取得部と、
前記取得部により取得された前記第１暗号鍵で暗号化されているデータを前記第１復号鍵で復号する復号部と、
前記復号部で復号されたデータに対して所定の演算を実行する演算実行部と、
前記演算実行部による演算結果のデータを前記第１暗号鍵で暗号化する暗号化部と、
前記暗号化された前記演算結果のデータを前記情報処理装置に出力する出力部と、
を備えることを特徴とする演算装置。
【請求項２】
前記演算実行部は、
異なる演算を実行可能な複数の演算部を有し、
前記取得部は、前記情報処理装置から前記データに対して実行する演算の指示を取得し、
前記演算実行部は、前記演算の指示に対応する演算を実行する演算部を選択し、選択した演算部により、前記データに対する演算を実行する
ことを特徴とする請求項１に記載の演算装置。
【請求項３】
前記情報処理装置は、前記演算装置に実行させる演算についての演算式を前記演算装置に送信し、
前記演算装置の前記演算実行部は、
前記情報処理装置から受信した演算式を実行する
ことを特徴とする請求項１に記載の演算装置。
【請求項４】
前記演算装置は、第２復号鍵を外部から読出不能に記憶し、
前記クライアント装置から、前記第２復号鍵に対応する第２暗号鍵により暗号化された前記第１暗号鍵及び前記第１復号鍵を受信して、前記第２復号鍵を用いて前記暗号化された前記第１暗号鍵及び前記第１復号鍵を復号することにより、前記第１暗号鍵及び第１復号鍵を共有する
ことを特徴とする請求項１から請求項３のいずれか一項に記載の演算装置。
【請求項５】
前記鍵共有部は、
ランダムな第１整数を生成する生成部と、
前記第１整数と生成元とを用いて離散対数問題が困難な有限巡回群の元として第１公開鍵を作成する作成部と、
を備え、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記第１公開鍵を送信し、
前記取得部は、
ランダムな第２整数と前記第１公開鍵とを用いて共有用共通鍵を作成する前記クライアント装置から、前記第２整数と前記生成元とを用いて前記クライアント装置で作成された

離散対数問題が困難な有限巡回群の元である第２公開鍵と、前記クライアント装置において前記共有用共通鍵を用いて暗号化された前記第１暗号鍵及び前記第１復号鍵とを取得し、
前記作成部は、
前記第１整数と前記第２公開鍵とを用いて共有用共通鍵を作成し、
前記復号部は、前記作成部により作成された前記共有用共通鍵を用いて前記暗号化された前記第１暗号鍵及び前記第１復号鍵を復号する
ことを特徴とする請求項１から請求項３のいずれか一項に記載の演算装置。
【請求項６】
前記鍵共有部は、さらに、
秘密鍵を記憶する記憶部
を備え、
前記作成部は、さらに、
前記秘密鍵と前記公開鍵のハッシュ値とを用いて電子署名を作成し、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記電子署名を出力し、
前記取得部は、
前記クライアント装置で前記電子署名により前記第１公開鍵の正当性が確認されたとき、前記クライアント装置で作成された前記第２公開鍵と、前記暗号化された前記第１暗号鍵及び前記第１復号鍵とを取得する
ことを特徴とする請求項５に記載の演算装置。
【請求項７】
前記鍵共有部は、
第１整数と、前記第１整数、第１公開鍵及び秘密鍵を用いて作成された電子署名と、を記憶する記憶部と、
前記第１整数と生成元とを用いて離散対数問題が困難な有限巡回群の元として第１公開鍵を作成する作成部と、
を備え、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記電子署名と、前記第１公開鍵とを出力し、
前記取得部は、
前記電子署名の検証を実行して前記第１公開鍵の正当性が確認されたとき、ランダムな第２整数と前記第１公開鍵とを用いて共有用共通鍵を作成する前記クライアント装置から、前記第２整数と前記生成元とを用いて前記クライアント装置で作成された離散対数問題が困難な有限巡回群の元である第２公開鍵と、前記クライアント装置において前記共有用共通鍵を用いて暗号化された前記第１暗号鍵及び前記第１復号鍵とを取得し、
前記作成部は、
前記第１整数と前記第２公開鍵とを用いて共有用共通鍵を作成し、
前記復号部は、前記作成部により作成された前記共有用共通鍵を用いて前記暗号化された前記第１暗号鍵及び前記第１復号鍵を復号する
ことを特徴とする請求項１から請求項３のいずれか一項に記載の演算装置。
【請求項８】
前記鍵共有部は、
第１整数と、前記第１整数、第１公開鍵及び秘密鍵を用いて作成された電子署名と、前記第１整数及び生成元を用いて作成された離散対数問題が困難な有限巡回群の元である第１公開鍵とを記憶する記憶部
を備え、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記電子署名と、前記第１公開鍵と

を出力し、
前記取得部は、
前記電子署名の検証を実行して前記第１公開鍵の正当性が確認されたとき、ランダムな第２整数と前記第１公開鍵とを用いて共有用共通鍵を作成する前記クライアント装置から、前記第２整数と前記生成元とを用いて前記クライアント装置で作成された離散対数問題が困難な有限巡回群の元である第２公開鍵と、前記クライアント装置において前記共有用共通鍵を用いて暗号化された前記第１暗号鍵及び前記第１復号鍵とを取得し、
前記作成部は、
前記第１整数と前記第２公開鍵とを用いて共有用共通鍵を作成し、
前記復号部は、前記作成部により作成された前記共有用共通鍵を用いて前記暗号化された前記第１暗号鍵及び前記第１復号鍵を復号する
ことを特徴とする請求項１から請求項３のいずれか一項に記載の演算装置。
【請求項９】
前記共有用共通鍵は、
前記第１整数と前記第２公開鍵とを用いた値にハッシュ値を適用した値である
ことを特徴とする請求項５から８のいずれか一項に記載の演算装置。
【請求項１０】
クライアント装置とネットワークを介して接続される情報処理装置にバスを介して接続される演算装置であって、
前記クライアント装置は、処理対象のデータを通信用共通鍵で暗号化させて、前記情報処理装置に送信し、前記情報処理装置から送信された暗号化された処理結果のデータを、前記通信用共通鍵で復号し、
前記演算装置は、
前記クライアント装置との間で前記通信用共通鍵を外部に秘匿した状態で共有する鍵共有部と、
前記クライアント装置から送信されたデータに基づく前記通信用共通鍵で暗号化されているデータを前記情報処理装置から取得する取得部と、
前記取得部により取得された前記通信用共通鍵で暗号化されているデータを前記通信用共通鍵で復号する復号部と、
前記復号部で復号されたデータに対して所定の演算を実行する演算実行部と、
前記演算実行部による演算結果のデータを前記通信用共通鍵で暗号化する暗号化部と、
前記暗号化された前記演算結果のデータを前記情報処理装置に出力する出力部と、
を備えることを特徴とする演算装置。
【請求項１１】
前記演算実行部は、
異なる演算を実行可能な複数の演算部を有し、
前記取得部は、前記情報処理装置から前記データに対して実行する演算の指示を取得し、
前記演算実行部は、前記演算の指示に対応する演算を実行する演算部を選択し、選択した演算部により、前記データに対する演算を実行する
ことを特徴とする請求項１０に記載の演算装置。
【請求項１２】
前記情報処理装置は、前記演算装置に実行させる演算についての演算式を前記演算装置に送信し、
前記演算装置の前記演算実行部は、
前記情報処理装置から受信した演算式を実行する
ことを特徴とする請求項１０に記載の演算装置。
【請求項１３】
前記演算装置は、第２復号鍵を外部から読出不能に記憶し、
前記クライアント装置から、前記第２復号鍵に対応する第２暗号鍵により暗号化された

前記通信用共通鍵を受信して、前記第２復号鍵を用いて前記暗号化された前記通信用共通鍵を復号することにより、前記通信用共通鍵を共有する
ことを特徴とする請求項１０から請求項１２のいずれか一項に記載の演算装置。
【請求項１４】
前記鍵共有部は、
ランダムな第１整数を生成する生成部と、
前記第１整数と生成元とを用いて離散対数問題が困難な有限巡回群の元として第１公開鍵を作成する作成部と、
を備え、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記第１公開鍵を送信し、
前記取得部は、
ランダムな第２整数と前記第１公開鍵とを用いて共有用共通鍵を作成する前記クライアント装置から、前記第２整数と前記生成元とを用いて前記クライアント装置で作成された離散対数問題が困難な有限巡回群の元である第２公開鍵と、前記クライアント装置において前記共有用共通鍵を用いて暗号化された前記通信用共通鍵とを取得し、
前記作成部は、
前記第１整数と前記第２公開鍵とを用いて共有用共通鍵を作成し、
前記復号部は、前記作成部により作成された前記共有用共通鍵を用いて前記暗号化された前記通信用共通鍵を復号する
ことを特徴とする請求項１０から請求項１２のいずれか一項に記載の演算装置。
【請求項１５】
前記鍵共有部は、さらに、
秘密鍵を記憶する記憶部
を備え、
前記作成部は、さらに、
前記秘密鍵と前記公開鍵のハッシュ値とを用いて電子署名を作成し、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記電子署名を出力し、
前記取得部は、
前記クライアント装置で前記電子署名により前記第１公開鍵の正当性が確認されたとき、前記クライアント装置で作成された前記第２公開鍵と、前記暗号化された前記通信用共通鍵とを取得する
ことを特徴とする請求項１４に記載の演算装置。
【請求項１６】
前記鍵共有部は、
第１整数と、前記第１整数、第１公開鍵及び秘密鍵を用いて作成された電子署名と、を記憶する記憶部と、
前記第１整数と生成元とを用いて離散対数問題が困難な有限巡回群の元として第１公開鍵を作成する作成部と、
を備え、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記電子署名と、前記第１公開鍵とを出力し、
前記取得部は、
前記電子署名の検証を実行して前記第１公開鍵の正当性が確認されたとき、ランダムな第２整数と前記第１公開鍵とを用いて共有用共通鍵を作成する前記クライアント装置から、前記第２整数と前記生成元とを用いて前記クライアント装置で作成された離散対数問題が困難な有限巡回群の元である第２公開鍵と、前記クライアント装置において前記共有用共通鍵を用いて暗号化された前記通信用共通鍵とを取得し、

