【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8月26日(2021.8.26)

【公開番号】特開2019-35949(P2019-35949A)
【公開日】平成31年3月7日(2019.3.7)
【年通号数】公開・登録公報2019-009
【出願番号】特願2018-135417(P2018-135417)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ０６Ｆ　16/00　(2019.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６６０Ｄ
Ｇ０９Ｃ　1/00　６５０Ｚ
Ｇ０６Ｆ　17/30　１２０Ａ
Ｇ０６Ｆ　17/30　３４０Ｄ

【手続補正書】
【提出日】令和3年7月13日(2021.7.13)
【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】
暗号化データベースを生成する方法であって、前記方法は、
（ａ）１つ以上の列に平文データエントリを有する平文データベースを受信することと、
（ｂ）拡張された平文データベースを生成するために前記受信した平文データベースを拡張することであって、前記拡張が１つ以上の列を前記受信した平文データベースに追加することを含み、前記追加された各列が条件付きクエリのために利用可能にされるべき属性に対応する、拡張することと、
（ｃ）前記拡張された平文データベースを暗号化して、暗号化データエントリを含む前記暗号化データベースを生成することと
を備え、
前記暗号化データベースが、前記追加された列に対応するそれらの属性についての少なくとも１つの形式の条件付きクエリをサポートし、前記少なくとも１つの形式の条件付きクエリが、暗号化結果を生成するように、その復号なしで前記暗号化データエントリについて計算される、
方法。
【請求項２】
前記暗号化データが、意味的にセキュアな暗号化によって暗号化される、請求項１に記載の方法。
【請求項３】
前記暗号化データが、準同型暗号システムを使用して暗号化される、請求項２に記載の方法。
【請求項４】
前記準同型暗号システムが、相加的準同型暗号システムである、請求項３に記載の方法。

【請求項５】
前記準同型暗号システムが、２－ＤＮＦ（論理和標準形）演算をサポートする、請求項３に記載の方法。
【請求項６】
前記少なくとも１つの形式の条件付きクエリが、ＷＨＥＲＥクエリまたはＧＲＯＵＰＢＹクエリのうちの１つである、請求項１に記載の方法。
【請求項７】
暗号化データベースを管理するシステムであって、前記システムは、
ハードウエアを介して実装された抽出、転送、および書き込み（ＥＴＬ）サーバであって、前記ＥＴＬサーバは、（ｉ）１つ以上の列において暗号化されていないデータエントリを有する平文データベースを入力として受信し、（ｉｉ）拡張された平文データベースを生成するように前記受信した平文データベースを拡張し、前記拡張された平文データベースが、前記入力された平文データベースに対する１つ以上の列の追加を含み、前記追加された各列が条件付きクエリに利用可能にされるべき属性に対応し、（ｉｉｉ）暗号化データエントリを含む前記暗号化データベースを生成するように前記拡張された平文データベースを暗号化するように動作する、ＥＴＬサーバと、
ハードウエアを介して実装されたデータベース（ＤＢ）サーバであって、前記ＤＢサーバは、（ｉ）前記ＥＴＬサーバから前記暗号化データベースを受信して保持し、（ｉｉ）前記ＤＢサーバに提出されたクエリに応答して暗号化データを返すように動作する、ＤＢサーバと、
ハードウエアを介して実装された計算サーバであって、（ｉ）クエリを前記ＤＢサーバに提出し、（ｉｉ）前記ＤＢサーバから返された暗号化データに関する計算を実行するように動作する、計算サーバと
を備え、前記計算が、前記暗号化データの復号なしに前記暗号化データベースからの前記暗号化データに対して実行され、前記計算から得られた結果が暗号化され、前記暗号化データベースが、前記暗号化データの基礎となる前記暗号化されていないデータのサンプルを明らかにすることなく、少なくとも１つの形式の条件付きクエリに応答して正しい暗号化結果を得ることをサポートするように構成されている、システム。
【請求項８】
前記暗号化データが、意味的にセキュアな暗号化によって暗号化される、請求項７に記載のシステム。
【請求項９】
前記暗号化データが、準同型暗号システムを使用して暗号化される、請求項８に記載のシステム。
【請求項１０】
前記準同型暗号システムが、相加的準同型暗号システムである、請求項９に記載のシステム。