【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】令和3年9月30日(2021.9.30)

【公表番号】特表2020-532771(P2020-532771A)
【公表日】令和2年11月12日(2020.11.12)
【年通号数】公開・登録公報2020-046
【出願番号】特願2020-534803(P2020-534803)
【国際特許分類】
*Ｇ０９Ｃ　1/00　(2006.01)*
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｚ

【手続補正書】
【提出日】令和3年8月18日(2021.8.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
個々のパーティによって与えられた入力データのプライバシを保護しながら、セキュアマルチパーティ計算を行って、結果を出すための方法であって、前記方法が、
ディーラコンピューティングシステムが、複数の関連数字マスキングデータ成分セットを作り出すことであって、関連数字マスキングデータ成分セットごとに、前記セットの各成分が、スカラ、ベクトル、および行列のうちの１つである、作り出すことと、
前記ディーラコンピューティングシステムが、複数のパーティコンピューティングシステム間で、前記複数の関連数字マスキングデータ成分セットの各セットの各成分を秘密分散させることと、
前記複数のパーティコンピューティングシステムのパーティコンピューティングシステムごとに、前記パーティコンピューティングシステムが、
前記ディーラコンピューティングシステムから、前記複数の数字マスキングデータ成分セットの各セットの各成分のそれぞれの秘密シェアを受信し、少なくとも１つの入力データセットに対し、前記入力データセットの秘密シェアを受信することと、
前記パーティコンピューティングシステムに、１つ以上のマルチパーティ計算を行わせて、計算済み秘密分散型データの１つ以上のインスタンスを作り出させる、プログラム命令セットを実行することであって、インスタンスごとに、各パーティコンピューティングシステムが、入力データセットの少なくとも１つの秘密シェアか、または計算済み秘密分散型データの別のインスタンスの少なくとも１つの秘密シェアに基づき、前記インスタンスの秘密シェアを計算し、数字マスキングデータ成分の受信した秘密シェアが、前記計算中に伝えられたデータをマスクするのに使用され、前記計算が、
（ａ）複数の確定済みフーリエ級数から、前記入力データセットか、または計算済み秘密分散型データの前記別のインスタンスに基づき、選択されたフーリエ級数を使用して連続関数の値を近似することであって、前記複数の確定済みフーリエ級数の各々が、前記連続関数の定義域の対応する部分区間に対して前記連続関数を近似するように構成されている、近似すること、
（ｂ）計算され、浮動小数点表示で格納された秘密分散型データのインスタンスを、計算済み秘密分散型データの同等な、同等に正確で、かつ同等にセキュアなインスタンスに変換する秘密シェア縮小であって、前記変換は、少なくとも、

前記複数のパーティコンピューティングシステムの各パーティコンピューティングシステムが、
所定の切り捨て位置を越える秘密シェアの最上位桁集合を選択し、
前記切り捨て位置までに、前記秘密シェアの最下位桁集合を保持し、
前記複数のパーティコンピューティングシステムにわたって、選択した最上位桁集合で表される値の和を確定し、かつ
前記複数のパーティコンピューティングシステムの前記秘密シェアの保持した最下位桁集合にわたって、確定した和を分配することによって、行われる、秘密シェア縮小、および
（ｃ）前記入力データセットか、または計算済み秘密分散型データの前記別のインスタンスに対して、フーリエ級数評価の秘密シェアを確定することであって、少なくとも、
前記入力データセット、または計算済み秘密分散型データの前記別のインスタンスの秘密シェアを、数字マスキングデータ成分の前記秘密シェアでマスクし、
マスク済み秘密シェアに相当する値を確定して、明かし、
前記マスク済み秘密シェアに相当する確定値に基づき、フーリエ級数基底評価の値を計算し、かつ
前記フーリエ級数基底関数の計算値、および数字マスキングデータ成分の前記秘密シェアに基づき、前記フーリエ級数評価の前記秘密シェアを計算すること、によって行われる、確定することと、のうちの少なくとも１つを含む、実行することと、
前記複数のパーティコンピューティングシステムのパーティコンピューティングシステムごとに、前記パーティコンピューティングシステムが、前記複数のパーティコンピューティングシステムのうちの１つ以上の他のシステムに、計算済み秘密分散型データのインスタンスの秘密シェアを送信することと、
前記複数のパーティコンピューティングシステムの少なくとも１つのパーティコンピューティングシステムでは、前記パーティコンピューティングシステムが、
前記複数のパーティコンピューティングシステムのうちの１つ以上の他のシステムから、計算済み秘密分散型データのインスタンスの１つ以上の秘密シェアを受信し、かつ
計算済み秘密分散型データの前記インスタンスの前記受信した秘密シェアを結合して、前記結果を出すことと、を含む、方法。
【請求項２】
前記計算が、（ａ）および（ｂ）を含む、請求項１に記載の方法。
【請求項３】
前記計算が、（ａ）を含む、請求項１に記載の方法。
【請求項４】
前記連続関数の定義域の一部分を複数の部分区間に分割することと、
前記複数の部分区間の部分区間ごとに、
前記部分区間において前記関数のフーリエ級数近似値を確定することと、をさらに含む、請求項３に記載の方法。
【請求項５】
前記マルチパーティ計算が、ガーブル化回路および紛失選択のうちの少なくとも１つを使用して、対応する部分区間を選択することをさらに含む、請求項３に記載の方法。
【請求項６】
前記近似値が、前記連続関数の一様近似値である、請求項３に記載の方法。
【請求項７】
前記連続関数が、機械学習活性化関数である、請求項３に記載の方法。
【請求項８】
前記機械学習活性化関数が、シグモイド関数である、請求項７に記載の方法。
【請求項９】
前記機械学習活性化関数が、双曲線正接関数である、請求項７に記載の方法。
【請求項１０】