前記作成部は、
前記第１整数と前記第２公開鍵とを用いて共有用共通鍵を作成し、
前記復号部は、前記作成部により作成された前記共有用共通鍵を用いて前記暗号化された前記通信用共通鍵を復号する
ことを特徴とする請求項１０から請求項１２のいずれか一項に記載の演算装置。
【請求項１７】
前記鍵共有部は、
第１整数と、前記第１整数、第１公開鍵及び秘密鍵を用いて作成された電子署名と、前記第１整数及び生成元を用いて作成された離散対数問題が困難な有限巡回群の元である第１公開鍵とを記憶する記憶部
を備え、
前記出力部は、
前記情報処理装置を介して前記クライアント装置に前記電子署名と、前記第１公開鍵とを出力し、
前記取得部は、
前記電子署名の検証を実行して前記第１公開鍵の正当性が確認されたとき、ランダムな第２整数と前記第１公開鍵とを用いて共有用共通鍵を作成する前記クライアント装置から、前記第２整数と前記生成元とを用いて前記クライアント装置で作成された離散対数問題が困難な有限巡回群の元である第２公開鍵と、前記クライアント装置において前記共有用共通鍵を用いて暗号化された前記通信用共通鍵とを取得し、
前記作成部は、
前記第１整数と前記第２公開鍵とを用いて共有用共通鍵を作成し、
前記復号部は、前記作成部により作成された前記共有用共通鍵を用いて前記暗号化された前記通信用共通鍵を復号する
ことを特徴とする請求項１０から請求項１２のいずれか一項に記載の演算装置。
【請求項１８】
前記共有用共通鍵は、
前記第１整数と前記第２公開鍵とを用いた値にハッシュ値を適用した値である
ことを特徴とする請求項１４から１７のいずれか一項に記載の演算装置。
【請求項１９】
クライアント装置とネットワークを介して接続される情報処理装置と、前記情報処理装置にバスを介して接続される演算装置と、を備える演算システムであって、
前記クライアント装置は、処理対象のデータを第１暗号鍵で暗号化させて、前記情報処理装置に送信し、前記情報処理装置から送信された暗号化された処理結果のデータを、前記第１暗号鍵に対応する第１復号鍵で復号し、
前記演算装置は、
前記クライアント装置との間で前記第１暗号鍵及び前記第１復号鍵を外部に秘匿した状態で共有する鍵共有部と、
前記クライアント装置から送信されたデータに基づく前記第１暗号鍵で暗号化されているデータを前記情報処理装置から取得する取得部と、
前記取得部により取得されたデータを前記第１復号鍵で復号する復号部と、
前記復号部で復号されたデータに対して所定の演算を実行する演算実行部と、
前記演算実行部による演算結果のデータを前記第１暗号鍵で暗号化する暗号化部と、
前記暗号化された前記演算結果のデータを前記情報処理装置に出力する出力部と、を有し、
前記情報処理装置は、
前記クライアント装置から前記第１暗号鍵で暗号化されたデータを受信する受信部と、
前記データに対して実行する処理中の、少なくとも暗号化されたデータのままで実行不能な演算について、前記演算装置の前記演算実行部に実行させることにより、前記処理の結果を算出する演算制御部と、

前記処理の結果を前記クライアント装置に送信する送信部と、
を備えることを特徴とする演算システム。
【請求項２０】
前記第１暗号鍵及び前記第１復号鍵は、準同型暗号方式に従う鍵であり、
前記情報処理装置の前記演算制御部は、
前記処理中の暗号化されたデータに対してそのまま実行できる演算の少なくとも一部を実行する
ことを特徴とする請求項１９に記載の演算システム。
【請求項２１】
前記データに対して実行する処理は、畳込み演算を行う畳込レイヤーと、畳込レイヤーによる演算結果に対して活性化演算を実行する活性化レイヤーとを含むニューラルネットワークモデルによって実現される推論処理であり、
前記演算制御部は、少なくとも畳込レイヤーの演算を実行し、
前記演算装置の演算実行部は、前記活性化レイヤーの演算を実行する
ことを特徴とする請求項２０に記載の演算システム。
【請求項２２】
前記演算制御部は、
前記処理中の自情報処理装置と、前記演算装置とのいずれでも実行可能な演算について、前記情報処理装置の処理負荷と前記演算装置の処理負荷との少なくとも一方に基づいて、いずれで実行させるかを制御する
ことを特徴とする請求項１９に記載の演算システム。
【請求項２３】
クライアント装置とネットワークを介して接続される情報処理装置と、前記情報処理装置にバスを介して接続される演算装置と、を備える演算システムにおける演算装置による演算方法であって、
前記クライアント装置は、処理対象のデータを第１暗号鍵で暗号化させて、前記情報処理装置に送信し、前記情報処理装置から送信された暗号化された処理結果のデータを、前記第１暗号鍵に対応する第１復号鍵で復号し、
前記演算装置は、
前記クライアント装置との間で前記第１暗号鍵及び前記第１復号鍵を外部に秘匿した状態で共有し、
前記クライアント装置から送信されたデータに基づく前記第１暗号鍵で暗号化されているデータを前記情報処理装置から取得し、
取得されたデータを前記第１復号鍵で復号し、
復号されたデータに対して所定の演算を実行し、
演算結果のデータを前記第１暗号鍵で暗号化し、
前記暗号化された前記演算結果のデータを前記情報処理装置に出力する
演算方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データの漏洩を防止でき、広範な処理を実行可能にする技術に関する。
【背景技術】
【０００２】
従来、負荷が大きい処理をサーバで実行させて、その処理結果をクライアント装置で利用するサーバ・クライアントモデルが知られている。
【０００３】
このサーバ・クライアントモデルを用いると、処理対象のデータをクライアント装置からサーバに送信することになるため、データに含まれる個人情報等の機密性の高いデータが漏洩してしまうことがある。

【０００４】
このような問題に対処するために、データを暗号化したまま演算を行う秘匿演算方法を使用することが考えられる。秘匿演算方法としては、大きく分けると、準同型暗号を用いる方法と、ＭＰＣ（Ｍｕｌｔｉ－Ｐａｒｔｙ－Ｃｏｍｐｕｔａｔｉｏｎ）を用いる方法とがある。
【０００５】
まず、準同型暗号を用いる方法について説明する。
【０００６】
準同型暗号とは、平文と或る演算に対して、準同型な関係にある暗号文と演算との組が存在する暗号方式である。準同型暗号を厳密に表すと、平文ａ，ｂとその二変数関数Ｆ（ａ，ｂ）に対して、暗号化関数をＥｎｃとすると、暗号文ｃ１＝Ｅｎｃ（ａ）、暗号文ｃ２＝Ｅｎｃ（ｂ）が存在し、Ｅｎｃ（Ｆ（ａ，ｂ））＝Ｇ（ｃ１，ｃ２）となる関数Ｇが存在する暗号方式である。
【０００７】
準同型暗号にはいくつか種類があり、Ｆ（ａ，ｂ）＝ａ＋ｂである場合を加法準同型暗号（ＡＨＥ）と呼ぶ。なお、実際には、Ｆ（ａ，ｂ）＝ａ＋ｂ　ｍｏｄ　ｎである場合も、扱う平文が十分小さければ実質ａ＋ｂとみなせるので、加法準同型暗号と呼ばれる。
【０００８】
また、Ｆ（ａ，ｂ）＝ａ×ｂである場合を乗法準同型暗号（ＭＨＥ）と呼ぶ。なお、実際には、Ｆ（ａ，ｂ）＝ａ×ｂ　ｍｏｄ　ｎである場合も、扱う平文が十分小さければ実質ａ×ｂとみなせるので、乗法準同型暗号と呼ばれる。
【０００９】
また、加法と乗法の両方の演算が扱える場合を、完全準同型暗号（ＦＨＥ）と呼ばれる。この完全準同型暗号は、計算量や鍵長などの点から実用的ではないと現在みなされている。
【００１０】
また、演算回数に上限を設けることで、加法と乗法の両方が行え、かつある程度実用的なものとして、Ｓｏｍｅｗｈａｔ準同型暗号（ＳＨＥ）が存在する。
【００１１】
例えば、特許文献１には、準同型暗号を用いてデータを暗号化したまま推論を行う技術が開示されている。
【００１２】
一方、ＭＰＣとは、複数のコンピュータを用いて通信を行いながら、暗号化されたデータを演算するシステムであり、準同型暗号と比べて多種類の演算を行うことのできるシステムが提案されている。
【先行技術文献】
【特許文献】
【００１３】
【特許文献１】特許第６３９１９００号明細書
【発明の概要】
【発明が解決しようとする課題】
【００１４】
上記した加法準同型暗号及び乗法準同型暗号を用いた場合には、暗号化したまま行える演算に制約があるという問題点がある。また、完全準同型暗号を用いた場合には、計算量、鍵長が莫大なものであるという問題がある。また、Ｓｏｍｅｗｈａｔ準同型暗号を用いた場合には、演算回数に上限があるという問題がある。
【００１５】
一方、ＭＰＣを用いた場合には、一般的にコンピュータ間の通信速度によって処理性能が制約される問題がある。また、ＭＰＣにおいては、複数のコンピュータが結託して悪意を持つことが無いという前提条件を満たす必要があり、現実的な問題として、この前提条

件を満たすことが難しいという問題がある。例えば、複数のコンピュータが同時に悪意の有る演算を行えば、暗号を解読することができてしまうので、データが漏洩してしまうことがある。

【００１６】

本発明は、上記事情に鑑みなされたものであり、その目的は、データの漏洩を防止でき、且つ広範な処理を実行することのできる技術を提供することにある。

【課題を解決するための手段】

【００１７】

上記目的を達成するため、第１の観点に係る演算装置は、クライアント装置とネットワークを介して接続される情報処理装置にバスを介して接続される。クライアント装置は、処理対象のデータを第１暗号鍵で暗号化させて、情報処理装置に送信し、情報処理装置から送信された暗号化された処理結果のデータを、第１暗号鍵に対応する第１復号鍵で復号する。そして、演算装置は、鍵共有部と、取得部と、復号部と、演算実行部と、暗号化部と、出力部とを備える。鍵共有部は、クライアント装置との間で第１暗号鍵及び第１復号鍵を外部に秘匿した状態で共有する。取得部は、クライアント装置から送信されたデータに基づく第１暗号鍵で暗号化されているデータを情報処理装置から取得する。復号部は、取得部により取得された第１暗号鍵で暗号化されているデータを第１復号鍵で復号する。演算実行部は、復号部で復号されたデータに対して所定の演算を実行する。暗号化部は、演算実行部による演算結果のデータを第１暗号鍵で暗号化する。出力部は、暗号化された演算結果のデータを情報処理装置に出力する。

【発明の効果】

【００１８】

本発明によれば、データの漏洩を防止でき、且つ広範な処理を実行することができる。

【図面の簡単な説明】

【００１９】

【図１】図１は、一実施形態に係る計算機システムの全体構成図である。

【図２】図２は、一実施形態に係るクライアント装置の機能構成図である。

【図３】図３は、一実施形態に係るサーバの機能構成図である。

【図４】図４は、一実施形態に係る演算装置の機能構成図である

【図５】図５は、一実施形態に係るニューラルネットワークモデルの構成図である。

【図６】図６は、一実施形態に係る計算機システムの処理動作を示すシーケンス図である。

【図７】図７は、一実施形態に係るコンピュータ装置の構成図である。

【図８】図８は、第１変形例に係る演算装置の機能構成図である。

【図９】図９は、第２変形例に係る計算機システムの全体構成図である。

【図１０】図１０は、第２変形例に係るクライアント装置が備える鍵共有部の機能構成図である。

【図１１】図１１は、第２変形例に係る演算装置が備える鍵共有部の機能構成図である。

【発明を実施するための形態】

【００２０】

実施形態について、図面を参照して説明する。なお、以下に説明する実施形態は特許請求の範囲に係る発明を限定するものではなく、また実施形態の中で説明されている諸要素及びその組み合わせの全てが発明の解決手段に必須であるとは限らない。

