(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6640858号
(P6640858)

(45)発行日　令和2年2月5日(2020.2.5)　(24)登録日　令和2年1月7日(2020.1.7)

(51)Int.Cl.		F I		
H04L 9/14	(2006.01)	H04L	9/00	641
G06Q 20/24	(2012.01)	G06Q	20/24	
G06Q 20/38	(2012.01)	G06Q	20/38	310
G06F 16/00	(2019.01)	G06F	16/00	

請求項の数 15　(全 21 頁)

(21)出願番号　特願2017-533197(P2017-533197)
(86)(22)出願日　平成28年1月6日(2016.1.6)
(65)公表番号　特表2018-507582(P2018-507582A)
(43)公表日　平成30年3月15日(2018.3.15)
(86)国際出願番号　PCT/US2016/012389
(87)国際公開番号　WO2016/112137
(87)国際公開日　平成28年7月14日(2016.7.14)
審査請求日　平成30年6月20日(2018.6.20)
(31)優先権主張番号　201510007411.8
(32)優先日　平成27年1月7日(2015.1.7)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所

最終頁に続く

(54)【発明の名称】取引を処理するための方法及び装置

(57)【特許請求の範囲】
【請求項１】
１つまたは複数のコンピューティングデバイスによって実装される方法であって、前記方法が、
取引を処理する要求の元のカード番号を受信することと、
前記元のカード番号に対応するハッシュ値を、前記元のカード番号に基づいて計算することと、前記元のカード番号に対応するインデックスカード番号を、前記元のカード番号に対応する前記ハッシュ値に基づいて取得することであって、前記インデックスカード番号を取得することは、
データベースを検索して、前記データベースに前記ハッシュ値を有するカード番号レコードが存在するかどうかを判定することと、
前記データベースに前記ハッシュ値を有するカード番号レコードが存在しないと判定した場合、
前記元のカード番号に対応するハッシュ番号に第１の値を設定し、前記元のカード番号にインデックスカード番号を割り当てることと、
秘密鍵辞書から最新の秘密鍵及び前記最新の秘密鍵のバージョンを取得することと、
前記最新の秘密鍵を使用して前記元のカード番号を暗号化し、前記最新の秘密鍵のバージョンと前記暗号化から取得された暗号文の先頭を組み合わせて、前記元のカード番号に対応する暗号文を取得することと、
前記元のカード番号、前記割り当てられたインデックスカード番号、前記元のカード

番号に対応する前記暗号文、前記元のカード番号に対応する前記ハッシュ値、及び前記ハッシュ値に対応する前記ハッシュ番号を含む、前記元のカード番号に対応する新しいカード番号レコードを前記データベースに格納することと、を含み、

前記元のカード番号に対応する前記新しいカード番号レコードを前記データベースに格納するときに、前記ハッシュ値及び前記ハッシュ番号の制限に違反がない場合、前記インデックスカード番号は、前記元のカード番号に正常に割り当てられていると判定される、

ことと、

前記インデックスカード番号に基づいて前記取引を処理する装置に前記インデックスカード番号を送信することと

を含む、１つまたは複数のコンピューティングデバイスによって実装される方法。

【請求項２】

前記データベースに前記ハッシュ値を有する１つまたは複数のカード番号レコードが存在すると判定した場合、前記方法がさらに、

前記１つまたは複数のカード番号レコードの各カード番号レコード内のそれぞれのカード番号暗号文を取得することと、

前記それぞれのカード番号暗号文から秘密鍵バージョンを傍受することと、

前記秘密鍵バージョンに少なくとも部分的に基づいて秘密鍵辞書を読み取って、前記各カード番号暗号文を暗号化するために使用される秘密鍵を取得することと、

前記それぞれのカード番号暗号文を復号化するための秘密鍵を使用して、各カード番号レコードからそれぞれの元のカード番号を取得することと、

前記各カード番号レコードのそれぞれの元のカード番号と前記受信した元のカード番号とを比較することと

を含む、請求項１に記載の方法。

【請求項３】

前記１つまたは複数のカード番号レコードの特定のカード番号レコードの元のカード番号が、前記受信した元のカード番号と同一であると判定することと、

前記特定のカード番号レコードから前記受信した元のカード番号に対応するインデックスカード番号を取得することと

をさらに含む、請求項２に記載の方法。

【請求項４】

前記受信した元のカード番号と同一の元のカード番号を有するカード番号レコードがないと判定することと、

前記元のカード番号に対応するハッシュ番号に第２の値を設定することと、

前記元のカード番号にインデックスカード番号が割り当てられることと、

秘密鍵辞書から最新の秘密鍵及び前記最新の秘密鍵のバージョンを取得することと、

前記最新の秘密鍵を使用して前記元のカード番号を暗号化することと、

前記最新の秘密鍵の前記バージョンと前記暗号化から取得された暗号文の先頭を組み合わせて、前記元のカード番号に対応する暗号文を取得することと、

前記元のカード番号、前記割り当てられたインデックスカード番号、前記元のカード番号に対応する前記暗号文、前記元のカード番号に対応する前記ハッシュ値及び前記ハッシュ値に対応する前記ハッシュ番号を含む、前記元のカード番号に対応するカード番号レコードを前記データベースに格納することと

をさらに含み、

前記元のカード番号に対応する前記新しいカード番号レコードを前記データベースに格納するときに、前記ハッシュ値及び前記ハッシュ番号の制限に違反がない場合、前記インデックスカード番号が、前記元のカード番号に正常に割り当てられていると判定される、請求項２に記載の方法。

【請求項５】

前記データベースに格納されたカード番号レコードをトラバースすることと、

現在トラバースしているカード番号レコードからカード番号暗号文を取得することと、前記カード番号暗号文から秘密鍵バージョンを傍受することと、
前記カード番号暗号文の前記秘密鍵バージョンを秘密鍵辞書から取得した最新の秘密鍵バージョンと比較することと、
前記カード番号暗号文の前記秘密鍵バージョンが、前記最新の秘密鍵バージョンでない場合、前記秘密鍵辞書から前記カード番号暗号文の秘密鍵バージョンに対応する秘密鍵を取得することと、前記カード番号暗号文を復号化するための前記取得した秘密鍵を使用して、前記元のカード番号を取得することと、
前記秘密鍵辞書から前記最新の秘密鍵バージョンに対応する新しい秘密鍵を取得することと、前記新しい秘密鍵を使用して前記元のカード番号を暗号化することと、前記暗号化から取得された暗号文を前記最新の秘密鍵バージョンと組み合わせて、更新されたカード番号暗号文を取得することと、
前記現在トラバースされているカード番号レコード内の前記カード番号暗号文のフィールドの内容が、更新されたカード番号暗号文として更新することと
をさらに含む、請求項１に記載の方法。
【請求項６】
１つまたは複数のプロセッサーと、
メモリーと、
取引を処理することを要求するために使用される元のカード番号を受信するように、前記メモリーに記憶され、前記１つまたは複数のプロセッサーによって実行可能な受信モジュールと、
前記受信モジュールによって受信された前記元のカード番号に基づいて前記元のカード番号に対応するハッシュ値を計算するように、前記メモリーに記憶され、前記１つまたは複数のプロセッサーによって実行可能な計算モジュールと、
前記計算モジュールによって計算された前記元のカード番号に対応する前記ハッシュ値に基づいて、前記元のカード番号に対応するインデックスカード番号を取得するように、前記メモリーに記憶され、前記１つまたは複数のプロセッサーによって実行可能な取得モジュールであって、
前記ハッシュ値を有する格納されたカード番号レコードについてデータベースを検索する検索サブモジュールと、
前記ハッシュ値を有するカード番号レコードが前記データベースに存在しないと判定する判定サブモジュールと、
前記元のカード番号に対応するハッシュ番号に第１の値を設定して、前記元のカード番号にインデックスカード番号を割り当てる割り当てサブモジュールと、
秘密鍵辞書から最新の秘密鍵及び前記最新の秘密鍵のバージョンを取得し、前記最新の秘密鍵を使用して前記元のカード番号を暗号化し、前記最新の秘密鍵の前記バージョンと前記暗号化から取得した暗号文の先頭を組み合わせて、前記元のカード番号に対応する暗号文を取得する暗号化サブモジュールと、
前記元のカード番号、前記割り当てサブモジュールによって割り当てられた前記インデックスカード番号、前記暗号化サブモジュールによって取得された前記元のカード番号に対応する前記暗号文、前記元のカード番号に対応する前記ハッシュ値、及び前記ハッシュ値に対応する前記ハッシュ番号を含む、前記元のカード番号に対応する新しいカード番号レコードを前記データベースに格納する記憶サブモジュールと
を含む、取得モジュールと、
前記取引を処理する装置に、前記取得モジュールによって取得された前記インデックスカード番号を送信するように、前記１つまたは複数のプロセッサーによって実行可能な送信モジュールと
を含む、装置。
【請求項７】
前記判定サブモジュールがさらに、前記記憶サブモジュールが、前記元のカード番号に