前記機械学習活性化関数が、ニューラルネットワーク向けの整流器活性化関数である、請求項７に記載の方法。
【請求項１１】
前記連続関数が、前記シグモイド関数である、請求項３に記載の方法。
【請求項１２】
前記計算が、（ｂ）を含む、請求項１に記載の方法。
【請求項１３】
前記複数のパーティコンピューティングシステムにわたって前記選択した最上位桁集合に相当する値の和を確定することが、
前記和がゼロになる数字マスキングデータ成分セットを確定することと、
前記パーティコンピューティングシステムの各々に、確定済みセットの１つの項を分配することと、
各パーティコンピューティングシステムが、前記確定済みセットのそれぞれの項を受信することと、
各パーティコンピューティングシステムが、受信した項を、その秘密シェアのその選択した最上位桁集合に加え、マスク済み最上位桁集合を得ることと、
前記マスク済み最上位集合を合計することと、を含む、請求項１２に記載の方法。
【請求項１４】
前記結果が、ロジスティック回帰分類モデルの係数集合である、請求項１に記載の方法。
【請求項１５】
前記方法が、ロジスティック回帰分類器を実装し、前記結果が、前記入力データに基づく前記ロジスティック回帰分類器の予測である、請求項１に記載の方法。
【請求項１６】
前記ディーラコンピューティングシステムが、信頼できるディーラコンピューティングシステムであり、前記パーティコンピューティングシステム間の通信が、前記信頼できるディーラコンピューティングシステムにはアクセス不能である、請求項１に記載の方法。
【請求項１７】
前記ディーラコンピューティングシステムが、ｈｏｎｅｓｔ－ｂｕｔ－ｃｕｒｉｏｕｓディーラコンピューティングシステムであり、前記パーティコンピューティングシステム間の通信が前記ｈｏｎｅｓｔ－ｂｕｔ－ｃｕｒｉｏｕｓディーラコンピューティングシステムによってアクセスされ得るか否かに関わらず、前記パーティコンピューティングシステムのうちの１つ以上によって与えられた秘密分散型入力データのプライバシが保護される、請求項１に記載の方法。
【請求項１８】
少なくとも１つの入力データセットに対し、前記入力データセットにおいて統計解析を行って、入力データセット統計値を確定することと、
前記入力データセット統計値を使用して、ソースコード命令セットの事前実行を行い、１つ以上の変数型の各々に対して統計的型パラメータを生成することと、
統計的型パラメータ集合に基づいて、前記ソースコード命令セットをコンパイルして、前記プログラム命令セットを生成することと、をさらに含む、請求項１に記載の方法。
【請求項１９】
前記事前実行が、
反復回数が確定可能である前記ソースコード命令セットにおいてｌｏｏｐを公開することと、
前記ソースコード命令セットにおいて関数呼び出しを公開することと、に続いて行われる、請求項１８に記載の方法。
【請求項２０】
少なくとも１つの関連数字マスキングデータ成分セットが、３つの成分から成り、前記３つの成分が、前記成分のうちの１つが前記成分のうちの残りの２つの乗算積に等しいと

いう関係性を有する、請求項１に記載の方法。
【請求項２１】
少なくとも１つの関連数字マスキングデータ成分セットが、数字と、前記数字に対して評価されたフーリエ基底関数の１つ以上の対応値集合と、を含む、請求項１に記載の方法。
【請求項２２】
前記計算が、（ｃ）を含む、請求項１に記載の方法。
【請求項２３】
前記フーリエ級数評価の前記秘密シェアを前記計算することが、式に基づき行われ、

$$[\![e^{imx}]\!]_+ = e^{im(x\oplus\lambda)}\cdot[\![e^{im(-\lambda)}]\!]_+$$

式中、ｘは、前記入力データセット、または計算済み秘密分散型データの前記別のインスタンスを表し、λは前記マスキングデータを表し、ｍは整数を表し、記号

$$[\![n]\!]_+$$

は、個数ｎの加法的秘密シェアを示し、前記記号

$$\oplus$$

は、２πを法とする加法を示す、請求項２２に記載の方法。
【請求項２４】
前記計算が、（ａ）（ｂ）、および（ｃ）を含む、請求項１に記載の方法。
【請求項２５】
前記計算が、（ａ）および（ｃ）を含む、請求項１に記載の方法。
【請求項２６】
前記結果が、前記結果の平文計算に関して所定の精度を有する、請求項１～２５のいずれか一項に記載の方法。
【請求項２７】
前記複数のパーティコンピューティングシステムのうちの少なくとも１つが、前記複数のパーティコンピューティングシステム間で、それぞれの入力データセットを秘密分散させることをさらに含む、請求項１～２５のいずれか一項に記載の方法。
【請求項２８】
複数のコンピューティングシステムを備えるシステムであって、前記複数のコンピューティングシステムが、請求項１～２５のいずれか一項に記載の方法を行うように構成されている、システム。
【請求項２９】
請求項１～２５のいずれか一項に記載のプログラム命令セットで符号化された非一時的コンピュータ可読媒体。
【請求項３０】
複数のコンピュータシステムによって実行されると、前記複数のコンピュータシステムに、請求項１～２５のいずれか一項に記載の方法を行わせる、コンピュータコードで符号化された非一時的コンピュータ可読媒体。