【００２１】

まず、一実施形態に係る計算機システムについて説明する。

【００２２】

図１は、一実施形態に係る計算機システムの全体構成図である。

【００２３】

計算機システム１は、クライアント装置１０と、演算システム２とを備える。演算システム２は、サーバ２０と、演算装置３０とを備える。クライアント装置１０と、サーバ２

０とは、ネットワーク４０を介して接続されている。ネットワーク４０は、例えば、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｏｗｏｒｋ）や、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等である。サーバ２０と、演算装置３０とは、バス５０を介して接続されている。サーバ２０は、情報処理装置の一例である。

【００２４】

クライアント装置１０は、処理対象のデータを暗号化して演算システム２に送信し、演算システム２から暗号化された処理結果（例えば、推論結果）を受信し、暗号化された処理結果を復号し、処理結果を利用する。演算システム２は、暗号化されたデータを受信し、暗号化されたデータに対して所定の処理（例えば、推論処理）を実行し、暗号化された処理結果をクライアント装置１０に送信する。

【００２５】

図２は、一実施形態に係るクライアント装置の機能構成図である。

【００２６】

クライアント装置１０は、表示部１１と、暗号化部１２と、送信部１３と、記憶部１４と、鍵共有部１５と、復号部１６と、受信部１７とを含む。

【００２７】

記憶部１４は、処理を実行させる対象データ１４１と、対象データ１４１に対して推論処理を実行した結果である処理結果１４２と、データを復号及び暗号化するための秘密鍵１４３（第１復号鍵）及び公開鍵１４４（第１暗号鍵）とを記憶する。本実施形態では、秘密鍵１４３及び公開鍵１４４は、例えば、準同型暗号用の鍵である。準同型暗号としては、例えば、Ｐａｉｌｌｉｅｒ暗号や、ｌｉｆｔｅｄ－ＥｌＧａｍａｌ暗号等の加法準同型暗号であってもよく、乗法準同型暗号であってもよい。なお、処理結果１４２は、サーバ２０から処理結果が送信された場合に格納されるものであり、サーバ２０による推論処理が行われていない対象データ１４１に対する処理結果については、存在しない。また、記憶部１４は、秘密鍵１４３と公開鍵１４４とに代えて、通信用共通鍵を記憶してもよい。この場合には、以下の説明において、秘密鍵１４３と公開鍵１４４とは、通信用共通鍵と読み替える。すなわち、通信用共通鍵は、秘密鍵１４３と公開鍵１４４として機能する。

【００２８】

暗号化部１２は、記憶部１４に格納されている暗号化されていない対象データ１４１を、暗号化して、送信部１３に渡す。本実施形態では、暗号化部１２は、記憶部１４に格納されている公開鍵１４４を用いて対象データ１４１を暗号化する。送信部１３は、暗号化された推論処理の対象データ１４１をサーバ２０に送信する。なお、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いる場合には、暗号化部１２は、記憶部１４に格納されている通信用共通鍵を用いて対象データ１４１を暗号化する。

【００２９】

受信部１７は、サーバ２０から暗号化された処理結果１４２を受信して復号部１６に渡す。復号部１６は、受信部１７から渡された暗号化された処理結果１４２を復号し、復号した処理結果１４２を記憶部１４に格納する。本実施形態では、復号部１６は、記憶部１４に格納されている秘密鍵１４３を用いて暗号化された処理結果１４２を復号する。なお、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いる場合には、復号部１６は、記憶部１４に格納されている通信用共通鍵を用いて暗号化された処理結果１４２を復号する。

【００３０】

表示部１１は、記憶部１４に記憶された処理結果１４２に基づいて各種情報を表示する。表示部１１は、処理結果１４２をそのまま表示してもよく、処理結果１４２に基づいて所定の処理を実行し、その実行結果を表示するようにしてもよい。

【００３１】

鍵共有部１５は、演算装置３０との間で、外部（クライアント装置１０及び演算装置３０以外）に秘匿した状態で秘密鍵１４３及び公開鍵１４４を共有する処理（鍵共有処理）

を実行する。すなわち、鍵共有部１５は、サーバ２０にも知られることなく、秘密鍵１４３及び公開鍵１４４をクライアント装置１０と演算装置３０との間で共有する機能を有する。

【００３２】

ここで、加法準同型暗号について、加法準同型暗号であるＰａｉｌｌｉｅｒ暗号を例に挙げて説明する。

【００３３】

暗号に係る処理を行う場合には、以下のような各種設定を決定しておく。すなわち、暗号において使用する安全な素数ｐ及びｑを用意する。なお、素数の決定における手順や注意点は、ＲＳＡ暗号と同じでよい。また、Ｎ＝ｐ×ｑとする。また、ｋを１≦ｋ≦Ｎ－１の範囲で任意に設定する。ｇ＝１＋ｋＮとする。ここで、ｐ、ｑは、秘密鍵、ｇ、Ｎは、公開鍵、兼システムパラメータである。

【００３４】

例えば、平文データをＡ、Ｂ（０≦Ａ≦Ｎ－１、０≦Ｂ≦Ｎ－１）とすると、それぞれを暗号化した暗号化データe_A、e_Bは、以下の式（１）、（２）に示すように表される。

$e_A = g^A \times r_1^N \mod N^2$　・・・（１）

$e_B = g^B \times r_2^N \mod N^2$　・・・（２）

ここで、r_1（$0 \leqq r_1 \leqq N-1$）、及びr_2（$0 \leqq r_2 \leqq N-1$）は、乱数である。

【００３５】

Ｐａｉｌｌｉｅｒ暗号の暗号化データは、平文データ同士の和演算に対応する演算を、暗号化データの乗算として実行可能である。暗号化データの乗算、すなわち、$e_A \times e_B$は、式（３）に示すようになる。

$$e_A \times e_B = g^A \times g^B \times r_1^N \times r_2^N \mod N^2$$
$$= g^{(A+B)} \times r_1^N \times r_2^N \mod N^2 \cdots (A)$$

ここで、ｇ＝（１＋ｋＮ）であるので、g^Nのｇに（１＋ｋＮ）を代入して、g^N＝（１＋ｋＮ）^{N}が得られる。また、（１＋ｋＮ）^{N}を二項定理で展開すると、（１＋ｋＮ）^{N}＝１＋ｋN^2＋…となる。展開後の式１＋ｋN^2＋…の第二項以降は、全てN^2の倍数であるため、１＋ｋN^2＋…をN^2で割ったあまりは１である。したがって、$g^N \mod N^2 = 1$である。そして、$g^N = 1$であるため、$g^{(A+B)} = g^{(A+B \mod N)}$が成り立つ。すると、式（Ａ）は、$g^{(A+B)} = g^{(A+B \mod N)}$の関係を用いて、下記式のように変形できる。

$$\text{式（A）} = g^{(A+B \mod N)} \times r_1^N \times r_2^N \mod N^2$$
$$= g^{(A+B \mod N)} \times (r_1 \times r_2)^N \mod N^2 \cdots (B)$$

$r_3 = r_1 \times r_2 \mod N$と置いたとき、$r_1$も$r_2$も乱数なので、$r_3$も乱数となる。したがって、式（Ｂ）は下記式のように変形できる。

$$\text{式（B）} = g^{(A+B \mod N)} \times r_3^N \mod N^2$$
$$= e(A+B \mod N) \cdots (3)$$

式（３）に示すｅ（Ａ＋Ｂ　ｍｏｄ　Ｎ）は、復号すると、Ａ＋Ｂ　ｍｏｄ　Ｎとなる。したがって、ＡおよびＢがＮに比べて十分小さければ、実質Ａ＋Ｂとみなすことができるため、暗号化データの乗算は、平文データの和演算に対応していることがわかる。

【００３６】

また、Ｐａｉｌｌｉｅｒ暗号の暗号化データは、平文データと、平文データの整数との乗算に対応する演算を実行可能である。

平文データＡと整数Ｃとの乗算であるＡ×Ｃは、ＡをＣ回加算するという和演算に対応する。したがって、この和演算のそれぞれについて、暗号化データの乗算を行うことにより、暗号化データに対して平文データＡと整数Ｃとの乗算に対応する演算を実行することができる。

具体的には、$e_A \times e_A \times \cdots$、すなわち暗号化データの累乗（整数Ｃ乗）を行えばよいこととなり、式（４）に示すようになる。

$e_A \times e_A \times \cdots = e_{A+A+\cdots} = e_{AC}$ ・・・（４）

式（４）に示すe_{AC}は、復号すると、ＡＣとなり、平文データＡと整数Ｃとの乗算の結果となる。したがって、Ｐａｉｌｌｉｅｒ暗号の同じ暗号化データを累乗する演算が、平文データと、平文データの整数との乗算に対応する演算であることがわかる。

【００３７】

図３は、一実施形態に係るサーバの機能構成図である。

【００３８】

サーバ２０は、中継部２１と、推論処理制御部２２と、受信部２３と、記憶部２４と、送信部２５とを備える。推論処理制御部２２は、演算制御部の一例である。

【００３９】

中継部２１は、クライアント装置１０の鍵共有部１５と、演算装置３０の後述する鍵共有部３３、４０との間の鍵交換処理における通信を中継する。

【００４０】

推論処理制御部２２は、記憶部２４に格納されているモデル情報２４２に従って、暗号化された対象データ２４１を暗号化した状態で用いてニューラルネットワークモデルによる推論処理を実行する。そして、推論処理制御部２２は、暗号化された状態の推論処理の処理結果１４２を送信部２５に渡す。例えば、推論処理制御部２２は、ニューラルネットワークモデルの中の自身が担当する処理レイヤーについては、この処理レイヤーの処理を実行する。そして、推論処理制御部２２は、ニューラルネットワークモデル中の演算装置３０が担当する処理レイヤーについては、この処理レイヤーを演算処理３０に実行させるように制御する。ここで、ニューラルネットワークモデルに含まれる自身が担当する処理レイヤーは、暗号化されたデータのままで実行可能な処理レイヤーである。なお、ニューラルネットワークモデルの構成及び処理レイヤーの例については後述する。

【００４１】

記憶部２４は、暗号化された対象データ２４１と、推論処理制御部２２により実行される推論処理で用いられるニューラルネットワークモデルの各処理レイヤーの構成及び各処理レイヤーで使用する設定値の情報を含むモデル情報２４２と、を記憶する。対象データ２４１は、推論処理を実行させる対象のデータである。モデル情報２４２に含まれる設定値としては、例えば、畳込処理レイヤーで使用されるフィルタの係数や、アフィンレイヤーで用いられる重み等がある。なお、各処理レイヤーで使用する設定値等は、ニューラルネットワークモデルを用いた学習により得られた値を含む。