対応する前記新しいカード番号レコードを前記データベースに格納するときに、前記ハッシュ値及び前記ハッシュ番号の制限に違反がない場合、前記インデックスカード番号が、前記元のカード番号に正常に割り当てられていると判定する、請求項６に記載の装置。

【請求項８】

前記取得モジュールがさらに、

前記検索サブモジュールによって見つけられた各カード番号レコード内のそれぞれのカード番号暗号文を取得し、前記それぞれのカード番号暗号文から秘密鍵バージョンを傍受し、前記秘密鍵のバージョンに基づいて秘密鍵辞書を読み取って、前記それぞれのカード番号暗号文を暗号化するために使用される前記秘密鍵を取得する取得サブモジュールと、

前記取得サブモジュールによって取得された前記最新の秘密鍵を使用して、前記それぞれのカード番号暗号文を復号化して、各カード番号レコードからそれぞれの元のカード番号を取得する復号化サブモジュールと、

前記復号化サブモジュールによって取得された各カード番号レコードの前記それぞれの元のカード番号と前記受信した元のカード番号を比較する比較サブモジュールと

を含む、請求項６に記載の装置。

【請求項９】

前記取得サブモジュールが、前記受信した元のカード番号と同一の対応するカード番号を有するカード番号レコードから、前記受信した元のカード番号に対応するインデックスカード番号をさらに取得する、請求項８に記載の装置。

【請求項１０】

前記取得モジュールが、設定サブモジュールをさらに含み、前記比較サブモジュールが、前記受信した元のカード番号と同一のカード番号を有するカード番号レコードが前記データベースに存在しないと判定した場合、前記設定サブモジュールが、前記元のカード番号に対応するハッシュ番号に第２の値を設定し、前記記憶サブモジュールが、前記元のカード番号、及び前記元のカード番号に対応する前記ハッシュ番号を含む、前記元のカード番号に対応する新しいカード番号レコードを前記データベースに格納する、請求項８に記載の装置。

【請求項１１】

前記取得モジュールが、

データベースに格納されたカード番号レコードをトラバースするトラバースサブモジュールと、

現在トラバースしているカード番号レコードからそれぞれのカード番号暗号文を取得し、前記それぞれのカード番号暗号文から秘密鍵バージョンを傍受する取得サブモジュールと、

前記取得サブモジュールによって取得された前記秘密鍵バージョンを、秘密鍵辞書から取得された最新の秘密鍵バージョンと比較する比較サブモジュールと

を含む、請求項６に記載の装置。

【請求項１２】

前記取得サブモジュールによって取得された前記秘密鍵バージョンが前記最新の秘密鍵バージョンではないと前記比較サブモジュールが判定した場合に、前記復号化サブモジュールが、前記元のカード番号を取得した後、前記取得サブモジュールがさらに、前記秘密鍵辞書から前記カード番号暗号文の前記秘密鍵バージョンに対応する秘密鍵を取得し、前記秘密鍵辞書から前記最新の秘密鍵バージョンに対応する新しい秘密鍵を取得する、請求項１１に記載の装置。

【請求項１３】

前記取得モジュールがさらに、

前記取得サブモジュールによって取得された前記新しい秘密鍵を使用して、前記カード番号暗号文を復号化し、前記元のカード番号を取得する復号化サブモジュールと、

前記取得サブモジュールによって取得された前記新しい秘密鍵を使用して、前記復号化サブモジュールによって取得された前記元のカード番号を暗号化し、前記暗号化により取

得された暗号文を前記最新の秘密鍵バージョンと組み合わせて、更新されたカード番号暗号文を取得する暗号化サブモジュールと、
前記現在トラバースされているカード番号レコード内の前記カード番号暗号文のフィールドの内容を、前記暗号化サブモジュールによって取得された前記更新されたカード番号暗号文として更新する更新サブモジュールと
を含む、請求項１２に記載の装置。
【請求項１４】
実行可能命令を格納する１つまたは複数のコンピューター可読媒体であって、前記実行可能命令は、１つまたは複数のプロセッサーによって実行されると、前記１つまたは複数のプロセッサーに、
取引を処理する要求の元のカード番号を受信することと、
前記元のカード番号に対応するハッシュ値を、前記元のカード番号に基づいて計算することと、前記元のカード番号に対応するインデックスカード番号を、前記元のカード番号に対応する前記ハッシュ値に基づいて取得することであって、前記インデックスカード番号を取得することは、
データベースを検索して、前記データベースに前記ハッシュ値を有するカード番号レコードが存在するかどうかを判定することと、
前記データベースに前記ハッシュ値を有するカード番号レコードが存在しないと判定した場合、
前記元のカード番号に対応するハッシュ番号に第１の値を設定し、前記元のカード番号にインデックスカード番号を割り当てることと、
秘密鍵辞書から最新の秘密鍵及び前記最新の秘密鍵のバージョンを取得することと、
前記最新の秘密鍵を使用して前記元のカード番号を暗号化し、前記最新の秘密鍵のバージョンと前記暗号化から取得された暗号文の先頭を組み合わせて、前記元のカード番号に対応する暗号文を取得することと、
前記元のカード番号、前記割り当てられたインデックスカード番号、前記元のカード番号に対応する前記暗号文、前記元のカード番号に対応する前記ハッシュ値、及び前記ハッシュ値に対応する前記ハッシュ番号を含む、前記元のカード番号に対応する新しいカード番号レコードを前記データベースに格納することと、を含み、
前記元のカード番号に対応する前記新しいカード番号レコードを前記データベースに格納するときに、前記ハッシュ値及び前記ハッシュ番号の制限に違反がない場合、前記インデックスカード番号は、前記元のカード番号に正常に割り当てられていると判定される、
ことと、
前記インデックスカード番号に基づいて前記取引を処理する装置に前記インデックスカード番号を送信することと
を含む動作を実行させる、１つまたは複数のコンピューター可読媒体。
【請求項１５】
前記データベースに前記ハッシュ値を有する１つまたは複数のカード番号レコードが存在すると判定した場合、前記動作がさらに、
前記１つまたは複数のカード番号レコードの各カード番号レコード内のそれぞれのカード番号暗号文を取得することと、
前記それぞれのカード番号暗号文から秘密鍵バージョンを傍受することと、
前記秘密鍵バージョンに少なくとも部分的に基づいて秘密鍵辞書を読み取って、前記それぞれのカード番号暗号文を暗号化するために使用される秘密鍵を取得することと、
前記それぞれのカード番号暗号文を復号化するための秘密鍵を使用して、各カード番号レコードからそれぞれの元のカード番号を取得することと、
前記各カード番号レコードの前記それぞれの元のカード番号と前記受信した元のカード番号とを比較することと
を含む、請求項１４に記載の１つまたは複数のコンピューター可読媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
関連特許出願の相互参照
本出願は、２０１５年1月7日に出願された「Ｍｅｔｈｏｄ ａｎｄ Ａｐｐａｒａｔｕｓ ｆｏｒ Ｐｒｏｃｅｓｓｉｎｇ Ｔｒａｎｓａｃｔｉｏｎｓ」と題する中国特許出願第２０１５１０００７４１１．８号の外国優先権を主張するものであり、その全体が本明細書に援用される。
【０００２】
本開示は、インターネット技術の分野に関し、より詳細には、取引を処理するための方法及び装置に関する。
【背景技術】
【０００３】
クレジットカード決済をサポートする決済システムでは、ユーザーのクレジットカード情報、特にクレジットカード番号の受信、転送、及び保存の操作に厳しいセキュリティ要件がある。国際慣行によれば、クレジットカード番号などの元の情報を処理する決済システムは、少なくともクレジット化カード業界（以下、ＰＣＩという）の認証に合格する必要がある。
【０００４】
ＰＣＩ認証では、一般的な解決策は、実際の各クレジットカード番号に仮想インデックスカード番号を割り当てることである。クレジットカード情報を処理する過程で、クレジットカードの元のカード番号は、転送及び記憶のためのそのようなインデックスカード番号に置き換えられる。クレジットカードの元のカード番号を使用する必要がある場合のみ、対応する元のカード番号が使用される。これは、クレジットカードの元のカード番号が、最低限のレベルで使用され、統一された方法で制御及び管理できることを保証するためである。
【０００５】
しかし、既存の技術では、実際のクレジットカード番号に仮想インデックスカード番号を割り当てる処理には以下の問題がある。
【０００６】
１．複数のユーザーが同一または異なるクレジットカードを使用して同時に支払いを行う場合、インデックスカード番号の作成に関する同時実行の問題があり、同時実行の場合、２つの異なるインデックスカード番号が、同じクレジットカードに割り当てられることが避けられない。
【０００７】
２．ＰＣＩの要件によれば、クレジットカードの元のカード番号は、平文で保存することができず、暗号化する必要がある。しかし、アルゴリズム及び秘密鍵のセキュリティ制約のため、クレジットカードの元のカード番号の暗号文及び暗号化の秘密鍵を頻繁に変更する必要がある。クレジットカードの元のカード番号を暗号化する既存の方法では、クレジットカード番号の暗号文と秘密鍵を柔軟に変更することができず、混乱を生じやすくなる場合がある。
【０００８】
３．ビジネス取引要件によれば、システムは、クレジットカードの元のカード番号に基づいて、暗号化されたクレジットカード番号と対応するインデックスカード番号を迅速に検索する必要がある。しかし、既存の技術では、暗号化されたクレジットカード番号と対応するインデックスカード番号を検索する効率はかなり低い。
【０００９】
この概要は、以下の詳細な説明でさらに説明される概念の選択を簡略化された形で紹介するために提供される。この概要は、特許請求される主題のすべての重要な特徴または不可欠な特徴を特定することを意図しておらず、特許請求される主題の範囲を判定するため

