【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７部門第３区分
【発行日】平成26年9月4日(2014.9.4)

【公開番号】特開2012-70380(P2012-70380A)
【公開日】平成24年4月5日(2012.4.5)
【年通号数】公開・登録公報2012-014
【出願番号】特願2011-206944(P2011-206944)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｃ
Ｇ０９Ｃ　1/00　６５０Ｚ

【手続補正書】
【提出日】平成26年7月16日(2014.7.16)
【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】
第１のベクトルおよび第２のベクトルに関数を適用した結果を求めるための方法であって、該関数は、正規化和型関数であり、前記第１のベクトルは、第１のプロセッサにおいて格納され、前記第２のベクトルは、第２のプロセッサにおいて格納され、該方法は、
セキュアなマルチパーティー計算（ＳＭＰＣ）を用いて前記第１のベクトルおよび前記第２のベクトルの経験的同時確率分布（ＪＥＰＤ）を求めるステップと、
前記関数の前記結果を、前記ＪＥＰＤの値と該関数の対応する値との積の正規化された総和として求めるステップと
を含み、該方法の前記２つのステップは、少なくとも前記第１のプロセッサおよび前記第２のプロセッサによって実行される、方法。
【請求項２】
前記第１のベクトルおよび前記第２のベクトルの受信に応じて難読化されたＪＥＰＤを求めるステップであって、前記第１のベクトルおよび前記第２のベクトルは、それぞれ第１の難読化規則および第２の難読化規則に基づいて可逆的に難読化される、求めるステップと、
前記難読化されたＪＥＰＤを第１の加法シェアおよび第２の加法シェアに分割するステップと、
前記第１の加法シェアを前記第１のプロセッサに送信し、前記第２の加法シェアを前記第２のプロセッサに送信するステップであって、前記第１のプロセッサが前記第１の難読化規則および前記第２の難読化規則に基づいて前記第１の加法シェアを逆にして前記関数の前記結果の第１の加法シェアを求め、前記第２のプロセッサが前記第１の難読化規則および前記第２の難読化規則に基づいて前記第２の加法シェアを逆にして前記関数の前記結果の第２の加法シェアを求めるようにする、送信するステップと、
それぞれ前記第１のプロセッサおよび前記第２のプロセッサから受信した前記関数の前記結果の前記第１の加法シェアおよび前記第２の加法シェアに基づいて前記関数の前記結果を求めるステップと
をさらに含む、請求項１に記載の方法。

【請求項３】
前記難読化されたＪＥＰＤに対応する１組のインジケーター行列を求めるステップであって、各該インジケーター行列が前記第１の加法シェアおよび前記第２の加法シェアに分割されるようにする、求めるステップ
をさらに含む、請求項２に記載の方法。
【請求項４】
前記関数は、前記第１のベクトルおよび前記第２のベクトルの値の対応する対の該関数のとり得る結果としてメモリ内に明示的に格納される、請求項１に記載の方法。
【請求項５】
前記第１のベクトルおよび前記第２のベクトルは、各該ベクトルから要素をランダムに選択することによってサブサンプリングされる、請求項１に記載の方法。
【請求項６】
前記ＪＥＰＤは部分ＪＥＰＤである、請求項５に記載の方法。
【請求項７】
前記ＳＭＰＣは、計算機密性に基づくプロトコル、無条件機密性に基づくプロトコル、およびそれらの組み合わせからなるグループから選択されたプロトコルである、請求項１に記載の方法。
【請求項８】
前記ＳＭＰＣは、前記第１のベクトルおよび前記第２のベクトルの難読化に対して前記ＪＥＰＤが不変であることに基づいている、請求項１に記載の方法。
【請求項９】
前記第１のベクトルおよび前記第２のベクトルは、それぞれ第１のパッドベクトルおよび第２のパッドベクトルに基づいて、前記第１のベクトルおよび前記第２のベクトルからの要素を、それぞれ前記第１のパッドベクトルおよび前記第２のパッドベクトルの対応する要素と結合することによって可逆的に難読化され、前記第１のベクトルおよび前記第２のベクトルのそれぞれのアルファベットは、有限加法群として扱われる、請求項８に記載の方法。
【請求項１０】
前記アルファベットは、バイナリである、請求項９に記載の方法。
【請求項１１】
可逆的に難読化された形式で前記第１のベクトルおよび前記第２のベクトルを受信するステップと、
前記第１のベクトルおよび前記第２のベクトルの要素の対応する対毎に、難読化されたＪＥＰＤを表す１組のインジケーター行列を求めるステップと、
前記１組のインジケーター行列を第１の加法シェアおよび第２の加法シェアに分割するステップと、
前記第１の加法シェアを前記第１のプロセッサに送信し、前記第２の加法シェアを前記第２のプロセッサに送信するステップであって、前記第１のプロセッサが前記第１の難読化規則および前記第２の難読化規則に基づいて前記第１の加法シェアを逆にして前記関数の前記結果の第１の加法シェアを求め、前記第２のプロセッサが前記第１の難読化規則および前記第２の難読化規則に基づいて前記第２の加法シェアを逆にして前記関数の前記結果の第２の加法シェアを求めるようにする、送信するステップと、
それぞれ前記第１のプロセッサおよび前記第２のプロセッサから受信した前記関数の前記結果の前記第１の加法シェアおよび前記第２の加法シェアに基づいて前記関数の前記結果を求めるステップと
をさらに含む、請求項１に記載の方法。
【請求項１２】
第３のプロセッサを用いて第１のベクトルおよび第２のベクトルに関数を適用した結果をセキュアに求めるためのシステムであって、該関数は、正規化和型関数であり、前記第１のベクトルは、第１のプロセッサのみにおいて格納され、前記第２のベクトルは、第２

のプロセッサのみにおいて格納され、該システムは、
セキュアなマルチパーティー計算（ＳＭＰＣ）を用いて前記第１のベクトルおよび前記第２のベクトルの経験的同時確率分布（ＪＥＰＤ）を求める手段と、
前記関数を、前記ＪＥＰＤの値と該関数の対応する値との積の正規化された総和として求める手段と
を備え、前記方法の前記ステップは少なくとも前記第１のプロセッサおよび前記第２のプロセッサによって実行される、システム。
【請求項１３】
可逆的に難読化された形式で前記第１のベクトルおよび前記第２のベクトルを受信する手段と、
前記第１のベクトルおよび前記第２のベクトルの要素の対応する対毎に、難読化されたＪＥＰＤを表す１組のインジケーター行列を求める手段と、
前記１組のインジケーター行列を第１の加法シェアおよび第２の加法シェアに分割する手段と、
前記第１の加法シェアを前記第１のプロセッサに送信し、前記第２の加法シェアを前記第２のプロセッサに送信する手段であって、前記第１のプロセッサが前記第１の難読化規則および前記第２の難読化規則に基づいて前記第１の加法シェアを逆にして前記関数の前記結果の第１の加法シェアを求め、前記第２のプロセッサが前記第１の難読化規則および前記第２の難読化規則に基づいて前記第２の加法シェアを逆にして前記関数の前記結果の第２の加法シェアを求めるようにする、送信する手段と、
それぞれ前記第１のプロセッサおよび前記第２のプロセッサから受信した前記関数の前記結果の前記第１の加法シェアおよび前記第２の加法シェアに基づいて前記関数の前記結果を求める手段と
をさらに備える、請求項１２に記載のシステム。
【請求項１４】
前記第１のベクトルおよび前記第２のベクトルの値の対応する対に関する前記関数の結果を格納するためのメモリをさらに備える、請求項１２に記載のシステム。