【００４２】

受信部２３は、クライアント装置１０から送信される暗号化された対象データ１４１を受信して記憶部２４に格納する。送信部２５は、推論処理制御部２２によって得られた暗号化されている処理結果１４２をクライアント装置１０に送信する。対象データ２４１は、暗号化された対象データ１４１、演算装置３０から取得する暗号化された演算結果、及び情報処理装置２０において暗号化されたまま処理された暗号化されたデータの少なくとも一つを含むデータである。

【００４３】

図４は、一実施形態に係る演算装置の機能構成図である

【００４４】

演算装置３０は、例えば、専用ＬＳＩ（Ｌａｒｇｅ－Ｓｃａｌｅ Ｉｎｔｅｇｒａｔｅｄ ｃｉｒｃｕｉｔ）や、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）や、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）により構成されている。本実施形態では、演算装置３０は、サーバ２０の内部バスに接続されている。演算装置３０は、復号部３１と、演算実行部３２と、鍵共有部３３と、暗号化部３４と、取得部３５と、出力部３６とを備える。演算装置３０は、例えば、外部の装置（サーバ２０等）に対しては暗号化されたデータのみしか出力しないように構成されている。演算装置３０は、例えば、全体又は大部分が、処理を実行するハードウェア回路で構成されており、不正にデータを出力するなどの不正動作

を起こさせるようにすることが困難（不可能又はほぼ不可能）となっている。したがって、サーバ２０によって、演算装置３０から処理途中の暗号化されていない状態のデータを取り出すことは、不可能又はほぼ不可能である。なお、演算装置３０は、外部の装置に対して少なくとも一部が暗号化されたデータを出力してもよい。

【００４５】

鍵共有部３３は、クライアント装置１０との間の鍵共有処理で使用する共有用秘密鍵３３１（第２復号鍵）及び共有用公開鍵３３２（第２暗号鍵）を記憶する。本実施形態では、共有用秘密鍵３３１は、演算装置３０の外部から読み取り不能に記憶されている。ここで、外部から読み取り不能な状態としては、ハードウェアの構成に起因して読み取り不能であってもよい。共有用秘密鍵３３１は、例えば、ハードワイヤード（結線論理）で記憶されていてもよい。鍵共有部３３は、クライアント装置１０との間で、外部（クライアント装置１０及び演算装置３０以外）に秘匿した状態で秘密鍵１４３及び公開鍵１４４を共有する処理（鍵共有処理）を実行する。具体的には、例えば、鍵共有部３３は、共有用公開鍵３３２をクライアント装置１０に送信し、クライアント装置１０で共有用公開鍵３３２により暗号化された秘密鍵１４３及び公開鍵１４４を取得する。そして、鍵共有部３３は、共有用秘密鍵３３１により暗号化された秘密鍵１４３及び公開鍵１４４を復号して、秘密鍵１４３及び公開鍵１４４を取得する。この鍵共有処理によると、クライアント装置１０と演算装置３０との間の経路では、秘密鍵１４３及び公開鍵１４４は暗号化されており、秘匿状態を確保できる。また、共有用秘密鍵３３１は、演算装置３０の外部から読み取り不能であるので、サーバ２０から読み出されて取得されることがないので、秘匿状態を厳重に維持することができる。

【００４６】

また、鍵共有部３３は、取得した秘密鍵１４３を復号部３１に設定し、取得した公開鍵１４４を暗号化部３４に設定する。なお、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いる場合には、鍵共有部３３は、取得した通信用共通鍵を復号部３１及び暗号化部３４に設定する。

【００４７】

取得部３５は、サーバ２０から渡される暗号化されているデータを取得する。そして、復号部３１は、サーバ２０から渡される暗号化されているデータを、設定されている秘密鍵１４３により復号する。なお、サーバ２０から渡される暗号化されているデータは、クライアント装置１０から送信された暗号化された対象データに基づく、暗号化されているデータである。すなわち、サーバ２０から渡される暗号化されているデータは、クライアント装置１０から送信された暗号化された対象データそのままの場合や、暗号化された対象データに対して何らかの処理が行われた後の暗号化されているデータである。復号部３１は、復号したデータを演算実行部３２に渡す。なお、取得部３５は、暗号化されているデータとともに、処理で使用する設定値をサーバ２０から受け取るようにし、受け取った設定値を演算実行部３２に設定又は通知するようにしてもよい。なお、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いる場合には、復号部３１は、サーバ２０から渡される暗号化されているデータを、設定されている通信用共通鍵により復号する。

【００４８】

演算実行部３２は、復号部３１から渡された復号されたデータに対して所定の処理を実行する。ここでの所定の処理は、ニューラルネットワークモデルにおける暗号化されたデータのままでは実行不可能な処理レイヤーを含む処理である。演算実行部３２は、演算結果を暗号化部３４に渡す。

【００４９】

暗号化部３４は、演算実行部３２から渡された演算結果を、設定された公開鍵１４４で暗号化して、暗号化したデータをサーバ２０の推論処理制御部２２に渡す。なお、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いる場合には、暗号化部３４は、演算実行部３２から渡された演算結果を、設定された通信用共通鍵で暗号化して、暗号化したデータをサーバ２０の推論処理制御部２２に渡す。

【００５０】
次に、ニューラルネットワークモデルの一例について説明する。
【００５１】
図５は、一実施形態に係るニューラルネットワークモデルの構成図である。
【００５２】
ニューラルネットワークモデル３は、推論処理制御部２２による推論処理の構成を示すニューラルネットワークモデルであり、例えば、処理対象とする画像データが何を表しているか、例えば、人、犬、猫等の何を表しているかを推論する推論処理を実行して処理結果を出力するための畳込みニューラルネットワーク（ＣＮＮ）のモデルである。
【００５３】
ニューラルネットワークモデル３は、複数の処理レイヤー４により構成されている。具体的には、ニューラルネットワークモデル３は、畳込レイヤー４－１、活性化レイヤー４－２、プーリングレイヤー４－３、活性化レイヤー４－ｎ－２、アフィンレイヤー４－ｎ－１、及びＳｏｆｔＭａｘレイヤー４－ｎ等を含む。畳込レイヤー４－１は、画像データについて畳込処理を実行する。活性化レイヤー４－２は、前レイヤーからの入力データに対して活性化処理を実行する。プーリングレイヤー４－３は、前レイヤーから入力されたデータについてダウンサンプリング処理を実行する。活性化レイヤー４－ｎ－２は、前レイヤーからの入力データに対して活性化処理を実行する。アフィンレイヤー４－ｎ－１は、前レイヤーからの入力データに対してアフィン変換処理を実行する。ＳｏｆｔＭａｘレイヤー４－ｎは、前レイヤーからの入力データに対してソフトマックス（ＳｏｆｔＭａｘ）関数による処理を実行する。活性化処理を行う活性化レイヤーとしては、例えば、ＲｅＬＵ関数（Ｒｅｃｔｉｆｉｅｄ Ｌｉｎｅａｒ Ｕｎｉｔ Ｒｅｃｔｉｆｉｅｒ：正規化線形関数）による活性化処理を行う活性化レイヤーがある。
【００５４】
本実施形態では、畳込みレイヤー４－１の演算処理については、加法準同型暗号による暗号化データをそのまま用いて処理を行うことができるものとなっている。また、その他のレイヤー４については、暗号化されたデータをそのまま用いて処理することができないものとなっている。
【００５５】
このようなニューラルネットワークモデル３について、推論処理制御部２２は、暗号化されたデータのままで演算できる処理レイヤーは、予め決められた設定に従って、サーバ２０と演算装置３０とのいずれかに実行させる。また、推論処理制御部２２は、暗号化されたデータのままで演算できない処理レイヤーは、演算装置３０に実行させる。したがって、暗号化されたデータのままで演算できる処理レイヤーは、設定によって、全てをサーバ２０側で実行するようにすることも、一部をサーバ２０側で実行するようにすることも、すべてを演算装置３０側で実行させるようにすることもできる。なお、演算装置３０で処理レイヤーを実行させるためには、例えば、演算装置３０の演算実行部３２に、演算装置３０側で実行させる全ての処理レイヤー４を実行するための回路を構成しておけばよい。この場合、処理レイヤー４で使用する変数等の設定値については、予め固定的に設定してもよく、処理に際して、推論処理制御部２２から演算装置３０に渡して設定するようにしてもよい。
【００５６】
次に、計算機システム１における処理動作について説明する。
【００５７】
図６は、一実施形態に係る計算機システムの処理動作を示すシーケンス図である。
【００５８】
クライアント装置１０の鍵共有部１５は、ユーザから所定の対象データに対する処理の指示を受け取ると、共有用公開鍵の要求を、サーバ２０を介して演算装置３０に送信する（ステップＳ１０１，Ｓ１０２）。これに対して、演算装置３０の鍵共有部３３は、共有用公開鍵３３２を、サーバ２０を介してクライアント装置１０に送信する（ステップＳ１

０３，Ｓ１０４）。
【００５９】
クライアント装置１０の鍵共有部１５は、共有用公開鍵３３２を受信し、共有用公開鍵３３２を使用して、秘密鍵１４３及び公開鍵１４４を暗号化する（ステップＳ１０５）。次いで、クライアント装置１０の鍵共有部１５は、暗号化した秘密鍵１４３及び公開鍵１４４を、サーバ２０を介して演算装置３０に送信する（ステップＳ１０６，Ｓ１０７）。
【００６０】
演算装置３０の鍵共有部３３は、暗号化された秘密鍵１４３及び公開鍵１４４を受信し、共有用秘密鍵３３１を用いて暗号化された秘密鍵１４３及び公開鍵１４４を復号して、秘密鍵１４３及び公開鍵１４４を得る。そして、鍵共有部３３は、秘密鍵１４３を復号部３１に設定するとともに、公開鍵１４４を暗号化部３４に設定する（ステップＳ１０８）。このようなステップＳ１０１～Ｓ１０８により、クライアント装置１０と演算装置３０との間で外部に秘匿した状態で秘密鍵１４３及び公開鍵１４４の共有が完了する。
【００６１】
次いで、クライアント装置１０の暗号化部１２は、公開鍵１４４を用いて、対象データ１４１を暗号化し、送信部１３に渡す（ステップＳ１０９）。次いで、送信部１３は、暗号化された対象データをサーバ２０に送信する（ステップＳ１１０）。
【００６２】
サーバ２０では、暗号化された対象データを受信部２３が受信して記憶部２４に格納する。そして、推論処理制御部２２が対象データに対する推論処理を開始する（ステップＳ１１１）。
【００６３】
この推論処理においては、サーバ２０が実行するレイヤーの処理については、推論処理制御部２２は、暗号化されたデータをそのまま使用して演算を実行する（ステップＳ１１２）。
【００６４】
一方、演算装置３０で実行する１以上の処理レイヤーの処理については、推論処理制御部２２は、暗号化されている処理用のデータ、すなわち、暗号化されている対象データ又は、直前のレイヤーによる処理結果のデータを演算装置３０に送信する（ステップＳ１１３）。演算装置３０では、暗号化されている処理用のデータを受信すると、復号部３１が秘密鍵１４３を用いて処理用データを復号して演算実行部３２に渡す。演算実行部３２は、復号された処理用データに対して所定の演算を実行し、演算処理後のデータを暗号化部３４に渡す（ステップＳ１１５）。暗号化部３４は、演算処理後のデータを、公開鍵１４４を用いて暗号化し（ステップＳ１１６）、暗号化された演算処理後のデータをサーバ２０に送信する（ステップＳ１１７）。
【００６５】
このようにして推論処理を実行する全てのレイヤーの処理が実行されることにより推論処理が終了し、暗号化されている処理結果が得られることとなる。
【００６６】
推論処理が終了すると、サーバ２０の推論処理制御部２２は、暗号化されている処理結果を送信部２５に渡す。そして、送信部２５は、暗号化されている処理結果をクライアント装置１０に送信する（ステップＳ１１８）。
【００６７】
クライアント装置１０では、暗号化されている処理結果を受信部１７が受信して、復号部１６に渡す。また、復号部１６は、受け取った暗号化されている処理結果を秘密鍵１４３で復号して記憶部１４に格納する。そして、表示部１１は、処理結果に基づいて情報を表示する（ステップＳ１１９）。
【００６８】
以上説明したように、計算機システム１の処理において、サーバ２０は、暗号化したままでデータを処理するので、データが漏洩することを防止できる。また、演算装置３０内