の支援として単独で使用されることも意図していない。例えば、用語「ｔｅｃｈｎｉｑｕｅｓ（技法）」は、上記及び本開示全体を通じて文脈により許可された、デバイス（複数可）、システム（複数可）、方法（複数可）及び／またはコンピューター可読命令を指し得る。

【００１０】

本開示の目的は、既存の技術における、上記の技術的問題の１つまたは複数を解決することである。

【００１１】

したがって、本開示の第１の目的は、取引を処理するための方法を提供することである。本方法は、システム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行う。

【００１２】

本開示の第２の目的は、取引を処理するための装置を提供することである。

【００１３】

実施形態を実施するために、第１の態様における本開示の実施形態による取引を処理する方法は、取引の処理を要求するための元のカード番号を受信することと、元のカード番号に基づいて元のカード番号に対応するハッシュ値を計算することと、元のカード番号に対応するハッシュ値に基づいて、元のカード番号に対応するインデックスカード番号を取得することと、エンティティが、インデックスカード番号に基づいて取引を処理するために、取引を処理するエンティティにインデックスカード番号を送信することとを含む。

【００１４】

本開示の実施形態による開示された方法では、取引の処理を要求するための元のカード番号を受信した後、元のカード番号に基づいて元のカード番号に対応するハッシュ値を計算し、元のカード番号に対応するハッシュ値に基づいて元のカード番号に対応するインデックスカード番号を取得し、それによって、システム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行う。

【００１５】

実施形態を実施するために、第２の態様の本開示の実施形態による装置は、取引の処理を要求するための元のカード番号を受信する受信モジュールと、受信モジュールによって受信された元のカード番号に基づいて、元のカード番号に対応するハッシュ値を計算する計算モジュールと、計算モジュールにより計算された元のカード番号に対応するハッシュ値に基づいて、元のカード番号に対応するインデックスカード番号を取得する取得モジュールと、エンティティがインデックスカード番号に基づいて取引を処理できるように、取引を処理するエンティティに取得モジュールによって取得されたインデックスカード番号を送信するための送信モジュールとを含む。

【００１６】

本開示の実施形態によるサービス処理装置では、受信モジュールが取引の処理を要求するための元のカード番号を受信した後、計算モジュールが、元のカード番号に基づいて元のカード番号に対応するハッシュ値を計算し、取得モジュールが、元のカード番号に対応するハッシュ値に基づいて、元のカード番号に対応するインデックスカード番号を取得し、それによって、関連するシステム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行う。

【００１７】

本開示のその他の特徴及び利点は、以下の説明に記載され、一部は説明から明らかにな

るか、または応用例の実施によって理解されるであろう。本出願の目的及びその他の利点は、記述された明細書、特許請求の範囲、ならびに実現及び達成が具体的に指摘されている構造の図面によって取得することができる。

【図面の簡単な説明】

【００１８】

本開示の実施形態をより良く説明するために、以下は、実施形態の説明に使用される図の簡単な紹介である。以下の図は、本開示のいくつかの実施形態にのみ関係することは明らかである。当業者は、創造的な努力なしに、本開示の図に従って他の図を得ることができる。

【００１９】

【図１】本開示の一実施形態による取引を処理するための方法の流れ図である。

【図２】本開示の別の実施形態による取引を処理するための方法の流れ図である。

【図３】本開示のさらに別の実施形態による取引を処理するための方法の流れ図である。

【図４】本発明の一実施形態による暗号文及び秘密鍵の更新の流れ図である。

【図５】本開示の一実施形態によるサービス処理装置の構造模式図である。

【図６】本開示の別の実施形態によるサービス処理装置の構造模式図である。

【図７】図５及び図６でより詳細に記載されている装置の構造模式図である。

【００２０】

図面に示されている順序は、説明のみのためのものである。モジュールは、異なる順序または並列で実行できる。

【発明を実施するための形態】

【００２１】

本開示の実施形態は以下のように具体的に説明され、例示的な実施形態が図面に示されており、同一または同様のラベルは、本開示全体を通じて同一または同様の機能を有する同一の要素または同様の要素を表す。参照図面によって記載された以下の実施形態は例示的なものであり、本開示を説明するためだけに使用され、本開示を限定するものとして解釈することはできない。代わりに、本開示の実施形態は、添付の特許請求の範囲の精神及び範囲内のすべての変形、修正及び等価物を含む。

【００２２】

図１は、本開示の一実施形態による取引を処理するための方法の流れ図である。図１に示すように、方法には次のものが含まれる。

【００２３】

ブロック１０１では、取引の処理を要求するために使用される元のカード番号が受信され、元のカード番号はクレジットカード番号であり得る。

【００２４】

ブロック１０２では、元のカード番号に対応するハッシュ値が、元のカード番号に基づいて計算され、元のカード番号に対応するインデックスカード番号が、元のカード番号に対応するハッシュ値に基づいて取得される。

【００２５】

ブロック１０３では、エンティティがインデックスカード番号に基づいて取引を処理できるように、取引を処理するエンティティにインデックスカード番号が送信される。

【００２６】

一実施形態では、取引の処理を要求するために使用される元のカード番号を受信した後、元のカード番号に基づいて元のカード番号に対応するハッシュ値を計算し、元のカード番号に対応するハッシュ値に基づいて元のカード番号に対応するインデックスカード番号を取得し、それによって、システム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行う。

【００２７】

図２は、本開示の別の実施形態による取引を処理する方法の流れ図である。図２に示すように、方法には次のものが含まれる。

【００２８】

ブロック２０１では、取引を処理する要求のための元のカード番号が受信される。

【００２９】

一実施形態では、元のカード番号は、クレジットカード番号であり得る。

【００３０】

ブロック２０２では、元のカード番号に対応するハッシュ値が、元のカード番号に基づいて計算される。

【００３１】

一実施形態では、ハッシュ値は、ＰＣＩの規制に準拠した元のカード番号に逆変換することはできない。カードのハッシュ値が変更されることはない。しかし、ハッシュの衝突が発生し得るため、異なるカードが同じハッシュ値を有し得る。したがって、同時実行の場合に、クレジットカードの書き込みを制御するための一意の制限としてハッシュ値のフィールドを使用するだけで、同じハッシュ値を有する２つのクレジットカードの場合は、インデックスカード番号が１枚のカードにのみ割り当てられ保存され得る。

