(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7691998号
(P7691998)

(45)発行日　令和7年6月12日(2025.6.12)

(24)登録日　令和7年6月4日(2025.6.4)

(51)国際特許分類		FI		
G09C 1/00 (2006.01)		G09C	1/00	620Z
H04L 9/08 (2006.01)		H04L	9/08	C
		H04L	9/08	F

請求項の数　11　（全29頁）

(21)出願番号　特願2022-558211(P2022-558211)
(86)(22)出願日　令和3年4月6日(2021.4.6)
(65)公表番号　特表2023-520776(P2023-520776A)
(43)公表日　令和5年5月19日(2023.5.19)
(86)国際出願番号　PCT/GB2021/050838
(87)国際公開番号　WO2021/205154
(87)国際公開日　令和3年10月14日(2021.10.14)
審査請求日　令和6年2月28日(2024.2.28)
(31)優先権主張番号　2005237.9
(32)優先日　令和2年4月8日(2020.4.8)
(33)優先権主張国・地域又は機関
英国(GB)

(73)特許権者　522376634
ピーキューシールド エルティーディー
イギリス国，オックスフォードシャー　オーエックス２　７エイチティー　オックスフォード　バンベリー　ロード　２６７　プラマ　ハウス
(74)代理人　100079108
弁理士　稲葉 良幸
(74)代理人　100109346
弁理士　大貫 敏史
(74)代理人　100117189
弁理士　江口 昭彦
(74)代理人　100134120
弁理士　内藤 和彦
(72)発明者　プレスト，トーマス

最終頁に続く

(54)【発明の名称】　圧縮暗号化のための方法及びシステム

(57)【特許請求の範囲】

【請求項１】

複数の暗号化部分を含む暗号文を複数のユーザに送信する方法であって、コンピュータが、

（ａ）前記複数のユーザのシステムパラメータの共通セットを提供することと、

（ｂ）格子に基づく暗号化方式及び同種写像に基づく暗号化方式のいずれかと、前記複数のユーザの各ユーザに一意のパラメータとを使用して平文を暗号化することにより、前記複数の暗号化部分を生成することと、

（ｃ）前記システムパラメータの共通セットから導出された部分及び前記複数の暗号化部分を含む前記暗号文を生成することと、

（ｄ）前記暗号文を前記複数のユーザに送信することであって、前記暗号文は、少なくとも部分的に、前記複数のユーザの各ユーザに一意の前記パラメータを使用して復号可能である、送信することと

を含む方法。

【請求項２】

前記システムパラメータの共通セットは、シード及び疑似乱数生成器を使用して生成される、請求項１に記載の方法。

【請求項３】

前記複数のユーザの各ユーザに一意の前記パラメータのうちの少なくともパラメータは、シード及び疑似乱数生成器を使用して生成される、請求項１又は２に記載の方法。

【請求項４】
前記システムパラメータの共通セット又は前記複数のユーザの各ユーザに一意の前記パラメータは、非正方行列を含む、請求項１～３のいずれか一項に記載の方法。
【請求項５】
（ａ）前記システムパラメータの共通セットを含むシステムパラメータセットを生成することであって、前記システムパラメータセットは、前記複数のユーザのうちのユーザの公開鍵に依存しないパラメータを含む、生成することと、
（ｂ）前記システムパラメータセットに少なくとも部分的に基づいて、前記システムパラメータの共通セットから導出された部分である固定成分を生成することと
をさらに含み、
前記複数の暗号化部分を生成することは、前記複数のユーザの各公開鍵を使用して平文を暗号化することにより、複数の可変成分を生成することを含み、
前記暗号文は、少なくとも部分的に前記固定成分を使用して復号可能である、請求項１～４のいずれか一項に記載の方法。
【請求項６】
前記暗号化は、リンドナー－ペイカート方式、超特異同種写像ディフィー－ヘルマンプロトコル及び同種写像に基づく公開鍵暗号化方式からなる群から選択される暗号化方式に基づく、請求項５に記載の方法。
【請求項７】
データベースを編成することをさらに含み、前記データベースを編成することは、
項数ｍのツリー構造で複数の受信者を構造化することであって、「ｍ」は、少なくとも２である、構造化することを含み、
前記暗号文を前記複数のユーザに送信することは、前記暗号文を前記複数の受信者の全員よりも少ない数の受信者に送信することを含む、請求項１～６のいずれか一項に記載の方法。
【請求項８】
前記項数ｍは、８～１６である、請求項７に記載の方法。
【請求項９】
前記送信することは、前記ツリー構造の各ノードに同じメッセージを送信することを含む、請求項７又は８に記載の方法。
【請求項１０】
前記同じメッセージは、前記データベースのユーザの暗号鍵の更新情報を含む、請求項９に記載の方法。
【請求項１１】
１つ又は複数のコンピュータプロセッサと、それに結合されたコンピュータメモリとを含むシステムであって、前記コンピュータメモリは、前記１つ又は複数のコンピュータプロセッサによって実行されると、請求項１～１０のいずれか一項に記載の方法を実施する機械実行可能コードを含む、システム。
【発明の詳細な説明】
【背景技術】
【０００１】
背景
[0001] 実用的な大規模量子計算の間近に迫った到来には、幾つかのセキュリティ課題が付随し、そのうちの特に重要であるのは、現在使用されている暗号化方法が、量子コンピュータに基づく攻撃に対して強靭でないことである。したがって、新たな暗号化方法が開発中であるが、それらは、方法のサイズ及び通信要件を含めて、より確立された方法の成熟性及び深みを欠く傾向がある。
【発明の概要】
【課題を解決するための手段】
【０００２】