では、データが復号されて処理されるが、サーバ２０から演算装置３０内の暗号化されていないデータを取り出すことは不可能であるので、データが漏洩することを防止できる。

【００６９】

上記したクライアント装置１０及びサーバ２０は、それぞれコンピュータ装置により構成することができる。

【００７０】

図７は、一実施形態に係るコンピュータ装置の構成図である。なお、本実施形態では、クライアント装置１０及びサーバ２０は、別々のコンピュータ装置で構成されているが、これらコンピュータ装置は、一部の構成を除き同様な構成を有するものとすることができる。したがって、以下の説明では、便宜的に図７に示すコンピュータ装置を用いて、クライアント装置１０及びサーバ２０を構成するコンピュータ装置について説明することとする。

【００７１】

コンピュータ装置１００は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎ Ｕｎｉｔ）１０１（プロセッサ）と、メインメモリ１０２と、ＧＰＵ（Ｇｒａｐｈｉｃｓ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１０３と、リーダライタ１０４と、通信インターフェース（通信Ｉ／Ｆ）１０５と、補助記憶装置１０６と、入出力インターフェース（入出力Ｉ／Ｆ）１０７と、表示装置１０８と、入力装置１０９とを備える。ＣＰＵ１０１、メインメモリ１０２、ＧＰＵ１０３、リーダライタ１０４、通信Ｉ／Ｆ１０５、補助記憶装置１０６、入出力Ｉ／Ｆ１０７、及び表示装置１０８は、バス１１０を介して接続されている。クライアント装置１０と、サーバ２０とは、それぞれコンピュータ装置１００に記載の構成要素の一部または全てを適宜選択して構成される。本実施形態では、サーバ２０を構成するコンピュータ装置１００においては、バス１１０を介して演算装置３０が接続されている。なお、演算装置３０は、コンピュータ装置１００の構成要素の一部またはすべてを適宜選択して構成してもよい。また、ＣＰＵ１０１は、例えば、ＡＳＩＣ及びＦＰＧＡなどの他の種類のプロセッサでもよい。

【００７２】

ここで、メインメモリ１０２又は補助記憶装置１０６の少なくとも一方が、クライアント装置１０の記憶部１４、サーバ２０の記憶部２４として機能する。なお、メインメモリ１０２又は補助記憶装置１０６の少なくとも一方が、後述する演算装置３０の記憶部として機能してもよい。また、メインメモリ１０２又は補助記憶装置１０６の少なくとも一方が、後述する演算装置６０の記憶部６０Ｂとして機能してもよい。さらに、メインメモリ１０２又は補助記憶装置１０６の少なくとも一方が、後述する演算装置７０の記憶部７０Ｂとして機能してもよい。

【００７３】

クライアント装置１０を構成するコンピュータ装置１００において、ＣＰＵ１０１は、補助記憶装置１０６に格納された処理プログラムを実行することにより、例えば、表示部１１、暗号化部１２、鍵共有部１５、復号部１６、及び後述する鍵共有部６０の制御部６０Ａとして機能してもよい。サーバ２０を構成するコンピュータ装置１００において、ＣＰＵ１０１は、補助記憶装置１０６に格納された処理プログラムを実行することにより、例えば、推論処理制御部２２として機能してもよい。なお、サーバ２０を構成するコンピュータ装置１００のＣＰＵ１０１は、クライアント装置１０を構成するコンピュータ装置１００のＣＰＵ１０１よりも処理性能が良いものとしてもよい。なお、ＣＰＵ１０１は、演算装置３０の復号部３１、演算実行部３２、鍵共有部３３、暗号化部３４、及び後述する鍵共有部７０の制御部７０Ａとして機能してもよい。

【００７４】

メインメモリ１０２は、例えば、ＲＡＭ、ＲＯＭ等であり、ＣＰＵ１０１に実行されるプログラム（処理プログラム等）や、各種情報を記憶する。補助記憶装置１０６は、例えば、ＨＤＤ（Ｈａｒｄ　ＤＩＳＫ　Ｄｒｉｖｅ）、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）等の非一時的記憶デバイス（不揮発性記憶デバイス）であり、ＣＰＵ１０１で

実行されるプログラムや、各種情報を記憶する。クライアント装置１０を構成するコンピュータ装置１００では、メインメモリ１０２は、例えば、対象データ１４１、処理結果１４２、秘密鍵１４３、及び公開鍵１４４を記憶する。サーバ２０を構成するコンピュータ装置１００では、メインメモリ１０２は、例えば、対象データ２４１やモデル情報２４２を記憶する。

【００７５】

ＧＰＵ１０３は、例えば、画像処理等の特定の処理の実行に適しているプロセッサであり、例えば、並列的に行われる処理の実行に適している。本実施形態では、ＧＰＵ１０３は、ＣＰＵ１０１の指示に従って所定の処理を実行する。

【００７６】

リーダライタ１０４は、記録媒体１１１を着脱可能であり、記録媒体１１１からのデータの読み出し、及び記録媒体１１１へのデータの書き込みを行う。記録媒体１１１としては、例えば、ＳＤメモリーカード、ＦＤ（フロッピーディスク：登録商標）、ＣＤ、ＤＶＤ、ＢＤ（登録商標）、フラッシュメモリ等の非一時的記録媒体（不揮発性記録媒体）がある。本実施形態においては、記録媒体１１１に、処理プログラムを格納しておき、リーダライタ１０４により、これを読み出して、利用するようにしてもよい。また、クライアント装置１０を構成するコンピュータ装置１００において、記録媒体１１１に、処理対象データを格納しておき、リードライタ１０４により、これを読み出して記憶部１４に格納するようにしてもよい。

【００７７】

通信Ｉ／Ｆ１０５は、ネットワーク４０に接続されており、ネットワーク４０に接続された他の装置との間でのデータの送受信を行う。クライアント装置１０の送信部１３、受信部１７、及び鍵共有部１５、サーバ２０の受信部２３、送信部２５、及び中継部２１は、それぞれを構成するコンピュータ装置１００の通信Ｉ／Ｆ１０５及びＣＰＵ１０１によって構成される。通信Ｉ／Ｆ１０５は、演算装置３０において、取得部３５と、出力部３６として機能してもよい。

【００７８】

入出力Ｉ／Ｆ１０７は、例えば、マウス、キーボード等の入力装置１０９と接続されている。クライアント装置１０を構成するコンピュータ装置１００において、入出力Ｉ／Ｆ１０７は、入力装置１０９を用いた、クライアント装置１０のユーザによる操作入力を受け付ける。また、サーバ２０を構成するコンピュータ装置１００において、入出力Ｉ／Ｆ１０７は、入力装置１０９を用いた、サーバ２０の管理者による操作入力を受け付ける。入出力Ｉ／Ｆ１０７は、演算装置３０において、取得部３５と、出力部３６として機能してもよい。

【００７９】

表示装置１０８は、例えば、液晶ディスプレイ等のディスプレイ装置であり、各種情報を表示出力する。表示装置１８は、例えば、クライアント装置１０において、表示部１１として機能する。

【００８０】

次に、変形例に係る計算機システムについて説明する。

【００８１】

図８を参照して、第１変形例について説明する。

図８は、第１変形例に係る演算装置の機能構成図である。なお、実施形態に係る演算装置３０と同様の構成には、同一の符号を付し、重複する説明を省略する。

【００８２】

変形例に係る演算装置３０Ａは、上記した演算装置３０において、演算実行部３２に代えて演算実行部３８を備え、復号部３１に代えて復号部３７を備えている。

復号部３７は、復号部３１の機能に加えて、取得部３５を介して推論処理制御部２２から実行する演算の種類の指定を受け付けて、演算実行部３８に渡す。なお、処理レイヤーの指定は、複数の処理レイヤーの指定であってもよい。