【００３２】

クレジットカード番号に基づいてレコードを検索する場合には、検索用のカード番号のハッシュ値に基づいてカード番号レコードを迅速に検索することが可能である。ハッシュの衝突があり得るため、ハッシュ値に基づいて取得されたレコードは、望ましいレコードではない場合がある。したがって、比較を行い、さらに確認する必要がある。しかし、ハッシュの衝突の可能性はかなり低いため、そのような検索処理は今なお効率が良い。本処理については、さらに詳細に以下で説明する。

【００３３】

ブロック２０３では、データベースが検索され、ハッシュ値を有するカード番号レコードが、データベースに格納されているかどうかが判定される。

【００３４】

ハッシュ値を有するカード番号レコードが見つからない場合、ブロック２０４が実行される。ハッシュ値を有するカード番号レコードが見つかった場合、ブロック２１２が実行される。

【００３５】

ブロック２０４では、元のカード番号が新しいカード番号として判定され、元のカード番号に対応するハッシュ番号が第１の値に設定される。ハッシュ番号は、あるカードを別のカードと区別するために使用される。一実施例として、異なる元のカード番号を有する２つのカードが、同じハッシュ値を有する場合、同時実行の場合と同様に、それぞれ異なるハッシュ番号が与えられる。

【００３６】

本実施形態では、第１の値は、システム性能及び実装要件に基づいて設定され得る。本実施形態は、第１の値の大きさにいかなる制限も課さない。例えば、第１の値は１であり得る。

【００３７】

一実施形態では、すべての格納されたカード番号レコードのうち、ハッシュの衝突レコードがない場合、ハッシュ番号は１である。ハッシュの衝突の場合、ハッシュ番号は順次増大する。簡単に言えば、２つのクレジットカード番号の間にハッシュ値の衝突がある場合、２つのカード番号レコードは同じハッシュ値になる。一方のハッシュ番号は１で、もう一方のハッシュ番号は２である。さらに多くのハッシュの衝突に、同じ方法で番号を付けることができる。例えば、表１に示すように、ハッシュ値の衝突の場合、カード番号が異なる２つのクレジットカード（例えば、インデックスカード番号１０００００００１と１０００００００２）は、同じハッシュ値を有する。表１では、異なるハッシュ番号は、番号１から順次増大し、各カードに付与される。

【００３８】
一実施形態では、クレジットカード番号に対応するハッシュ値及びハッシュ番号は、同時実行の場合に、インデックスカード番号が同じクレジットカードに繰り返し割り当てられることを防止する一意の制限として組み合わされ得る。
【００３９】
ブロック２０５では、インデックスカード番号が元のカード番号に割り当てられる。
【００４０】
ブロック２０６では、最新の秘密鍵及び最新の秘密鍵のバージョンが秘密鍵辞書から取得され、元のカード番号が最新の秘密鍵を使用して暗号化され、最新の秘密鍵のバージョンは、その暗号化から取得した暗号文の先頭と組み合わせて、元のカード番号に対応する暗号文を取得する。
【００４１】
ブロック２０７では、割り当てられたインデックスカード番号、元のカード番号に対応する暗号文、元のカード番号に対応するハッシュ値及びハッシュ値に対応するハッシュ番号が、元のカード番号に対応するカード番号レコードとして使用され、データベースに格納される。
【００４２】
一実施形態では、カード番号レコードのフォーマットは、表１に示す通りである。
【００４３】
【表１】

インデックスカード番号	元のカード番号に対応する暗号文	元のカード番号に対応するハッシュ値	ハッシュ番号
10000001	201410_afseqf1341S&%88fyFYVvy^RA^%ER^cvvIUR&R	6db06c4055368485	1
10000002	201409_afseqfadfadsf13413&%88fyFYVvy^RA^2233ds	6db06c4055368485	2
10000005	201410_15efwf(&&adsf13413&%88fyFYVvy^RA^24inuu	5b8bfb3ba45faf78	1
……	……	……	……

【００４４】
一実施形態では、システムは、各クレジットカードのインデックスカード番号としてシステムに書き込まれるクレジットカードに番号を順次割り当て得る。インデックスカード番号の外部転送及び記憶の場合、クレジットカードの元のカード番号は、ＰＣＩ規格に準拠したインデックスカード番号に基づいて復元することはできない。
【００４５】
元のカード番号に対応する暗号文は、対称暗号アルゴリズムに基づいてクレジットカード番号を暗号化した後に生成された暗号文と、生成された暗号文の先頭と組み合わせた秘密鍵のバージョンとを含む。このようにして、秘密鍵のバージョンに基づいて秘密鍵辞書に対応する秘密鍵を見つけることができ、したがって、元のカード番号に対応する暗号文を復号化することができる。
【００４６】
ブロック２０８では、元のカード番号に対応するカード番号レコードをデータベースに格納するときに、ハッシュ値及びハッシュ番号の一意の制限に違反
があるかどうかが判定される。そうでない場合、ブロック２０９が実行される。元のカード番号に対応するカード番号レコードをデータベースに格納するときに、ハッシュ値及びハッシュ番号の一意の制限に違反がある場合には、ブロック２１０が実行される。
【００４７】
ブロック２０９では、インデックスカード番号が、元のカード番号に正常に割り当てられたと判定され、ブロック２１１が実行される。

【００４８】
ブロック２１０では、インデックスカード番号が、元のカード番号に正常に割り当てられていないと判定され、例外メッセージが返され、ユーザーは再試行を促される。処理が終了する。
【００４９】
ブロック２１１では、エンティティがインデックスカード番号に基づいて取引を処理できるように、取引を処理するエンティティにインデックスカード番号が送信される。処理が終了する。
【００５０】
ブロック２１２では、見つかった各カード番号からカード番号暗号文が取得され、カード番号暗号文の秘密鍵のバージョンが傍受され、秘密鍵辞書が秘密鍵のバージョンに基づいて読み取られ、カード番号暗号文を暗号化するために使用される秘密鍵を取得する。
【００５１】
ブロック２１３では、秘密鍵を使用してカード番号暗号文を復号化し、各カード番号レコードから元のカード番号を取得し、取得した元のカード番号と受信した元のカード番号とを１つずつ比較する。
【００５２】
ブロック２１４では、受信した元のカード番号と同一のカード番号が存在するかどうかを、取得した元のカード番号の中から判定する。「はい」の場合、ブロック２１５が実行される。取得した元のカード番号の中に、受信した元のカード番号と同一のカード番号が存在しないと判定された場合、ブロック２１６が実行される。
【００５３】
ブロック２１５では、受信した元のカード番号に対応するインデックスカード番号が、同一のカード番号に対応するカード番号レコードから取得される。続いて、ブロック２１１が実行される。
【００５４】
ブロック２１６では、受信した元のカード番号が新しいカード番号として判定され、元のカード番号に対応するハッシュ番号が第２の値に設定される。ここで、第２の値は、見つかったカード番号レコードのハッシュ番号の最大値とプリセット値との合計である。
【００５５】
一実施形態では、プリセット値は、システム性能及び実装要件に基づいて設定され得る。本実施形態は、プリセット値の大きさにいかなる制限も課さない。例えば、プリセット値は１であり得る。
【００５６】
続いて、ブロック２０５～２１１が実行される。
【００５７】
本実施形態は、システム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行う。
【００５８】
図３は、本開示のさらに別の実施形態による取引を処理するための方法の流れ図である。一実施形態では、処理される要求が、カード番号データ照会の取引である場合、図３に示すように、方法には、以下が含まれる。
【００５９】
ブロック３０１では、取引を処理する要求のための元のカード番号が受信される。
【００６０】
一実施形態では、元のカード番号は、クレジットカード番号であり得る。
【００６１】
ブロック３０２では、元のカード番号に対応するハッシュ値が、元のカード番号に基づ

