【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３区分
【発行日】平成22年10月14日(2010.10.14)

【公表番号】特表2010-503118(P2010-503118A)
【公表日】平成22年1月28日(2010.1.28)
【年通号数】公開・登録公報2010-004
【出願番号】特願2009-527488(P2009-527488)
【国際特許分類】
Ｇ０６Ｆ　17/30　　(2006.01)
Ｇ０６Ｆ　21/24　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　17/30　　１７０Ｈ
Ｇ０６Ｆ　12/14　　５４０Ａ

【手続補正書】
【提出日】平成22年8月24日(2010.8.24)
【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】
データベースシステム中の非決定論的に暗号化されたデータの検索を行う方法であって、当該方法は、記憶装置に記憶されたコンピュータ実行可能命令を処理装置が実行することによって実施され、
ユーザーによって与えられた所望の平文データ項目のためのインデックス値を決定するステップであって、
前記所望の平文データ項目および暗号鍵に基づいてＭＡＣを計算するステップと、
前記計算されたＭＡＣにハッシュ関数を用いて、前記インデックス値を決定するステップと
を含む、決定するステップと、
前記インデックス値をインデックス構造中の対応するエントリーへのアクセスに使用し、前記所望の平文データ項目に対応する非決定論的に暗号化された暗号文を含むデータベースエントリーを得るステップであって、前記インデックス構造は複数の対データ項目を含み、各対データ項目は、第１の項目と、第２の項目または前記第２の項目への参照のいずれかと、を含み、前記第１の項目は、前記暗号鍵を使用して、それぞれの平文データ項目にＨＭＡＣを適用することに基づいた値を持つインデックスデータ項目であり、前記第２の項目は、前記それぞれの平文データ項目に対応する非決定論的に暗号化された暗号文である、得るステップと、
前記複数の対データ項目中の対応する１つの対データ項目の第２の項目を復号化するステップと、
前記復号化した第２の項目と前記所望の平文データ項目とを比較して、ハッシュの衝突が生じたか否かを判断するステップと
を含むことを特徴とする方法。
【請求項２】
前記インデックス構造は、対応する平文データ項目のＨＭＡＣに従ったそれぞれの項目に対して割り当てられた複数のハッシュバケットを含むことを特徴とする請求項１に記載の方法。

【請求項３】
データベースシステム中の非決定論的に暗号化されたデータの検索を実行する遠隔データベースを提供する方法であって、当該方法は、記憶装置に記憶されたコンピュータ実行可能命令を処理装置が実行することによって実施され、
ネットワークを介して要求側から、所望の平文データ項目に対応するデータベースエントリーのための前記データベースシステム中の非決定論的に暗号化されたデータを検索する遠隔要求を受け付けるステップと、
前記所望の平文データ項目および暗号鍵に基づいてコードを計算するステップと、
前記コードをインデックス構造に対するインデックスとして使用し、前記所望の平文データ項目に対応する前記データベースエントリーを得るステップであって、前記インデックス構造は、対応するハッシュ値に従ったそれぞれの項目に対する複数のハッシュバケットを含み、前記対応するハッシュ値は、対応する平文データ項目および前記暗号鍵に基づいてＨＭＡＣを計算するステップと、前記計算されたＨＭＡＣにハッシュ関数を用いて、前記対応するハッシュ値を生成するステップとによって決定される、得るステップと、
前記コードに対応する前記インデックス構造中のエントリーの非決定論的に暗号化された項目を復号化するステップと、
前記復号化した項目と前記所望の平文データ項目とを比較して、ハッシュの衝突が生じたか否かを判断するステップと、
前記要求側に対して、前記データベースシステムから得た前記所望の平文データ項目に対応するデータベースエントリーを含む返却データを返却するステップと
を含むことを特徴とする方法。
【請求項４】
コードを計算する前記ステップは、ＨＭＡＣを計算するステップをさらに含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記インデックス構造は複数の項目をさらに含み、各項目は、少なくともデュプレットの第１の項目と、前記デュプレットの第２の項目または前記第２の項目への参照のいずれかと、を含み、前記第１の項目は、それぞれの平文データ項目に対応するコードを含み、前記第２の項目は、前記それぞれの平文データ項目に対応する非決定論的に暗号化された暗号文を含むことを特徴とする請求項３に記載の方法。
【請求項６】
前記インデックス構造はＢ-treeを含むことを特徴とする請求項３に記載の方法。
【請求項７】
データベースシステム中の非決定論的に暗号化されたデータの検索を行う方法を処理装置に実行させるためのコンピュータ実行可能命令を記録したコンピュータ読み取り可能な記録媒体であって、前記方法は、
所望の平文データ項目および暗号鍵に基づいてＭＡＣを計算するステップと、
前記計算されたＭＡＣにハッシュ関数を用いて、前記インデックス値を決定するステップと、
前記インデックス値をインデックス構造中の対応するエントリーへのアクセスに使用し、前記所望の平文データ項目に対応する非決定論的に暗号化された暗号文を含むデータベースエントリーを得るステップであって、前記インデックス構造は複数の対データ項目を含み、各対データ項目は、第１の項目と、第２の項目または前記第２の項目への参照のいずれかと、を含み、前記第１の項目は、前記暗号鍵を使用して、それぞれの平文データ項目にＨＭＡＣを適用することに基づいた値を持つインデックスデータ項目であり、前記第２の項目は、前記それぞれの平文データ項目に対応する非決定論的に暗号化された暗号文である、得るステップと、
前記インデックス値を使用して前記インデックス構造中の前記対応するエントリーの対データ項目の第２の項目を得るステップと、
前記第２の項目を復号化するステップと、

前記復号化した第２の項目と前記所望の平文データ項目とを比較して、ハッシュの衝突が生じたか否かを判断するステップと
を含むことを特徴とするコンピュータ読み取り可能な記録媒体。