【００８３】
演算実行部３８は、処理レイヤー４に対応する処理を実行するハードウェア回路で構成された複数の演算部３８１、３８２等を有する。演算実行部３８は、復号部３７から渡された演算の種類の指定に対応する処理を実行する演算部３８１を選択し、復号部３７から渡されるデータを選択した演算部に入力する。なお、復号部３７から複数の演算の種類の指定を受け付けた場合には、その指定に対応する演算部を順次選択し、前の処理レイヤーを実行する演算部による処理結果のデータを、次の処理レイヤーの演算部への入力とする。
【００８４】
なお、変形例に係る演算装置３０Ａを利用する場合には、サーバ２０の推論処理制御部２２は、演算処理３０Ａに対して処理レイヤーの処理を実行させるとき、その処理レイヤーに対応する演算の種類の指定を演算装置３０Ａに送信する機能を備えている。また、上記の演算の種類の指定に代えて、処理レイヤーを指定してもよい。この場合には、演算実行部３８は、処理レイヤーの指定に対応する処理を実行する演算部を選択する。
【００８５】
図９から図１１を参照して、第２変形例について説明する。
第２変形例では、クライアント装置１０と演算装置３０との間で、共有用秘密鍵３３１及び共有用公開鍵３３２に代えて、共有用共通鍵を用いて秘密鍵１４３及び公開鍵１４４を共有する。すなわち、第２変形例では、クライアント装置１０と演算装置３０とが、それぞれ共有用共通鍵を記憶する。そして、クライアント装置１０は、共有用共通鍵を用いて秘密鍵１４３及び公開鍵１４４を暗号化して、暗号化した秘密鍵１４３及び公開鍵１４４を演算装置３０に送信する。演算装置３０は、暗号化された秘密鍵１４３及び公開鍵１４４を受信して、共有用共通鍵を用いて暗号化された秘密鍵１４３及び公開鍵１４４を復号する。以上により、クライアント装置１０及び演算装置３０とは、秘密鍵１４３及び公開鍵１４４を共有する。
【００８６】
なお、第２変形例において、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いてもよい。すなわち、クライアント装置１０は、共有用共通鍵を用いて通信用共通鍵を暗号化して、暗号化した通信用共通鍵を演算装置３０に送信する。演算装置３０は、暗号化された通信用共通鍵を受信して、共有用共通鍵を用いて暗号化された通信用共通鍵を復号する。この場合には、以下の説明において、秘密鍵１４３と公開鍵１４４とは、通信用共通鍵と読み替える。
【００８７】
第２変形例は、クライアント装置１０と演算装置３０との間において、外部に秘匿した状態で上述の共有用共通鍵を共有する方法に特徴を有するものである。以下の説明においては、第２変形例の特徴であるクライアント装置１０と演算装置３０との間における共有用共通鍵の共有の手法を説明する。なお、実施形態に係るクライアント装置１０及び演算装置３０と同様の構成には、同一の符号を付し、重複する説明を省略する。
【００８８】
図９は、第２変形例に係る計算機システムの全体構成図である。
クライアント装置１０は、公開鍵６６を記憶する。また、演算装置３０は、秘密鍵７５を記憶する。なお、演算装置３０は、第２変形例においては、後述する処理により作成される共有用共通鍵を用いて秘密鍵１４３及び公開鍵１４４をクライアント装置１０との間で共有するため、共有用秘密鍵３３１と共有用公開鍵３３２とを記憶しなくてもよい。
【００８９】
図１０は、第２変形例に係るクライアント装置が備える鍵共有部の機能構成図である。
図１０を参照して、第２変形例に係るクライアント装置１０が備える鍵共有部６０について説明する。なお、実施形態に係るクライアント装置１０と同様の構成は、図示を省略する。
【００９０】

クライアント装置１０は、鍵共有部１５に代えて、鍵共有部６０を備える。
鍵共有部６０は、制御部６０Ａと記憶部６０Ｂとを備える。制御部６０Ａは、検証部６１と、生成部６２と、作成部６３と、暗号化部６４と、復号部６５とを含む。また、記憶部６０Ｂは、公開鍵６６と、共有用共通鍵６７とを記憶する。なお、共有用共通鍵６７は、演算装置３０との鍵共有処理の結果として記憶される。

【００９１】

公開鍵６６は、演算装置３０に記憶されている秘密鍵７５に対応する公開鍵である。公開鍵６６は、例えば、演算装置３０の開発者及び製造者を含む開発者等が演算装置３０に秘密鍵７５を記憶させたとき、演算装置３０の使用者であるクライアントに配布される。公開鍵６６は、例えば、クライアント装置１０で推論処理を実行するアプリケーションが起動されたときに呼び出される、ＤＬＬ（Ｄｙｎａｍｉｃ　Ｌｉｎｋ　Ｌｉｂｒａｒｙ）に埋め込まれて配布されてもよい。なお、公開鍵６６は、秘密鍵７５に対応する復号鍵でもよい。
共有用共通鍵６７は、演算装置３０との間で、鍵共有を実行することにより、外部に秘匿した状態で共有される鍵であり、実施形態における共有用秘密鍵３３１及び共有用公開鍵３３２として機能する。

【００９２】

図１１は、第２変形例に係る演算装置が備える鍵共有部の機能構成図である。
図１１を参照して、第２変形例に係る演算装置３０が備える鍵共有部７０について説明する。なお、実施形態に係る演算装置３０と同様の構成は、図示を省略する。
演算装置３０は、鍵共有部３３に代えて、鍵共有部７０を備える。
鍵共有部７０は、制御部７０Ａと記憶部７０Ｂとを備える。制御部７０Ａは、生成部７１と、作成部７２と、暗号化部７３と、復号部７４とを含む。また、記憶部７０Ｂは、秘密鍵７５と、共有用共通鍵７６とを記憶する。なお、共有用共通鍵７６は、クライアント装置１０との鍵共有処理の結果として記憶される。

【００９３】

秘密鍵７５は、演算装置３０の外部から読み取り不可能な状態で記憶部７０Ｂに記憶される。秘密鍵７５は、例えば、演算装置３０の開発者及び製造者を含む開発者等により決定され、演算装置３０の製造時にハードワイヤードなどの耐タンパ性を有する記憶方法を用いて、記憶部７０Ｂに記憶されてもよい。共有用共通鍵７６は、クライアント装置１０との間で鍵共有を実行することにより、外部に秘匿した状態で共有される鍵であり、実施形態における共有用秘密鍵３３１及び共有用公開鍵３３２として機能する。すなわち、クライアント装置１０に記憶される共有用共通鍵６７と、演算装置３０に記憶される共有用共通鍵７６とは同じ値である。

【００９４】

図２から図４、並びに図１０及び図１１を参照して、クライアント装置１０と演算装置３０との間で実行される共有用共通鍵の鍵共有処理について説明する。以下の説明において、クライアント装置１０と演算装置３０とは、有限巡回群を定義する各種パラメータと、ハッシュ関数などとを共有しているものとする。

【００９５】

演算装置３０において、生成部７１は、ランダムな一時鍵ａを生成する。一時鍵ａは、整数の中からランダムに選択された値である。作成部７２は、一時鍵ａと生成元Ｇとを用いて離散対数問題が困難な有限巡回群の元として公開鍵ａＧを作成する。生成元Ｇは、例えば、楕円曲線群の基点Ｇ（ベースポイント）である。以下の説明では、有限巡回群が楕円曲線群であるものとして説明する。なお、有限巡回群が有限体乗法群である場合には、有限巡回群の生成元は生成元ｇであり、公開鍵$g^{a} \bmod n$が作成される。ｎは、素数である。一時鍵ａは、第１整数の一例である。また、公開鍵ａＧは、第１公開鍵の一例である。

【００９６】

作成部７２は、公開鍵ａＧにハッシュ関数Ｈを適用して、ハッシュ値Ｈ（ａＧ）を求め

る。さらに、作成部７２は、ハッシュ値Ｈ（ａＧ）と秘密鍵７５とを用いて、電子署名ｓを作成する。電子署名ｓは、例えば、ハッシュ値Ｈ（ａＧ）を、秘密鍵７５で暗号化した値である。なお、有限巡回群が有限体乗法群である場合には、ハッシュ値は、Ｈ（g^{a}ｍｏｄｎ）である。

【００９７】

出力部３６は、サーバ２０を介してクライアント装置１０に公開鍵ａＧと電子署名ｓとを送信する。具体的には、出力部３６は、サーバ２０に公開鍵ａＧと電子署名ｓとを出力し、サーバ２０の中継部２１がクライアント装置１０に公開鍵ａＧと電子署名ｓとを送信する。

クライアント装置１０において、受信部１７は、公開鍵ａＧと電子署名ｓとを受信する。検証部６１は、公開鍵ａＧにハッシュ関数を適用してハッシュ値Ｈ（ａＧ）を求める。そして、検証部６１は、ハッシュ値Ｈ（ａＧ）と、電子署名ｓ及び公開鍵６６とを用いて署名の検証を実行する。

【００９８】

電子署名ｓを用いた署名の検証の一例を説明する。検証部６１は、公開鍵ａＧにハッシュ関数Ｈを適用する。また、検証部６１は、公開鍵６６で電子署名ｓを復号する。そして、検証部６１は、公開鍵ａＧにハッシュ関数Ｈを適用した値と、電子署名ｓを復号した値とが等しいとき、公開鍵ａＧの正当性を確認する。公開鍵ａＧが正当であるとは、公開鍵ａＧが秘密鍵７５を保有する演算装置３０で作成されたことを保証することである。なお、署名の検証には、例えば、ＲＳＡ、ＤＳＡ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）、またはＥＣＤＳＡ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）などの署名アルゴリズムを用いてもよい。

【００９９】

生成部６２は、電子署名ｓにより公開鍵ａＧの正当性が確認されたとき、一時鍵ｂを生成する。一時鍵ｂは、整数の中からランダムに選択された値である。そして、作成部６３は、一時鍵ｂと生成元Ｇとを用いて離散対数問題が困難な有限巡回群の元として公開鍵ｂＧを作成する。なお、有限巡回群が有限体乗法群である場合には、有限巡回群の生成元は生成元ｇであり、公開鍵g^{b}ｍｏｄｎが作成される。一時鍵ｂは、第２整数の一例である。また、公開鍵ｂＧは、第２公開鍵の一例である。

【０１００】

作成部６３は、さらに、一時鍵ｂと公開鍵ａＧとを乗算した値にハッシュ関数Ｈを適用して共有用共通鍵６７としてＨ（ｂ×ａＧ）を作成する。なお、有限巡回群が有限体乗法群である場合には、共有用共通鍵６７としてＨ（（g^{a}ｍｏｄｎ）^{b}ｍｏｄｎ））が作成される。また、共有用共通鍵６７は、単にｂ×ａＧとしてもよい。

送信部１３は、公開鍵ｂＧを演算装置３０に送信する。具体的には、送信部１３は、サーバ２０に公開鍵ｂＧを送信し、サーバ２０の中継部２１が演算装置３０に公開鍵ｂＧを入力する。

【０１０１】

演算装置３０において、取得部３５は、公開鍵ｂＧを取得する。すなわち、取得部３５は、クライアント装置１０で電子署名ｓにより公開鍵ａＧの正当性が確認されたとき、クライアント装置１０で作成された公開鍵ｂＧを取得する。

そして、作成部７２は、一時鍵ａと公開鍵ｂＧとにハッシュ関数Ｈを適用して共有用共通鍵７６としてＨ（ａ×ｂＧ）を作成する。なお、有限巡回群が有限体乗法群である場合には、共有用共通鍵７６としてＨ（（g^{b}ｍｏｄｎ）^{a}ｍｏｄｎ））が作成される。また、共有用共通鍵７６は、単にａ×ｂＧとしてもよい。

【０１０２】

上述の処理により、クライアント装置１０と演算装置３０とは、外部に秘匿した状態で共有用共通鍵を共有する。すなわち、サーバ２０及びその他の装置は、公開鍵ａＧ及び公開鍵ｂＧを取得しても、公開鍵ａＧ及び公開鍵ｂＧは離散対数問題が困難なため、公開鍵

ａＧ及び公開鍵ｂＧから一時鍵ａ及び一時鍵ｂを求めることができない。また、サーバ２０及びその他の装置は、電子署名ｓを取得しても、電子署名ｓから一時鍵ａ及び一時鍵ｂを求めることができない。したがって、一時鍵ａ及び一時鍵ｂが得られないサーバ２０及びその他の装置は、ａ×ｂＧ及びｂ×ａＧを求めることができないので、共有用共通鍵を取得することが不可能である。