概要

[0002] 一態様において、本開示は、前量子及び後量子暗号化方式の両方を使用して生成される暗号化更新及び他の暗号化メッセージのサイズを下げる方法を提供する。暗号化プロセスで使用されるパラメータの少なくとも幾つかを再使用することにより、それらのパラメータの１つのコピーを暗号化と共に送信して、送信されるデータ量を低減し得る。１つのメッセージ当たり１つのコピーの代わりに、１つのコピーを使用することができるため、大きい効率利得を実現することができる。この再使用により、より好ましい組織的階層を使用することも可能になり、非再使用方式と比較した場合、多数の暗号化方法を送信する際に性能を改善することができる。パラメータの再使用を墨塗り又は消去署名方式と組み合わせると、暗号化メッセージの送信中に送信されるデータのサーバ側での大きい低減に繋がり得、効率利得に繋がる。

【０００３】

[0003] 別の態様において、本開示は、複数の暗号化部分を含む暗号文を複数のユーザに送信する方法を提供し、本方法は、（ａ）複数のユーザのシステムパラメータの共通セットを提供することと、（ｂ）複数のユーザの各ユーザに一意のパラメータを使用して平文を暗号化することにより、複数の暗号化部分を生成することと、（ｃ）システムパラメータの共通セットから導出された部分及び複数の暗号化部分を含む暗号文を生成することと、（ｄ）暗号文を複数のユーザに送信することであって、暗号文は、少なくとも部分的に、複数のユーザの各ユーザに一意のパラメータを使用して復号可能である、送信することとを含む。

【０００４】

[0004] 幾つかの実施形態において、暗号化部分は、格子に基づく暗号化方式を使用して暗号化される。幾つかの実施形態において、暗号化部分は、同種写像に基づく暗号化方式を使用して暗号化される。幾つかの実施形態において、システムパラメータの共通セットは、シード及び疑似乱数生成器を使用して生成される。幾つかの実施形態において、複数のユーザの各ユーザに一意のパラメータのうちの少なくともパラメータは、シード及び疑似乱数生成器を使用して生成される。幾つかの実施形態において、システムパラメータの共通セット又は複数のユーザの各ユーザに一意のパラメータは、非正方行列を含む。

【０００５】

[0005] 別の態様において、本開示は、暗号文を複数のユーザに送信する方法を提供し、本方法は、（ａ）システムパラメータセットを生成することであって、パラメータセットは、複数のユーザのうちのユーザの公開鍵に依存しないパラメータを含む、生成することと、（ｂ）システムパラメータセットに少なくとも部分的に基づいて固定成分を生成することと、（ｃ）複数のユーザの各公開鍵を使用して平文を暗号化することにより、複数の可変成分を生成することと、（ｄ）固定成分及び可変成分を含む暗号文を複数のユーザに送信することであって、暗号文は、少なくとも部分的に固定成分を使用して復号可能である、送信することとを含む。

【０００６】

[0006] 幾つかの実施形態において、暗号化は、リンドナー－ペイカート方式、超特異同種写像ディフィー－ヘルマンプロトコル及び同種写像に基づく公開鍵暗号化方式からなる群から選択される暗号化方式に基づく。

