【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】平成28年11月17日(2016.11.17)

【公表番号】特表2016-512612(P2016-512612A)
【公表日】平成28年4月28日(2016.4.28)
【年通号数】公開・登録公報2016-026
【出願番号】特願2015-561327(P2015-561327)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｚ

【手続補正書】
【提出日】平成28年9月26日(2016.9.26)
【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】
プライバシー保護リッジ回帰を提供するための方法であって、前記方法は、
暗号サービスプロバイダにガーブル回路を要求するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化されたデータを複数のユーザから収集するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化された前記データを合計するステップであって、暗号鍵を要求しない、前記合計するステップと、
準備されたマスクを前記合計されたデータに適用するステップと、
紛失通信を用いて、前記暗号サービスプロバイダから、準備されたマスクに対応するガーブルされた入力を受け取るステップと、
前記ガーブルされた入力およびマスクされたデータを用いて前記暗号サービスプロバイダからの前記ガーブル回路を評価するステップと、
を含む、前記方法。
【請求項２】
暗号サービスプロバイダにガーブル回路を要求する前記ステップは、
前記ガーブル回路に関する入力変数の次元を提供するステップと、
前記入力変数の値の範囲を提供するステップと、
を含む、請求項１に記載の方法。
【請求項３】
コンピューティングデバイス上で実装される評価器が、前記方法を実行する、請求項１に記載の方法。
【請求項４】
前記暗号サービスプロバイダは、前記評価器が実装される前記コンピューティングデバイスからリモートなコンピューティングデバイス上で実装される、請求項３に記載の方法。
【請求項５】
複数のユーザからの前記データを暗号化するための暗号鍵を提供するステップをさらに含む、請求項１に記載の方法。
【請求項６】

複数のユーザからの前記データは、前記暗号サービスプロバイダによって提供された暗号鍵を用いてさらに暗号化される、請求項５に記載の方法。
【請求項７】
前記ガーブル回路を評価する前記ステップは、
前記合計されたデータから前記準備されたマスクを除去するステップと、
前記ガーブル回路によって具現化されたリッジ回帰式を解くステップと、
をさらに含む、請求項１に記載の方法。
【請求項８】
データを複数のユーザから収集する前記ステップは、コンピューティングデバイスによって、前記複数のユーザの各々から送信されたデータを受信するステップを含む、請求項１に記載の方法。
【請求項９】
プライバシー保護リッジ回帰のためのコンピューティングデバイスであって、前記コンピューティングデバイスは、
ユーザデータを記憶するための記憶装置と、
処理のためのデータを記憶するためのメモリと、
暗号サービスプロバイダにガーブル回路を要求し、部分的準同型暗号を用いてフォーマット化され暗号化されたデータを複数のユーザから収集し、部分的準同型暗号を用いてフォーマット化され暗号化された前記データを合計するように構成されたプロセッサーであって、前記合計は暗号鍵を必要とせず、準備されたマスクを前記合計されたデータに適用し、紛失通信を用いて、前記暗号サービスプロバイダから、準備されたマスクに対応するガーブルされた入力を受け取り、前記ガーブルされた入力およびマスクされたデータを用いて前記暗号サービスプロバイダからの前記ガーブル回路を評価するように構成された、前記プロセッサーと、
を備えた、前記コンピューティングデバイス。
【請求項１０】
ネットワークに接続するためのネットワーク接続をさらに備えた、請求項９に記載のコンピューティングデバイス。
【請求項１１】
前記暗号サービスプロバイダは、別のコンピューティングデバイス上で実装される、請求項９に記載のコンピューティングデバイス。
【請求項１２】
暗号サービスプロバイダにガーブル回路を要求することは、
前記ガーブル回路に関する入力変数の次元を提供することと、
前記入力変数の値の範囲を提供することと、
を含む、請求項９に記載のコンピューティングデバイス。
【請求項１３】
前記ガーブル回路を評価することは、
前記合計されたデータから前記準備されたマスクを除去することと、
前記ガーブル回路によって具現化されたリッジ回帰式を解くことと、
をさらに含む、請求項９に記載のコンピューティングデバイス。
【請求項１４】
複数のユーザからの前記データは、前記暗号サービスプロバイダから提供された暗号鍵を用いて暗号化され、前記コンピューティングデバイスによって前記暗号鍵を用いて暗号化される、請求項９に記載のコンピューティングデバイス。
【請求項１５】
コンピューティングデバイスに、
暗号サービスプロバイダにガーブル回路を要求するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化されたデータを複数のユーザから収集するステップと、