【０１０３】

また、サーバ２０及びその他の装置は、一時鍵ａ´を生成し、公開鍵ａＧを別の値ａ´Ｇにすり替えてクライアント装置１０に送信する。さらに、サーバ２０及びその他の装置は、クライアント装置１０から公開鍵ｂＧを取得して不正な共有用共通鍵ａ´×ｂＧを作成する。これにより、サーバ２０及びその他の装置は、クライアント装置１０との間で不正な共有用共通鍵ａ´×ｂＧを共有する不正行為が考えられる。

【０１０４】

この場合でも、サーバ２０及びその他の装置は、秘密鍵７５を有していないため、別の値ａ´Ｇに対応する電子署名ｓ´を作成することができない。すると、クライアント装置１０は、別の値ａ´Ｇが正当なものであると確認できないため、サーバ２０に公開鍵ｂＧを送信することがないし、不正な共有用共通鍵ａ´×ｂＧを正当なものとして作成することもない。したがって、サーバ２０及びその他の装置は、不正な共有用共通鍵ａ´×ｂＧを用いて、クライアント装置１０から送信される暗号化データを復号することも不可能である。

【０１０５】

以上により、第２変形例に係るクライアント装置１０と演算装置３０とは、サーバ２０及びその他の装置の中間者攻撃を防ぐための処理として、複雑な演算と複数回の通信とが発生するＤＨ－ＥＫＥなどの煩雑な処理をすることなく、共有用共通鍵を共有することができる。

【０１０６】

共有用共通鍵を共有した後の秘密鍵１４３及び公開鍵１４４の共有処理について説明する。なお、以下の処理において、秘密鍵１４３及び公開鍵１４４に代えて、通信用共通鍵を用いる場合には、秘密鍵１４３と公開鍵１４４とを、通信用共通鍵と読み替える。

クライアント装置１０において、暗号化部６４は、共有用共通鍵６７を用いて、秘密鍵１４３及び公開鍵１４４を暗号化する。送信部１３は、暗号化した秘密鍵１４３及び公開鍵１４４を演算装置３０に送信する。具体的には、送信部１３は、サーバ２０に暗号化した秘密鍵１４３及び公開鍵１４４を送信し、サーバ２０の中継部２１が演算装置３０に暗号化した秘密鍵１４３及び公開鍵１４４を入力する。

【０１０７】

演算装置３０において、取得部３５は、暗号化された秘密鍵１４３及び公開鍵１４４を取得する。そして、復号部７４は、共有用共通鍵７６を用いて暗号化された秘密鍵１４３及び公開鍵１４４を復号する。これにより、クライアント装置１０及び演算装置３０とは、秘密鍵１４３及び公開鍵１４４を共有する。

【０１０８】

なお、秘密鍵１４３及び公開鍵１４４を演算装置３０からクライアント装置１０に送信して、秘密鍵１４３及び公開鍵１４４を共有する場合には、以下の処理を実行する。

演算装置３０において、暗号化部７３は、共有用共通鍵７６を用いて、秘密鍵１４３及び公開鍵１４４を暗号化する。出力部３６は、サーバ２０を介してクライアント装置１０に暗号化した秘密鍵１４３及び公開鍵１４４を送信する。具体的には、出力部３６は、サーバ２０に暗号化した秘密鍵１４３及び公開鍵１４４を出力し、サーバ２０の中継部２１がクライアント装置１０に暗号化した秘密鍵１４３及び公開鍵１４４を送信する。

【０１０９】

クライアント装置１０において、受信部１７は、暗号化された秘密鍵１４３及び公開鍵１４４を受信する。復号部６５は、共有用共通鍵６７を用いて暗号化された秘密鍵１４３及び公開鍵１４４を復号する。これにより、クライアント装置１０及び演算装置３０とは

、秘密鍵１４３及び公開鍵１４４を共有する。
なお、上述の説明において、説明の簡単化のため、暗号化部６４及び復号部６５とは、暗号化部１２及び復号部１６と別に設けられるものとして説明したが、暗号化部１２と復号部１６とが、それぞれ暗号化部６４と復号部６５として機能してもよい。また、暗号化部７３及び復号部７４とは、暗号化部３４及び復号部３１と別に設けられるものとして説明したが、暗号化部３４と復号部３１とが、それぞれ暗号化部７３と復号部７４として機能してもよい。

【０１１０】
上記の第２変形例の手法でも問題ない場合が多いが、秘密鍵７５を全デバイスに書き込んで配布するのでは、記憶部７０Ｂに耐タンパ性を持たせるなどの対策が必要であり、秘密鍵７５が安全に記憶できないことがある。この場合には、開発者等は、演算装置３０ごとに一時鍵ａを決定し、演算装置３０の電子署名ｓを求め、工場出荷時に秘密鍵７５に代えて、一時鍵ａと電子署名ｓとを演算装置３０の記憶部７０Ｂに書き込んでもよい。すなわち、記憶部７０Ｂは、一時鍵ａと電子署名ｓとを記憶する。なお、記憶部７０Ｂは、クライアント装置１０との鍵共有処理の結果として共有用共通鍵７６を記憶する。

【０１１１】
具体的には、演算装置３０において、記憶部７０Ｂは、一時鍵ａ、公開鍵ａＧ及び秘密鍵７５を用いて開発者等により作成された電子署名ｓと、一時鍵ａとを記憶する。作成部７２は、一時鍵ａと生成元Ｇとを用いて離散対数問題が困難な有限巡回群の元として公開鍵ａＧを作成する。そして、出力部３６は、サーバ２０を介してクライアント装置１０に公開鍵ａＧと、電子署名ｓとを出力する。

【０１１２】
クライアント装置１０において、検証部６１は、電子署名ｓにより公開鍵ａＧの正当性が確認されたとき、ランダムな一時鍵ｂと公開鍵ａＧとを用いて共有用共通鍵６７を作成する。また、作成部６３は、一時鍵ｂと生成元Ｇとを用いて離散対数問題が困難な有限巡回群の元として公開鍵ｂＧを作成する。そして、送信部１３は、サーバ２０を介して公開鍵ｂＧを演算装置３０に送信する。

【０１１３】
演算装置３０において、取得部３５は、クライアント装置１０から、公開鍵ｂＧを取得する。作成部７２は、前記憶部７０Ｂに記憶されている一時鍵ａと公開鍵ｂＧとを用いて共有用共通鍵７６を作成する。

【０１１４】
さらに、一時鍵ａを演算装置３０ごとに固定する構成の別構成を説明する。開発者等は、演算装置３０ごとに一時鍵ａを決定し、演算装置３０の電子署名ｓを求め、一時鍵ａと生成元Ｇとを用いて作成された離散対数問題が困難な有限巡回群の元として公開鍵ａＧを作成する。そして、開発者等は、工場出荷時に秘密鍵７５に代えて、一時鍵ａと電子署名ｓと公開鍵ａＧとを演算装置３０の記憶部７０Ｂに書き込む。すなわち、記憶部７０Ｂは、一時鍵ａと電子署名ｓと公開鍵ａＧとを記憶する。なお、記憶部７０Ｂは、クライアント装置１０との鍵共有処理の結果として共有用共通鍵７６を記憶する。

【０１１５】
具体的には、演算装置３０において、記憶部７０Ｂは、一時鍵ａ及び生成元Ｇを用いて開発者等により作成された公開鍵ａＧと、一時鍵ａ、公開鍵ａＧ及び秘密鍵７５を用いて開発者等により作成された電子署名ｓと、一時鍵ａとを記憶する。そして、出力部３６は、サーバ２０を介してクライアント装置１０に公開鍵ａＧと、電子署名ｓとを出力する。したがって、記憶部７０Ｂに公開鍵ａＧを記憶する構成においては、演算装置３０は、一時鍵ａと生成元Ｇとを用いて離散対数問題が困難な有限巡回群の元として公開鍵ａＧを作成する作成部７２を備えなくてもよい。

【０１１６】
クライアント装置１０において、検証部６１は、電子署名ｓにより公開鍵ａＧの正当性が確認されたとき、ランダムな一時鍵ｂと公開鍵ａＧとを用いて共有用共通鍵６７を作成

する。また、作成部６３は、一時鍵ｂと生成元Ｇとを用いて離散対数問題が困難な有限巡回群の元として公開鍵ｂＧを作成する。そして、送信部１３は、サーバ２０を介して公開鍵ｂＧを演算装置３０に送信する。

【０１１７】

演算装置３０において、取得部３５は、クライアント装置１０から、公開鍵ｂＧを取得する。作成部７２は、前記憶部７０Ｂに記憶されている一時鍵ａと公開鍵ｂＧとを用いて共有用共通鍵７６を作成する。

【０１１８】

以上のように、一時鍵ａを演算装置３０ごとに固定し、秘密鍵７５に代えて、一時鍵ａと、電子署名ｓとを記憶部７０Ｂに記憶する構成を用いて鍵共有処理を実行することにより、外部へ秘密鍵７５が漏洩することを防止することができる。なお、第１変形例の構成に、第２変形例の構成を組み合わせて構成してもよい。すなわち、第１変形例のクライアント装置１０の鍵共有部１５に代えて、第２変形例の鍵共有部６０を適用し、第１変形例の演算装置３０の鍵共有部３３に代えて、第２変形例の鍵共有部７０を適用してもよい。

【０１１９】

なお、本発明は、上述の実施形態及び変形例に限定されるものではなく、本発明の趣旨を逸脱しない範囲で、適宜変形して実施することが可能である。

【０１２０】

例えば、上記実施形態では、クライアント装置１０が演算装置３０から共有用公開鍵３３２を取得するようにしていたが、予め共有用公開鍵３３２を取得してクライアント装置１０に格納している場合には、ステップＳ１０１～Ｓ１０４の処理を実行しなくてもよい。

【０１２１】

また、クライアント装置１０と演算装置３０との間の秘密鍵１４３及び公開鍵１４４の共有方法は、上記に限られず、別のアルゴリズム、例えば、ＤＨ－ＥＫＥ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ　Ｅｎｃｒｙｐｔｅｄ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）を用いてもよい。

【０１２２】

また、上記実施形態又は変形例において、推論処理制御部２２は、暗号化されたデータのままで演算できる処理レイヤーについて、サーバ２０と演算装置３０（３０Ａ）とのいずれに実行させるかを設定に従って決めるようにしていた。本発明はこれに限られず、例えば、サーバ２０の処理負荷や、演算装置３０（３０Ａ）の処理負荷の少なくとも一方を検出し、この処理負荷に基づいて、サーバ２０と演算装置３０（３０Ａ）とのいずれに処理レイヤーを実行させるかを決定するようにしてもよい。例えば、推論処理制御部２２は、サーバ２０の処理負荷が所定以上の場合に、暗号化されたデータのままで演算できる処理レイヤーについて、演算装置３０（３０Ａ）に実行させてもよい。また、推論処理制御部２２は、演算装置３０（３０Ａ）の処理負荷が所定以上である場合に、暗号化されたデータのままで演算できる処理レイヤーについて、サーバ２０で実行させてもよい。これにより、サーバ２０や、演算装置３０（３０Ａ）の処理負荷を抑制することができる。