【０００７】

[0007] 別の態様において、本開示は、データベースを編成する方法を提供し、本方法は、（ａ）項数ｍのツリー構造で複数の受信者を構造化することであって、「ｍ」は、少なくとも２である、構造化することと、（ｂ）圧縮暗号文更新を複数の受信者の全て未満に送信することとを含む。

【０００８】

[0008] 幾つかの実施形態において、項数ｍは、少なくとも約８である。幾つかの実施形態において、項数ｍは、約８～約１６である。幾つかの実施形態において、送信することに使用されるバイト数は、更新を複数の受信者の各々に送信するためのバイト数の約１

／２以下である。幾つかの実施形態において、圧縮暗号文更新は、格子に基づく暗号化方式を使用して暗号化される。幾つかの実施形態において、圧縮暗号文更新は、同種写像に基づく暗号化方式を使用して暗号化される。幾つかの実施形態において、送信することは、ツリー構造の各ノードに同じメッセージを送信することを含む。幾つかの実施形態において、同じメッセージは、データベースのユーザの暗号鍵の更新情報を含む。別の態様において、本開示は、複数の暗号鍵及びマルチ暗号文を含む暗号化更新を複数の受信者ノードに対して実行する方法を提供し、本方法は、（ａ）暗号化更新を受信することと、（ｂ）複数の暗号鍵の１つ又は複数及びマルチ暗号文の１つ又は複数の暗号文を除去することにより、縮小暗号化更新を生成することと、（ｃ）縮小暗号化更新を複数の受信者ノードのうちの受信者ノードに送信することと、（ｄ）複数のノードのうちの１つ又は複数の他のノードについて（ｂ）～（ｃ）を繰り返すこととを含む。幾つかの実施形態において、各ノードは、複数の暗号鍵のうちの１つの暗号鍵及びマルチ暗号文のうちの１つの暗号文を含む縮小暗号化更新を受信する。幾つかの実施形態において、複数のノードの各ノードは、複数の暗号鍵のうちの異なる暗号鍵と、複数のノードのうちのそれぞれの他のノードからのマルチ暗号文のうちの異なる暗号文とを含む縮小暗号化更新を受信する。幾つかの実施形態において、受信者ノードは、子ノードを有する。幾つかの実施形態において、子ノードは、子ノードのパス中の各受信者ノードの復号鍵にアクセスすることができる。幾つかの実施形態において、（ｄ）は、複数のノードの各ノードと略同時に実行される。幾つかの実施形態において、本方法は、複数のノードに送信されるバイト数を約１／ｎ以下に低下させることを更に含み、ここで、ｎは、複数のノード中のノード数である。幾つかの実施形態において、１つ又は複数の暗号文は、格子に基づく暗号化方式を使用して暗号化される。幾つかの実施形態において、１つ又は複数の暗号文は、同種写像に基づく暗号化方式を使用して暗号化される。幾つかの実施形態において、暗号化更新は、黒塗り署名を用いて署名される。幾つかの実施形態において、黒塗り署名は、複数の暗号鍵及び複数のマルチ暗号文の１つ又は複数を除去することを促進する。

【０００９】

［0009］ 本開示の別の態様は、１つ又は複数のコンピュータプロセッサによって実行されると、上記方法又は本明細書の他の箇所における方法のいずれかを実施する機械実行可能コードを含む非一時的コンピュータ可読媒体を提供する。

【００１０】

［0010］ 本開示の別の態様は、１つ又は複数のコンピュータプロセッサと、それに結合されたコンピュータメモリとを含むシステムを提供する。本コンピュータメモリは、１つ又は複数のコンピュータプロセッサによって実行されると、上記方法又は本明細書の他の箇所における方法のいずれかを実施する機械実行可能コードを含む。

【００１１】

［0011］ 本開示の追加の態様及び利点は、本開示の単に例示的な実施形態が示され、説明される以下の詳細な説明から当業者に容易に明らかになるであろう。認識されるように、本開示は、他の異なる実施形態が可能であり、その幾つかの詳細は、全て本開示から逸脱することなく種々の明白な点で変更可能である。したがって、図面及び説明は、例示的な性質のものであると見なされるべきであり、限定として見なされるべきではない。