いて計算される。

【００６２】

ブロック３０３では、ハッシュ値を有するカード番号レコードが、データベースに格納されているかどうかが検索される。ハッシュ値を有するカード番号レコードが見つかった場合、ブロック３０４が実行される。ハッシュ値を有するカード番号レコードが見つからない場合、ブロック３０９が実行される。

【００６３】

ブロック３０４では、見つかった各カード番号レコードからカード番号暗号文が取得され、カード番号暗号文の秘密鍵のバージョンが傍受され、秘密鍵辞書が秘密鍵のバージョンに基づいて読み取られ、カード番号暗号文を暗号化するために使用される秘密鍵を取得する。

【００６４】

ブロック３０５では、秘密鍵を使用してカード番号暗号文を復号化し、各カード番号レコードから元のカード番号を取得し、取得した元のカード番号と受信した元のカード番号とを１つずつ比較する。

【００６５】

ブロック３０６では、受信した元のカード番号と同一のカード番号が存在するかどうかを、取得した元のカード番号の中から判定する。「はい」の場合、ブロック３０７が実行される。取得した元のカード番号の中に、受信した元のカード番号と同一のカード番号が存在しないと判定された場合、ブロック３０９が実行される。

【００６６】

ブロック３０７では、受信した元のカード番号に対応するインデックスカード番号が、同一のカード番号に対応するカード番号レコードから取得される。

【００６７】

ブロック３０８では、インデックスカード番号に基づいてインデックスカード番号に対応するカード番号データをエンティティが照会できるように、カード番号データ照会サービスを処理するエンティティに、受信した元のカード番号に対応するインデックスカード番号が送信され、照会されたカード番号データが返される。処理が終了する。

【００６８】

ブロック３０９では、データベース内に、受信した元のカード番号に対応するカード番号レコードが存在しないと判定され、ＮＵＬＬ結果が返される。処理が終了する。

【００６９】

本実施形態は、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行い、検索効率を向上させる。

【００７０】

図２及び図３に示す実施形態では、元のカード番号に対応するカード番号レコードの暗号文及び暗号秘密鍵を頻繁に更新する必要がある。暗号文及び暗号の秘密鍵を更新する処理は、図４に示す通りである。図４は、本発明の一実施形態による暗号文及び秘密鍵の更新の流れ図である。暗号文及び暗号の秘密鍵を更新する処理には、次のものが含まれる。

【００７１】

ブロック４０１では、データベースに格納されたカード番号レコードがトラバースされる。

【００７２】

ブロック４０２では、現在トラバースされているカード番号レコード内のカード番号暗号文が取得され、カード番号暗号文の秘密鍵のバージョンが傍受される。

【００７３】

ブロック４０３では、カード番号暗号文の秘密鍵のバージョンが、秘密鍵辞書から取得された秘密鍵の最新バージョンと比較される。

【００７４】

ブロック４０４では、カード番号暗号文の秘密鍵のバージョンが秘密鍵の最新バージョンであるかどうかが判定される。

【００７５】

そうでない場合、ブロック４０５が実行される。カード番号暗号文の秘密鍵のバージョンが秘密鍵の最新バージョンである場合、ブロック４０８が実行される。

【００７６】

ブロック４０５では、カード番号暗号文の秘密鍵のバージョンに対応する秘密鍵を秘密鍵辞書から取得し、取得した秘密鍵を使用して、カード番号暗号文を復号化して元のカード番号を取得する。

【００７７】

ブロック４０６では、秘密鍵の最新バージョンに対応する新しい秘密鍵が秘密鍵辞書から取得され、元のカード番号は新しい秘密鍵を使用して暗号化され、その暗号化から取得した暗号文を最新の秘密鍵と組み合わせて、更新されたカード番号暗号文を取得する。

【００７８】

ブロック４０７では、現在トラバースされているカード番号レコード内のカード番号暗号文のフィールドの内容は、更新されたカード番号暗号文に更新される。

【００７９】

ブロック４０８では、すべてのカード番号レコードがトラバースされているかどうかが判定される。そうでない場合、ブロック４０１が実行される。すべてのカード番号レコードがトラバースされている場合、処理は終了する。

【００８０】

前述の実施形態は、カード番号レコードの暗号文及び秘密鍵を、混乱を起こさずに柔軟に変更することを可能にする。

【００８１】

図５は、本開示の一実施形態による取引を処理するための装置５００の構造模式図である。本実施形態の装置は、本開示の図１に示す実施形態の処理を実施することができる。図５に示すように、装置５００は、受信モジュール５１、計算モジュール５２、取得モジュール５３、及び送信モジュール５４を含み得る。

【００８２】

受信モジュール５１は、元のカード番号がクレジットカード番号であり得る、取引の処理を要求するために使用される元のカード番号を受信するために使用される。

【００８３】

計算モジュール５２は、受信モジュール５１によって受信された元のカード番号に基づいて元のカード番号に対応するハッシュ値を計算するために使用される。

【００８４】

取得モジュール５３は、計算モジュール５２により計算された元のカード番号に対応するハッシュ値に基づいて、元のカード番号に対応するインデックスカード番号を取得するために使用される。

【００８５】

送信モジュール５４は、エンティティがインデックスカード番号に基づいて取引を処理できるように、取引を処理するエンティティに、取得モジュール５３によって取得されたインデックスカード番号を送信するために使用される。

【００８６】

一実施形態では、受信モジュール５１が、取引の処理を要求するためのカード番号を受信した後、計算モジュール５２が、元のカード番号に基づいて元のカード番号に対応するハッシュ値を計算する。続いて、取得モジュール５３は、元のカード番号に対応するハッシュ値に基づいて元のカード番号に対応するインデックスカード番号を取得し、それによって、システム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便

性の高い検索を確実に行う。

【００８７】

図６は、本開示の別の実施形態による取引を処理するための装置６００の構造模式図である。本実施形態の装置６００は、図２、図３、及び図４に示すような実施形態の方法を実施することができる。図５に示すような装置５００と比較して、図６に示す装置６００では、取得モジュール５３は、検索サブモジュール５３１、判定サブモジュール５３２、割り当てサブモジュール５３３、暗号化サブモジュール５３４及び、記憶サブモジュール５３５を含み得る。

【００８８】

検索サブモジュール５３１は、ハッシュ値を有するカード番号レコードが格納されているかどうかをデータベースで検索するために使用される。

【００８９】

判定サブモジュール５３２は、検索サブモジュール５３１がハッシュ値を有するカード番号レコードを見つけられなかった場合に、元のカード番号を新しいカード番号として設定するために使用される。

【００９０】

割り当てサブモジュール５３３は、判定サブモジュール５３２が、元のカード番号を新しいカード番号として判定した後、元のカード番号に対応するハッシュ番号を第１の値に設定し、元のカード番号にインデックスカード番号を割り当てるために使用される。一実施形態では、第１の値は、システム性能及び実装要件に基づいて設定され得る。本実施形態は、第１の値の大きさにいかなる制限も課さない。例えば、第１の値は１であり得る。

【００９１】

暗号化サブモジュール５３４は、秘密鍵辞書から最新の秘密鍵と最新の秘密鍵のバージョンを取得し、最新の秘密鍵を使用して元のカード番号を暗号化し、元のカード番号に対応する暗号文を取得するために、最新の秘密鍵のバージョンとその暗号化から取得した暗号文の先頭を組み合わせるために使用される。

【００９２】

記憶サブモジュール５３５は、割り当てサブモジュール５３３によって割り当てられたインデックスカード番号、暗号化サブモジュール５３４により取得された元のカード番号に対応する暗号文、元のカード番号に対応するハッシュ値及び元のカード番号に対応するカード番号レコードとしてのハッシュ値に対応するハッシュ番号を使用し、それらをデータベースに格納するものである。

【００９３】

判定サブモジュール５３２はさらに、記憶サブモジュール５３５が、元のカード番号に対応するカード番号レコードをデータベースに格納するときに、ハッシュ値及びハッシュ番号の一意の制限に違反がなければ、インデックスカード番号が、元のカード番号に正常に割り当てられていることを判定するために使用される。