【０１２３】

また、上記実施形態又は変形例において、演算装置３０（３０Ａ）の演算実行部３２（３８）に、簡易な演算式を実行可能なマイクロプロセッサを備えてもよい。この場合には、推論処理制御部２２は、演算装置３０（３０Ａ）に実行させる演算式を送信し、簡易な演算式を実行可能なマイクロプロセッサに演算式に対応する処理を実行させてもよい。このようにすると、演算装置３０（３０Ａ）において、回路として構成していなかった演算についても処理することができるようになる。

【０１２４】

また、演算システム２で実行する処理に対応するニューラルネットワークモデルの構成は、上記した例に限られず、より多くの処理レイヤーを有してもよく、上記した例と異なる処理を実行する処理レイヤーを含んでいてもよい。

【０１２５】

また、上記実施形態及び変形例では、演算システム２においてニューラルネットワークモデルに対応する処理を実行する例を示していたが、本発明はこれに限られず、例えば、ニューラルネットワークモデルに対応していない処理を実行するようにしてもよい。

【０１２６】

また、上記実施形態及び変形例においては、準同型暗号として、加法準同型暗号を例にしていたが、本発明はこれに限られず、乗法準同型暗号や、完全準同型暗号や、Ｓｏｍｅ Ｗｈａｔ準同型暗号としてもよい。

【０１２７】

また、上記実施形態及び変形例においては、準同型暗号により暗号化したデータを対象に処理を行う例を示していたが、他の暗号方式により暗号化されたデータを対象に処理を行うようにしてもよい。

【０１２８】

また、上記実施形態及び変形例においては、推論処理を実行する例を示していたが、これに限られず、本発明は、推論処理とは異なる処理を実行する場合にも適用することができる。

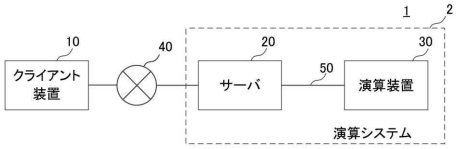
【符号の説明】

【０１２９】

１…計算機システム、２…演算システム、１０…クライアント装置、２０…サーバ、３０，３０Ａ…演算装置、３１，３７…復号部、３２，３８…演算実行部、３３、４０、５０…鍵共有部、３４…暗号化部

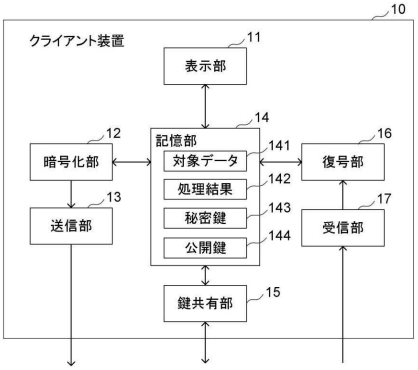
【図１】

図1



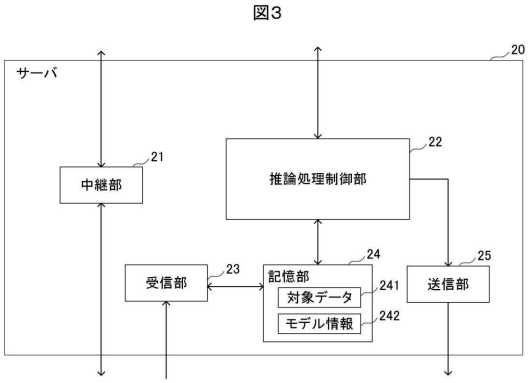
【図２】

図2



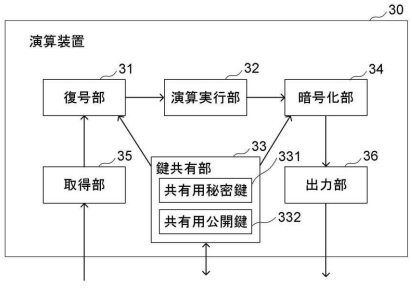
【図３】

図3



【図４】

図4



【図５】

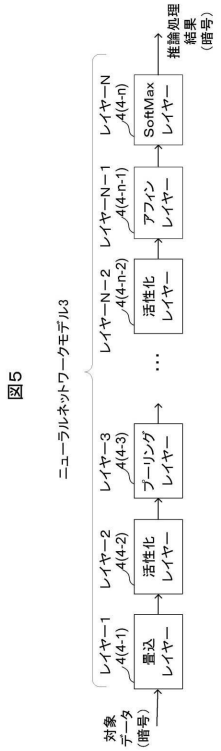


図5
ニューラルネットワークモデル3
推論処理結果（暗号）
SoftMaxレイヤー
アフィンレイヤー
活性化レイヤー
畳込レイヤー
プーリングレイヤー
活性化レイヤー
畳込レイヤー
レイヤーN
4(4-n)
レイヤーN−1
4(4-n-1)
レイヤーN−2
4(4-n-2)
レイヤー3
4(4-3)
レイヤー2
4(4-2)
レイヤー1
4(4-1)
対象データ（暗号）

【図６】

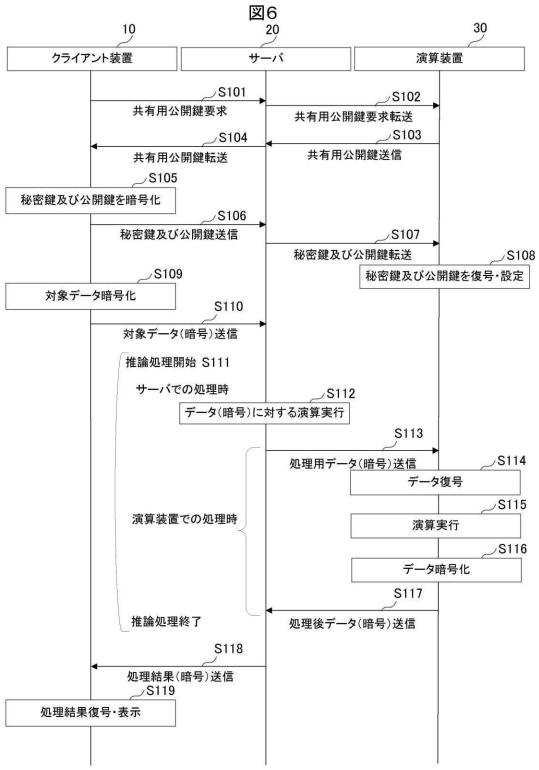


図6
10
クライアント装置
20
サーバ
30
演算装置
S101
共有用公開鍵要求
S102
共有用公開鍵要求転送
S103
共有用公開鍵送信
S104
共有用公開鍵転送
S105
秘密鍵及び公開鍵を暗号化
S106
秘密鍵及び公開鍵送信
S107
秘密鍵及び公開鍵転送
S108
秘密鍵及び公開鍵を復号・設定
S109
対象データ暗号化
S110
対象データ（暗号）送信
推論処理開始 S111
サーバでの処理時
S112
データ（暗号）に対する演算実行
S113
処理用データ（暗号）送信
S114
データ復号
演算装置での処理時
S115
演算実行
S116
データ暗号化
S117
処理後データ（暗号）送信
推論処理終了
S118
処理結果（暗号）送信
S119
処理結果復号・表示

【図７】

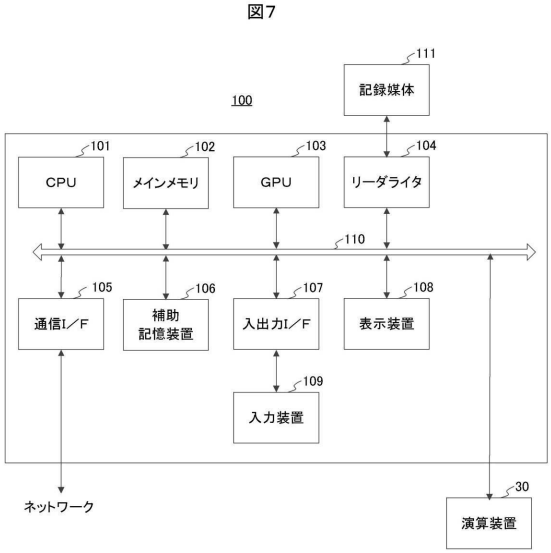


図7
100
111
記録媒体
101
CPU
102
メインメモリ
103
GPU
104
リーダライタ
110
105
通信I／F
106
補助記憶装置
107
入出力I／F
108
表示装置
109
入力装置
ネットワーク
30
演算装置

【図８】

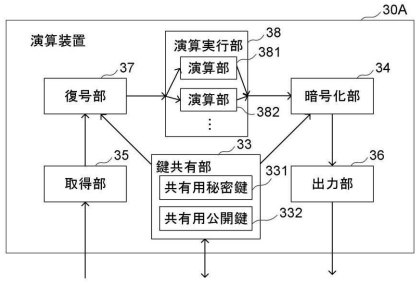


図8
30A
演算装置
演算実行部
38
演算部
381
演算部
382
37
復号部
34
暗号化部
33
鍵共有部
共有用秘密鍵
331
共有用公開鍵
332
35
取得部
36
出力部

【図９】

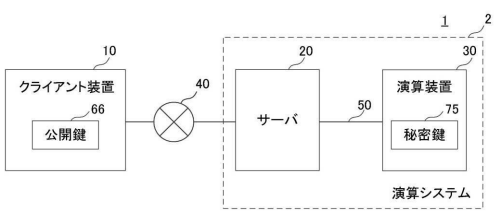
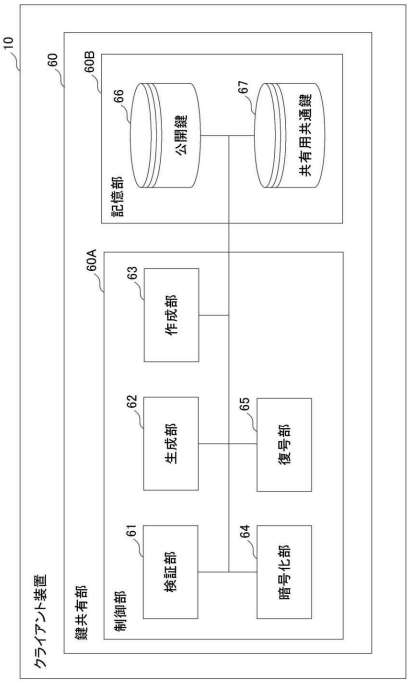


図9
1
2
10
クライアント装置
66
公開鍵
40
20
サーバ
50
30
演算装置
75
秘密鍵
演算システム

【図１０】

図10



【図１１】

図11