部分的準同型暗号を用いてフォーマット化され暗号化された前記データを合計するステップであって、暗号鍵を要求しない、前記合計するステップと、
準備されたマスクを前記合計されたデータに適用するステップと、
紛失通信を用いて、前記暗号サービスプロバイダから、準備されたマスクに対応するガーブルされた入力を受け取るステップと、
前記ガーブルされた入力およびマスクされたデータを用いて前記暗号サービスプロバイダからの前記ガーブル回路を評価するステップと、
を実行させる命令を含む、コンピュータプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０２２９
【補正方法】変更
【補正の内容】
【０２２９】
本明細書に記載されたすべての例および条件的な語句は、実施形態の原理、および当技術分野を発展させるために発明者によって提供された概念の理解において、読者を補助するための教育的な目的のためであり、このような具体的に記載された例および条件には限定されないものと解釈されるべきである。さらに、本明細書における、本発明の原理、態様、および多様な実施形態、ならびにそれらの特定の例を述べるすべての記述は、それらの構造的および機能的等価物の両方を包含することが意図される。さらにこのような等価物は、現在知られている等価物、および将来に開発される等価物、すなわち構造に拘わらず同じ機能を行うように開発される任意の要素の両方を含むものとする。
＜付記１＞
プライバシー保護リッジ回帰を提供するための方法であって、前記方法は、
暗号サービスプロバイダにガーブル回路を要求するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化されたデータを複数のユーザから収集するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化された前記データを合計するステップであって、前記合計するステップは、暗号鍵を要求しない、ステップと、
準備されたマスクを前記合計されたデータに適用するステップと、
紛失通信を用いて、前記暗号サービスプロバイダから、準備されたマスクに対応するガーブルされた入力を受け取るステップと、
前記ガーブルされた入力およびマスクされたデータを用いて前記暗号サービスプロバイダからの前記ガーブル回路を評価するステップと、
を含む、前記方法。
＜付記２＞
暗号サービスプロバイダにガーブル回路を要求する前記ステップは、
前記ガーブル回路に関する入力変数の次元を提供するステップと、
前記入力変数の値の範囲を提供するステップと、
を含む、請求項１に記載の方法。
＜付記３＞
コンピューティングデバイス上で実装される評価器が、前記方法を実行する、請求項１に記載の方法。
＜付記４＞
前記暗号サービスプロバイダは、前記評価器が実装される前記コンピューティングデバイスからリモートなコンピューティングデバイス上で実装される、請求項３に記載の方法。
＜付記５＞
複数のユーザからの前記データを暗号化するための暗号鍵を提供するステップをさらに含む、請求項１に記載の方法。

＜付記６＞
複数のユーザからの前記データは、前記暗号サービスプロバイダによって提供された暗号鍵を用いてさらに暗号化される、請求項５に記載の方法。
＜付記７＞
前記ガーブル回路を評価する前記ステップは、
前記合計されたデータから前記準備されたマスクを除去するステップと、
前記ガーブル回路によって具現化されたリッジ回帰式を解くステップと、
をさらに含む、請求項１に記載の方法。
＜付記８＞
データを複数のユーザから収集する前記ステップは、コンピューティングデバイスによって、前記複数のユーザの各々から送信されたデータを受信するステップを含む、請求項１に記載の方法。
＜付記９＞
プライバシー保護リッジ回帰のためのコンピューティングデバイスであって、前記コンピューティングデバイスは、
ユーザデータを記憶するための記憶装置と、
処理のためのデータを記憶するためのメモリと、
暗号サービスプロバイダにガーブル回路を要求し、部分的準同型暗号を用いてフォーマット化され暗号化されたデータを複数のユーザから収集し、部分的準同型暗号を用いてフォーマット化され暗号化された前記データを合計するように構成されたプロセッサーであって、前記合計は暗号鍵を必要とせず、準備されたマスクを前記合計されたデータに適用し、紛失通信を用いて、前記暗号サービスプロバイダから、準備されたマスクに対応するガーブルされた入力を受け取り、前記ガーブルされた入力およびマスクされたデータを用いて前記暗号サービスプロバイダからの前記ガーブル回路を評価するように構成された、プロセッサーと、
を備えた、前記コンピューティングデバイス。
＜付記１０＞
ネットワークに接続するためのネットワーク接続をさらに備えた、請求項９に記載のコンピューティングデバイス。
＜付記１１＞
前記暗号サービスプロバイダは、別のコンピューティングデバイス上で実装される、請求項９に記載のコンピューティングデバイス。
＜付記１２＞
暗号サービスプロバイダにガーブル回路を要求することは、
前記ガーブル回路に関する入力変数の次元を提供することと、
前記入力変数の値の範囲を提供することと、
を含む、請求項９に記載のコンピューティングデバイス。
＜付記１３＞
前記ガーブル回路を評価することは、
前記合計されたデータから前記準備されたマスクを除去することと、
前記ガーブル回路によって具現化されたリッジ回帰式を解くことと、
をさらに含む、請求項９に記載のコンピューティングデバイス。
＜付記１４＞
複数のユーザからの前記データは、前記暗号サービスプロバイダから提供された暗号鍵を用いて暗号化され、前記コンピューティングデバイスによる暗号鍵を用いて暗号化される、請求項９に記載のコンピューティングデバイス。
＜付記１５＞
実行されたとき、
暗号サービスプロバイダにガーブル回路を要求するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化されたデータを複数のユーザから

収集するステップと、
部分的準同型暗号を用いてフォーマット化され暗号化された前記データを合計するステップであって、前記合計するステップは、暗号鍵を要求しない、ステップと、
準備されたマスクを前記合計されたデータに適用するステップと、
紛失通信を用いて、前記暗号サービスプロバイダから、準備されたマスクに対応するガーブルされた入力を受け取るステップと、
前記ガーブルされた入力およびマスクされたデータを用いて前記暗号サービスプロバイダからの前記ガーブル回路を評価するステップと、
を含むステップを実行する命令を含む、機械可読媒体。