【００１２】

参照による援用

［0012］ 本明細書で引用される全ての公開公報、特許及び特許出願は、個々の各公開公報、特許又は特許出願が参照により援用されると特に個々に示されているのと同程度まで、参照により本明細書に援用される。参照により援用される公開公報及び特許又は特許出願が、本明細書に含まれる開示と競合する限り、本明細書がそのようなあらゆる競合資料に取って代わり、及び／又は優先されることが意図される。

【００１３】

図面の簡単な説明

［0013］ 本発明の新規な特徴を特に添付の特許請求の範囲に記載する。本発明の特徴及

び利点のよりよい理解は、本発明の原理が利用される例示的な実施形態を記載する以下の詳細な説明及び添付図面（同様に本明細書における「図（Figure）」及び「図（ＦＩＧ．）」）を参照することによって得られる。

【図面の簡単な説明】

【００１４】

【図１】[0014]複数の暗号文を複数のユーザに送信するプロセス例のフローチャートである。

【図２】[0015]複数の暗号文を複数のユーザに送信するプロセス例のフローチャートである。

【図３】[0016]複数の暗号鍵及び複数のマルチ暗号文を含む暗号化更新を複数の受信者ノードに対して実行するプロセス例のフローチャートである。

【図４Ａ】[0017]リンドナー－ペイカート枠組みの一例を示す。

【図４Ｂ】[0017]リンドナー－ペイカート枠組みの一例を示す。

【図４Ｃ】[0017]リンドナー－ペイカート枠組みの一例を示す。

【図４Ｄ】[0018]１人又は複数の受信者に送信される単一メッセージの暗号文圧縮の一実装形態の擬似コード例を示す。

【図５Ａ】[0019]１人又は複数の受信者に送信される１つ又は複数のメッセージの暗号文圧縮の一実装形態の擬似コード例を示す。

【図５Ｂ】[0020]ＳＩＫＥ公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図５Ｃ】[0020]ＳＩＫＥ公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図５Ｄ】[0020]ＳＩＫＥ公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図６Ａ】[0021]１人又は複数の受信者に送信される１つのメッセージのＳＩＫＥ公開鍵暗号化方式での暗号文圧縮の一実装形態の擬似コード例を示す。

【図６Ｂ】[0022]１人又は複数の受信者に送信される１つ又は複数のメッセージのＳＩＫＥ公開鍵暗号化方式での暗号文圧縮の一実装形態の擬似コード例を示す。

【図７Ａ】[0023]Kyber512鍵カプセル化メカニズムを使用する複数の異なる状況での更新サイズのプロットを示す。

【図７Ｂ】[0024]FrodoKEM-640鍵カプセル化メカニズムを使用する複数の異なる状況での更新サイズのプロットを示す。

【図７Ｃ】[0025]ＳＩＫＥ／p434鍵カプセル化メカニズムを使用する複数の異なる状況での更新サイズのプロットを示す。

【図８】[0026]種々の暗号化方式を用いる暗号文圧縮方法及びシステムを使用することの効率改善の表を示す。

【図９】[0027]超特異同種写像ディフィー－ヘルマン鍵交換（ＳＩＤＨ）の一例を示す。

【図１０Ａ】[0028]暗号文圧縮と併せて使用し得る複数のプロトコルを示す。

【図１０Ｂ】[0028]暗号文圧縮と併せて使用し得る複数のプロトコルを示す。

【図１０Ｃ】[0028]暗号文圧縮と併せて使用し得る複数のプロトコルを示す。

【図１０Ｄ】[0028]暗号文圧縮と併せて使用し得る複数のプロトコルを示す。

【図１０Ｅ】[0028]暗号文圧縮と併せて使用し得る複数のプロトコルを示す。

【図１１】[0029]本明細書で提供される方法を実施するようにプログラム又は他の方法で構成されたコンピュータシステムを示す。

【図１２Ａ】[0030]可換性超特異同種写像ディフィー－ヘルマン鍵交換（ｃＳＩＤＨ）公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図１２Ｂ】[0030]可換性超特異同種写像ディフィー－ヘルマン鍵交換（ｃＳＩＤＨ）公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図１２Ｃ】[0030]可換性超特異同種写像ディフィー－ヘルマン鍵交換（ｃＳＩＤＨ）公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図１２Ｄ】[0030]可換性超特異同種写像ディフィー－ヘルマン鍵交換（ｃＳＩＤＨ）公開鍵暗号化方式の一実装形態の擬似コード例を示す。