【００９４】

一実施形態では、取得モジュール５３は、取得サブモジュール５３６と、復号化サブモジュール５３７と、比較サブモジュール５３８とをさらに含み得る。

【００９５】

取得サブモジュール５３６は、検索サブモジュール５３１が、ハッシュ値を有するカード番号レコードを見つけた場合、見つかった各カード番号レコードのカード番号暗号文を取得し、カード番号暗号文の秘密鍵のバージョンを傍受し、カード番号暗号文を暗号化するために使用される秘密鍵を取得するために、秘密鍵のバージョンに基づいて秘密鍵辞書を読み取るために使用される。

【００９６】

復号化サブモジュール５３７は、各カード番号レコードから元のカード番号を取得するために、取得サブモジュール５３６により取得された秘密鍵を使用してカード番号暗号文を復号化するために使用される。

【００９７】
比較サブモジュール５３８は、復号化サブモジュール５３７によって取得された元のカード番号と、受信した元のカード番号とを１つずつ比較するために使用される。
【００９８】
取得サブモジュール５３６はさらに、比較サブモジュール５３８が、復号化サブモジュール５３７によって取得された元のカード番号の中に、受信した元のカード番号と同一のカード番号が存在すると判定した場合に、同一のカード番号に対応するカード番号レコードから、受信した元のカード番号に対応するインデックスカード番号を取得するために使用される。
【００９９】
さらに、取得モジュール５３は、設定サブモジュール５３９をさらに含み得る。
【０１００】
判定サブモジュール５３２はさらに、比較サブモジュール５３８が、復号化サブモジュール５３７によって取得された元のカード番号の中に、受信した元のカード番号と同一のカード番号が存在しないと判定した場合に、受信した元のカード番号を新しいカード番号として設定するために使用される。
【０１０１】
設定サブモジュール５３９は、元のカード番号に対応するハッシュ番号を第２の値に設定するために使用される。ここで、第２の値は、見つかったカード番号レコードのハッシュ番号の最大値とプリセット値との合計である。続いて、割り当てサブモジュール５３３、暗号化サブモジュール５３４及び記憶サブモジュール５３５が、インデックスカード番号を取得する処理を実行する。
【０１０２】
一実施形態では、プリセット値は、システム性能及び実施態様要件に基づいて設定され得る。本実施形態では、プリセット値の大きさに制限はない。例えば、プリセット値は１であり得る。
【０１０３】
一実施形態では、取引はカード番号データ照会であり得る。この場合、送信モジュール５４は、具体的には、エンティティが、インデックスカード番号に基づいてインデックスカード番号に対応するカード番号データを照会できるように、カード番号データ照会サービスを処理するエンティティに、取得モジュール５３によって取得されたインデックスカード番号を送信するために使用され、照会されたカード番号データが返される。
【０１０４】
さらに、取得モジュール５３は、トラバースサブモジュール５３１０、取得サブモジュール５３６、比較サブモジュール５３８、復号化サブモジュール５３７、暗号化サブモジュール５３４、及び更新サブモジュール５３１１を含み得る。
【０１０５】
トラバースサブモジュール５３１０は、データベースに格納されたカード番号レコードをトラバースするために使用される。
【０１０６】
取得サブモジュール５３６は、トラバースサブモジュール５３１０によって、現在トラバースされているカード番号レコード内のカード番号暗号文を取得し、カード番号暗号文の秘密鍵のバージョンを傍受するために使用される。
【０１０７】
比較サブモジュール５３８は、取得サブモジュール５３６によって取得された秘密鍵のバージョンと、秘密鍵辞書から取得された秘密鍵の最新バージョンを比較するために使用される。
【０１０８】
取得サブモジュール５３６はさらに、比較サブモジュール５３８が、取得サブモジュール５３６によって取得された秘密鍵のバージョンが、秘密鍵の最新バージョンではないと

判定した場合に、秘密鍵辞書からカード番号暗号文の秘密鍵のバージョンに対応する秘密鍵を取得し、復号化サブモジュール５３７が元のカード番号を取得した後、秘密鍵辞書から最新の秘密鍵に対応する新しい秘密鍵を取得する。

【０１０９】

復号化サブモジュール５３７は、取得サブモジュール５３６で取得された秘密鍵を使用して、元のカード番号を取得するために、カード番号暗号文を復号化するために使用される。

【０１１０】

暗号化サブモジュール５３４は、取得サブモジュール５３６によって取得された新しい秘密鍵を使用して、復号化サブモジュール５３７によって取得された元のカード番号を暗号化し、更新されたカード番号暗号文を取得するために、その暗号化から取得した暗号文と秘密鍵の最新バージョンを組み合わせるために使用される。

【０１１１】

更新サブモジュール５３１１は、トラバースサブモジュール５３１０によって現在トラバースされているカード番号レコードのカード番号暗号文のフィールドの内容を、暗号化サブモジュール５３４によって取得された更新されたカード番号暗号文に更新するために使用される。

【０１１２】

取引を処理するための上記の装置は、システム内のいくつかの元のカード番号に対応するインデックスカード番号をそれぞれ作成し、同時実行が多い場合のインデックスカード番号と元のカード番号との間の１対１の対応及びパスワードが頻繁に変更される暗号化されたクレジットカード番号の利便性の高い検索を確実に行う。

【０１１３】

本開示の説明において、「ｆｉｒｓｔ（第１）」及び「ｓｅｃｏｎｄ（第２）」などの用語は、説明のためにのみ使用され、相対的な重要性を示唆または意味するものと解釈することはできないことに留意されたい。また、本明細書において、「ａ　ｐｌｕｒａｌｉｔｙ　ｏｆ（複数）」とは、別段の定めがない限り、２つ以上を意味する。

【０１１４】

流れ図に記載された、または本明細書の他のいずれかの方法で説明された任意の処理または方法は、特定の論理機能または工程段階を実現する実行可能命令コードのための１つまたは複数のモジュール、セグメントまたは部分を含むと理解され得る。さらに、本開示の例示的な実施形態は、関連する機能に基づいて実質的に同時の方法または逆の順序を含む、図示または議論されるものとは異なる順序で機能が実行され得る、他の実施態様を含む。これは、本開示の実施形態が属する当業者によって理解されるべきである。

【０１１５】

本開示の各部分は、ハードウェア、ソフトウェア、ファームウェアまたはそれらの組み合わせによって実現され得ることを理解されたい。上記の実施形態では、複数の工程または方法は、メモリーに格納されたソフトウェアまたはファームウェアを使用して実施し得て、適切な命令実行システムを使用して実行し得る。例えば、ハードウェアを使用して実装されている場合、同様に他の実施形態でも、工程または方法は、当該技術分野で周知の次の技術の１つまたは組み合わせを使用することによって実施し得る。データ信号の論理機能を実現する論理ゲート回路を有するディスクリート論理回路、適切な組み合わせ論理ゲート回路を有する特定用途向け集積回路、プログラマブルゲートアレイ（ＰＧＡ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）など。

【０１１６】

当業者は、上記の方法の工程の全部または一部が、関連するハードウェアにプログラムを指示することによって達成され得ることを理解しなければならない。プログラムは、コンピューター可読記憶媒体に格納され得て、実行時、プログラムには、方法の実施形態における工程の１つまたは組み合わせが含まれる。

【０１１７】

さらに、本開示の各実施形態の各機能モジュールは、単一の処理モジュールに統合され得て、または、これらのモジュールが別個の物理的存在であり得るか、２つ以上のモジュールが単一の処理モジュールに統合され得る。統合モジュールは、ハードウェアの形で、またはソフトウェア機能モジュールの形で実現され得る。統合モジュールがソフトウェア機能モジュールの形で実現され、スタンドアロン製品として販売または使用される場合、統合モジュールはコンピューター可読記憶媒体に格納され得る。

【０１１８】

上記の記憶媒体は、読み出し専用メモリー、磁気ディスク、ＣＤなどであり得る。

【０１１９】

一実施形態では、本開示は、１つまたは複数のプロセッサー（ＣＰＵ）、入力／出力インターフェイス、ネットワークインターフェイス、及びメモリーを含む、コンピューティングデバイスを提供する。限定ではなく一実施例として、図７は、図５及び図６でさらに詳細に説明される、装置５００及び６００などの例示的な装置７００を示す。実施態様において、装置７００には、限定するものではないが、１つまたは複数のプロセッサー７０２、入力／出力（Ｉ／Ｏ）インターフェイス７０４、ネットワークインターフェイス７０６、及びメモリー７０８を含み得る。