【図１２Ｄ】[0031]１人又は複数の受信者に送信される単一メッセージの暗号文圧縮の一

実装形態の擬似コード例を示す。
【発明を実施するための形態】
【００１５】
詳細な説明
［0032］本発明の種々の実施形態を本明細書に示し、説明するが、そのような実施形態は、単なる例として提供されることが当業者に明らかになるであろう。本発明から逸脱することなく、多くの変形形態、変更形態及び置換形態が当業者に想到され得る。本明細書に記載の本発明の実施形態への種々の代替形態が採用され得ることを理解されたい。
【００１６】
［0033］「少なくとも」、「よりも大きい」又は「以上」という用語が２つ以上の一連の数値中の最初の数値に先行する場合には常に、「少なくとも」、「よりも大きい」又は「以上」という用語は、その一連の数値中の各数値に適用される。例えば、１、２、３以上は、１以上、２以上又は３以上と均等である。
【００１７】
［0034］「超えない」、「未満」又は「以下」という用語が２つ以上の一連の数値中の最初の数値に先行する場合には常に、「超えない」、「未満」又は「以下」という用語は、その一連の数値中の各数値に適用される。例えば、３、２又は１以下は、３以下、２以下又は１以下と均等である。
【００１８】
［0035］本明細書で使用される場合、「暗号文」という用語は、一般に、暗号化されたテキストを指す。暗号化は、アルゴリズムによって実行される暗号化であり得る。テキストは、数字（例えば、二進表現）、文字、単語等、又はそれらの任意の組合せであり得る。暗号文は、暗号化された平文であり得る。暗号文は、暗号化されたメッセージであり得る。マルチ暗号文は、同じパッケージ中の１つ又は複数の暗号文であり得る。
【００１９】
［0036］本明細書で使用される場合、「公開鍵」という用語は、一般に、暗号化に使用される暗号鍵を指す。公開鍵は、秘密に保たれなくてよい。公開鍵は、ユーザ（例えば、メッセージを送信するユーザ）、サービス（例えば、適宜構成されたコンピュータで実行中のソフトウェア）又は暗号化されたオブジェクトの他の任意の送信者／受信者によりアクセス可能である。公開鍵は、平文を暗号化して暗号文にするために使用され得る。例えば、ユーザであるアリスは、ユーザであるボブの公開鍵を使用して平文を暗号化することができ、その暗号文は、ボブによってのみ復号可能である。
【００２０】
［0037］本明細書で使用される場合、「秘密鍵」という用語は、一般に、復号に使用される暗号鍵を指す。秘密鍵は、ユーザ（例えば、メッセージを送信するユーザ）、サービス（例えば、適宜構成されたコンピュータで実行中のソフトウェア）又は暗号化されたオブジェクトの他の任意の送信者／受信者に対して秘密にされ得る。秘密鍵は、暗号文を復号して平文にするために使用され得る。
【００２１】
［0038］本明細書で使用される場合、「暗号化方式」という用語は、一般に、暗号化及び復号の方法を指す。暗号化方式は、格子に基づく方式であり得る。暗号化方式の例は、公開鍵暗号化、対称鍵暗号化（例えば、高度暗号化標準（ＡＥＳ））、Round5、Saber、NewHope、Kyber、FrodoKEM及び超特異同種写像鍵カプセル化であり得る。暗号化方式は、鍵カプセル化メカニズム（ＫＥＭ）であり得る。暗号化方式は、コードに基づく暗号化方式であり得る。コードに基づく暗号化方式の例は、BIKE-3、ROLLO-3、HQC、RQC等であり得る。格子に基づく、コードに基づく又は他の暗号化方式の他の例は、National Institutes for Standards and Testing (NIST) Post-Quantum Cryptography project files、例えば２０１９年１月３１日に発行されたAlagicらによる「Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process」（DOI: 10.6028/NIST.IR.8240）に見出すことができ、これは、全体的

に参照により本明細書に援用される。暗号化方式は、公開鍵暗号化方式（ＰＫＥ）であり得る。

【００２２】

［0039］ マルチ暗号文は、暗号文圧縮方式を実施するにあたって使用され得る。例えば、マルチ暗号文を使用して、鍵交換中に送信されるデータ量を削減することは、暗号文圧縮であり得る。したがって、これらの用語は、本開示全体を通して関連し得る。マルチ暗号文は、複数の暗号文を含み得る。

【００２３】

［0040］ 本開示は、複数の暗号化部分を含む暗号文を複数のユーザに送信する方法及びシステムを提供する。複数の暗号化部分を含む暗号文を複数のユーザに送信する方法は、複数のユーザのシステムパラメータの共通セットを提供することを含み得る。複数の暗号化部分は、複数のユーザの各ユーザに一意のパラメータを使用して平文を暗号化することによって生成され得る。システムパラメータの共通セットから導出される部分及び複数の暗号化部分を含む暗号文は、複数のユーザに送信され得る。複数の暗号文は、少なくとも部分的に、前記複数のユーザの各ユーザに一意のパラメータを使用して復号可能であり得る。

【００２４】

［0041］ 図１は、複数の暗号文を複数のユーザに送信する一例のプロセス１００のフローチャートを示す。動作１１０において、プロセス１００は、システムパラメータの共通セットを複数のユーザに提供することを含み得る。複数の暗号文は、少なくとも約２、３、４、５、６、７、８、９、１０、５０、１００、２５０、５００、１，０００、５，０００、１０，０００、５０，０００、１００，０００、５００，０００、１，０００，０００又は１，０００，０００超の暗号文であり得る。複数の暗号文は、最大で約１，０００，０００、５００，０００、１００，０００、５０，０００、１０，０００、５，０００、１，０００、５００、２５０、１００、５０、１０、９、８、７、６、５、４、３、２つ又は２つ未満の暗号文であり得る。複数のユーザ中のユーザ数は、複数の暗号文中の暗号文数よりも多数であるか、それと等しいか又はそれよりも少数であり得る。例えば、１，０００人のユーザに送られる５００の暗号文を生成することができる。複数のユーザは、例えば、サーバクライアント（例えば、サーバから更新を受信するクライアントデバイス、更新を受信し、他のクライアントに伝える等の中間サーバ）、メッセージング受信者、ウェブサイト訪問者、システム受信ソフトウェア更新等であり得る。メッセージング受信者は、デジタルメッセージ（例えば、電子メール、ショートメッセージサービス（ＳＭＳ）、マルチメディアメッセージングサービス（ＭＭＳ））の受信者であり得る。ソフトウェア更新を受信するシステムは、サーバデバイス（例えば、計算クラスタ）、エンドユーザデバイス（例えば、ラップトップコンピュータ、デスクトップコンピュータ、スマートフォン、タブレット）等であり得る。例えば、中央サーバは、複数のサーバノードによって受信される更新を出力することができる。別の例では、デスクトップコンピュータは、ピアツーピア更新を別のデスクトップコンピュータに出力することができる。暗号文は、格子に基づく暗号化方式、同種写像に基づく暗号化方式（例えば、超特異同種写像に基づく暗号化方式）、素因数分解に基づく暗号化方式、本明細書の他の箇所に記載の別の暗号化方式等であり得る。暗号化方式は、量子後暗号化方式（例えば、非古典的コンピュータによる攻撃に対してより強靭な方式）であり得る。暗号化方式は、量子前暗号化方式（例えば、現在利用されている暗号化方式）であり得る。暗号化方式は、選択暗号文攻撃（ＣＣＡ）セキュリティレベルで動作し得る。暗号化方式は、選択平文攻撃（ＣＰＡ）セキュリティレベルで動作し得る。

【００２５】

［0042］ システムパラメータの共通セットは、複数のユーザのうちのユーザの公開鍵に依存しなくてもよい。例えば、システムパラメータの共通セットは、複数のユーザの各ユーザに共通であり得る。システムパラメータの共通セットは、暗号文の生成に使用される暗号化方式のタイプに関連し得る。例えば、同種写像に基づく暗号化方法では、システム