【０１２０】

メモリー７０８は、コンピューター可読媒体の形、例えば、非永続的記憶装置、ランダムアクセスメモリー（ＲＡＭ）及び／または不揮発性記憶装置、例えば、読み出し専用メモリー（ＲＯＭ）またはフラッシュメモリー（フラッシュＲＡＭ）を含み得る。メモリー７０８は、コンピューター可読媒体の一実施例と見なすことができる。

【０１２１】

コンピューター可読媒体は、任意の方法または技術によって情報記憶の目的を達成することができる、永続的及び非永続的な、取外し可能及び取外し不可能な媒体を含む。情報は、コンピューター可読命令、データ構造、プログラムモジュール、または他のデータを指し得る。コンピューター記憶媒体の実施例には、相変化メモリー（ＰＲＡＭ）、スタティックランダムアクセスメモリー（ＳＲＡＭ）、ダイナミックランダムアクセスメモリー（ＤＲＡＭ）、ランダムアクセスメモリー（ＲＡＭ）のその他のタイプ、読み取り専用メモリー（ＲＯＭ）、電気的消去可能ＰＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリーまたはその他のメモリー技術、読み取り専用コンパクトディスク（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）またはその他の光記憶媒体、カセットテープ、ディスケットまたはその他の磁気記憶装置、またはコンピューティングデバイスによってアクセス可能な情報を格納するために使用することができる任意のその他の非伝送媒体が含まれるが、これらに限定されるものではない。本明細書で定義されているように、コンピューター可読媒体には、変調されたデータ信号及び搬送波などの一時的な媒体は含まれない。

【０１２２】

メモリー７０８は、プログラムモジュール７１０及びプログラムデータ７１２を含み得る。プログラムモジュール７１０は、前述の実施形態で説明したような装置５００及び／または装置６００の前述のモジュール及び／またはサブモジュールのうちの１つまたは複数を含み得る。これらのモジュールの詳細は、前述の説明で見出すことができるので、ここでは重複して説明しない。

【０１２３】

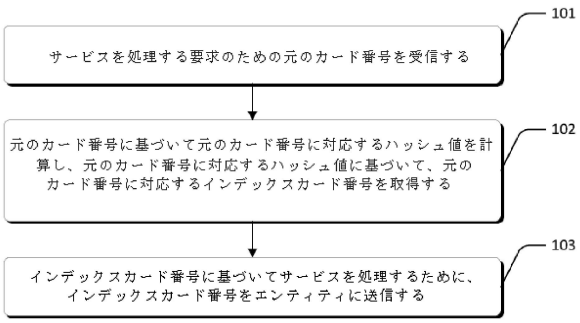
本明細書を通して、「ａｎ　ｅｍｂｏｄｉｍｅｎｔ（一実施形態）」、「ｓｏｍｅ　ｅｍｂｏｄｉｍｅｎｔｓ（いくつかの実施形態）」、「ａｎ　ｅｘａｍｐｌｅ（一実施例）」、「ａ　ｓｐｅｃｉｆｉｃ　ｅｘａｍｐｌｅ（特定の実施例）」、または「ｓｏｍｅ　ｅｘａｍｐｌｅｓ（いくつかの実施例）」への言及は、そのような実施形態または実施例に関連して説明されている特定の特徴、構造、材料、または特性が、本開示の少なくとも１つの実施形態または実施例に含まれることを意味する。本明細書を通して、これらの用語の表現は、必ずしも同じ実施形態または実施例を指しているわけではない。さらに、特定の特徴、構造、材料、または特性は、１つまたは複数の実施形態または実施例において

任意の適切な方法で組み合わせ得る。

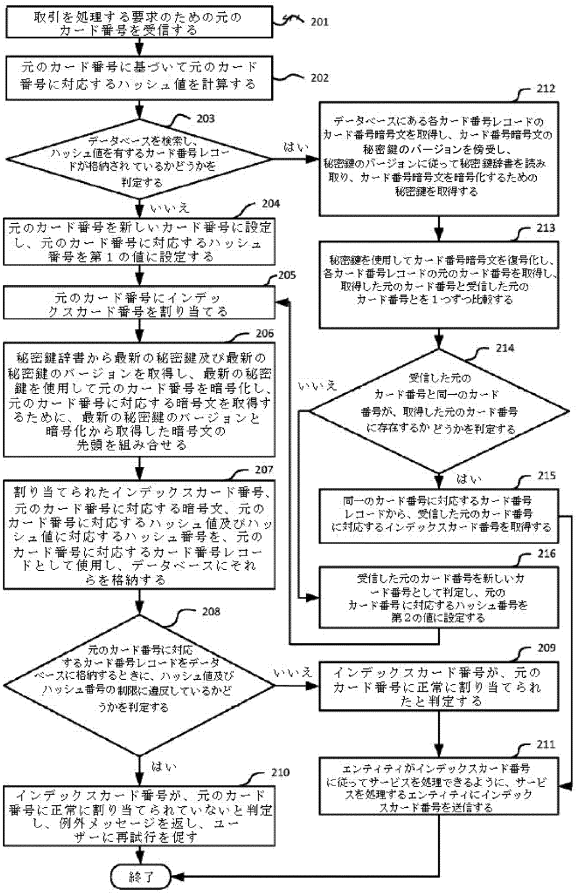
【０１２４】

本開示の実施形態を上記で示し説明してきたが、上記の実施形態は例示的なものであり、本開示を限定するものと解釈すべきではなく、当業者であれば、本開示の範囲内で、実施形態を変更、修正、置換、及び交替することができることが理解されよう。

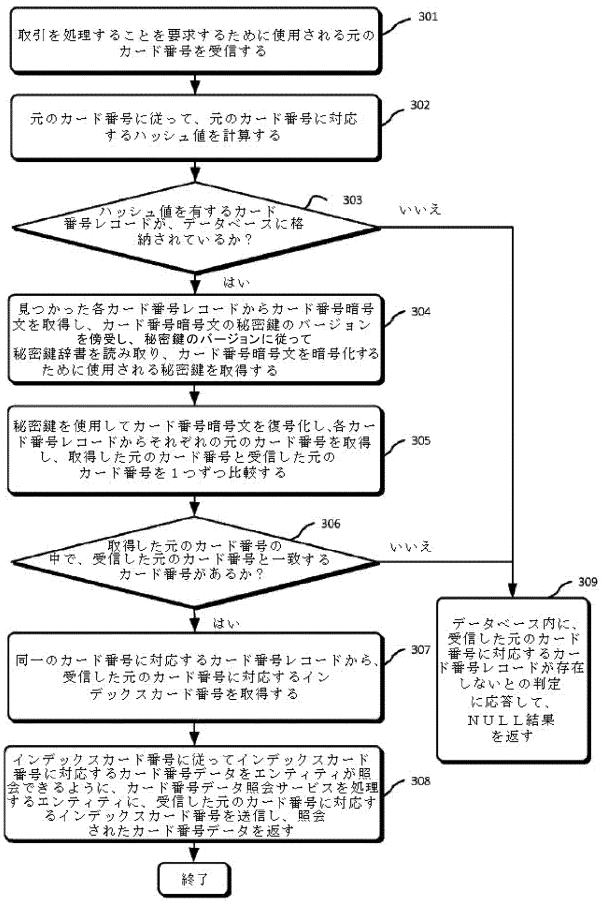
【図１】



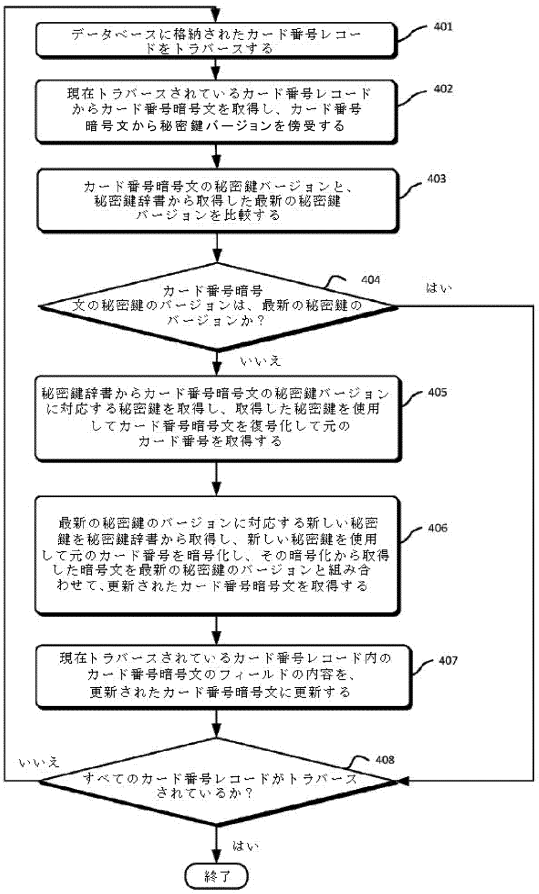
【図２】



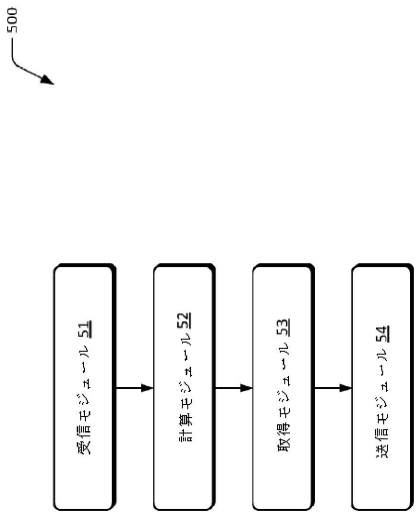
【図３】


取引を処理することを要求するために使用される元のカード番号を受信する
301
元のカード番号に従って、元のカード番号に対応するハッシュ値を計算する
302
ハッシュ値を有するカード番号レコードが、データベースに格納されているか？
303
いいえ
はい
見つかった各カード番号レコードからカード番号暗号文を取得し、カード番号暗号文の秘密鍵のバージョンを傍受し、秘密鍵のバージョンに従って秘密鍵辞書を読み取り、カード番号暗号文を暗号化するために使用される秘密鍵を取得する
304
秘密鍵を使用してカード番号暗号文を復号化し、各カード番号レコードからそれぞれの元のカード番号を取得し、取得した元のカード番号と受信した元のカード番号を１つずつ比較する
305
取得した元のカード番号の中で、受信した元のカード番号と一致するカード番号があるか？
306
いいえ
はい
同一のカード番号に対応するカード番号レコードから、受信した元のカード番号に対応するインデックスカード番号を取得する
307
インデックスカード番号に従ってインデックスカード番号に対応するカード番号データをエンティティが照会できるように、カード番号データ照会サービスを処理するエンティティに、受信した元のカード番号に対応するインデックスカード番号を送信し、照会されたカード番号データを返す
308
データベース内に、受信した元のカード番号に対応するカード番号レコードが存在しないとの判定に応答して、ＮＵＬＬ結果を返す
309
終了

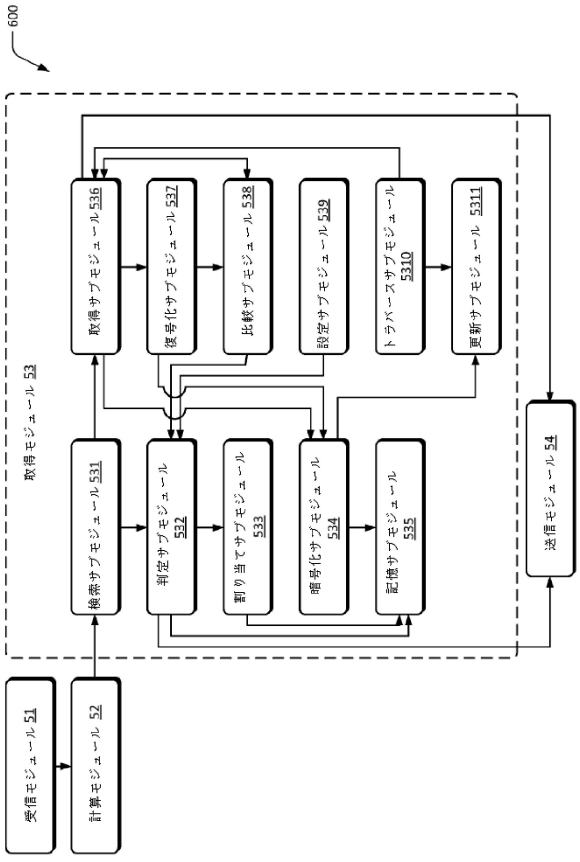
【図４】


データベースに格納されたカード番号レコードをトラバースする
401
現在トラバースされているカード番号レコードからカード番号暗号文を取得し、カード番号暗号文から秘密鍵バージョンを傍受する
402
カード番号暗号文の秘密鍵バージョンと、秘密鍵辞書から取得した最新の秘密鍵バージョンを比較する
403
カード番号暗号文の秘密鍵のバージョンは、最新の秘密鍵のバージョンか？
404
はい
いいえ
秘密鍵辞書からカード番号暗号文の秘密鍵バージョンに対応する秘密鍵を取得し、取得した秘密鍵を使用してカード番号暗号文を復号化して元のカード番号を取得する
405
最新の秘密鍵のバージョンに対応する新しい秘密鍵を秘密鍵辞書から取得し、新しい秘密鍵を使用して元のカード番号を暗号化し、その暗号化から取得した暗号文を最新の秘密鍵のバージョンと組み合わせて、更新されたカード番号暗号文を取得する
406
現在トラバースされているカード番号レコード内のカード番号暗号文のフィールドの内容を、更新されたカード番号暗号文に更新する
407
すべてのカード番号レコードがトラバースされているか？
408
いいえ
はい
終了

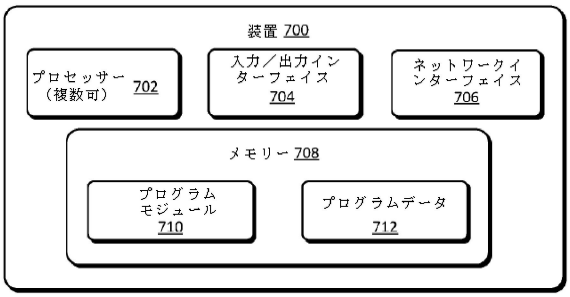
【図５】


500
受信モジュール 51
計算モジュール 52
取得モジュール 53
送信モジュール 54

【図６】


600
取得モジュール 53
取得サブモジュール 536
復号化サブモジュール 537
比較サブモジュール 538
設定サブモジュール 539
トラバースサブモジュール 5310
更新サブモジュール 5311
検索サブモジュール 531
判定サブモジュール 532
割り当てサブモジュール 533
暗号化サブモジュール 534
記憶サブモジュール 535
送信モジュール 54
受信モジュール 51
計算モジュール 52

【図７】


装置 700
プロセッサー（複数可） 702
入力／出力インターフェイス 704
ネットワークインターフェイス 706
メモリー 708
プログラムモジュール 710
プログラムデータ 712

フロントページの続き

(72)発明者　ジュン　イン
中華人民共和国　３１１１２１　ハンチョウ　ユー　ハン　ディストリクト　ウェスト　ウェン　イー　ロード　ナンバー９６９　ビルディング　３　５／エフ　アリババ　グループ　リーガル　デパートメント内

審査官　金沢　史明

(56)参考文献　特開２００２－０５６３３２（ＪＰ，Ａ）
特開２００２－１５７４２１（ＪＰ，Ａ）
特開２００２－３１２７０７（ＪＰ，Ａ）
特開２００３－１７８１８５（ＪＰ，Ａ）
特開２００８－０３３６４１（ＪＰ，Ａ）
米国特許第０８８９７４５１（ＵＳ，Ｂ１）
中国特許出願公開第１０３３２６９９４（ＣＮ，Ａ）
特表２０１２－５０７７６７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００－　９／３８
Ｇ０６Ｆ　２１／００－２１／８８
Ｇ０６Ｑ　２０／２４，２０／３８
Ｇ０６Ｆ　１６／００
Ｇ０９Ｃ　　１／００