パラメータの共通セットは、大きい整数であり得る。別の例において、システムパラメータの共通セットは、数字又は多項式を含む１つ又は複数の行列であり得る。システムパラメータの共通セットは、暗号化方式のインスタンスの詳細な説明を提供し得る。例えば、格子に基づく暗号化方式のシステムパラメータの共通セットは、素因数分解に基づく暗号化方式のパラメータの共通セットと異なり得る。別の例において、システムパラメータは、テンプレートとして使用する暗号化方式の一例であり得る。システムパラメータの共通セットの少なくとも１つのパラメータは、シード及び疑似乱数生成器を使用して生成され得る。例えば、暗号文として暗号化されるメッセージは、数値シードに変換され、疑似乱数生成器に供給されてシステムパラメータを生成し得る。システムパラメータの共通セットは、圧縮され得る。圧縮は、非可逆的圧縮又は可逆的圧縮であり得る。例えば、下位ビットを落として１つ又は複数のパラメータのサイズを低減し得る。システムパラメータの共通セットは、本明細書の他の箇所ではＡとして表され得る。

【００２６】

[0043] 別の動作１２０において、プロセス１００は、複数のユーザの各ユーザに一意のパラメータを使用して平文を暗号化することにより、複数の暗号化部分を生成することを含み得る。複数のユーザの各ユーザに一意のパラメータは、１つ又は複数の公開鍵を含み得る。例えば、ユーザであるアリスは、ユーザであるボブの公開鍵を使用してボブへのメッセージを暗号化することができ、アリスからボブに送信される暗号文は、暗号化されたメッセージを含む。公開鍵は、１つ又は複数の暗号鍵、１つ又は複数の検証鍵、１つ又は複数の識別番号等、又はそれらの任意の組合せを含み得る。暗号文は、固定部分及び可変部分を含み得る。固定部分は、システムパラメータの共通セットに依存し得る。固定部分は、複数のユーザの各ユーザで同じであり得る。固定部分は、本明細書の他の箇所でＵと呼ばれ得る。可変部分は、システムパラメータの共通セット及び複数のユーザの各ユーザに一意のパラメータ（例えば、複数のユーザの各ユーザの公開鍵）に従属し得る。可変部分は、本明細書の他の箇所でＶと呼ばれ得る。複数のユーザの各ユーザに一意のパラメータの少なくとも１つのパラメータは、シード及び疑似乱数生成器を使用して生成され得る。例えば、ユーザの公開鍵を含むシードを疑似乱数生成器に入力して、ユーザに一意のパラメータを生成し得る。別の例では、シードを疑似乱数生成器に入力して、ユーザの公開鍵を生成することができる。システムパラメータの共通セットは、１つ又は複数の非正方行列を含み得る。複数のユーザの各ユーザに一意のパラメータは、１つ又は複数の非正方行列を含み得る。非正方行列は、数字、多項式、他の方程式等を含み得る。暗号化することは、本明細書の他の箇所に記載される暗号化方式によって暗号化することであり得る。複数のユーザの各ユーザに一意のパラメータは、本明細書の他の箇所で公開鍵と呼ばれ得る。

【００２７】

[0044] 別の動作１３０において、プロセス１００は、システムパラメータの共通セットから導出された部分及び複数の暗号化部分を含む暗号文を生成することを含み得る。別の動作１４０において、プロセス１００は、暗号文を複数のユーザに送信することを含み得る。複数の暗号文は、少なくとも部分的に、複数のユーザの各ユーザに一意のパラメータを使用して復号可能であり得る。複数の暗号文を結合して単一のマルチ暗号文にし得る。例えば、単一の送信は、複数の暗号文を含むことができる。送信は、通信プロトコル（例えば、インターネットプロトコル（ＩＰ）、伝送制御プロトコル（ＴＣＰ）、ハイパーテキスト転送プロトコル（ＨＴＴＰ）又はそのセキュアバリアント（ＨＴＴＰＳ）等）を経由し得る。送信は、図１０Ａ～図１０Ｅのいずれかに示されるような方式であり得る。送信は、システムパラメータの共通セット及び複数の暗号文をディストリビュータに送信することを含み得、ディストリビュータは、システムパラメータの共通セット及び複数の暗号文のうちの１つの暗号文を複数のユーザの各ユーザに送信し得る。

【００２８】

[0045] システムパラメータの共通セットは、少なくとも部分的に確率分布によって生成され得る。パラメータの生成に確率分布を使用することは、本明細書に記載の方法及び

システムに追加のセキュリティを付与し得る。確率分布は、確率分布を使用して生成されたパラメータが、パラメータ∈Ｒであるように有限環Ｒ（ここで、Ｒは、Ｒ＝Ｚ$_{q}$又はＲ＝Ｚ$_{q}$／ｍを満たすことができ、式中、Ｚ$_{q}$は、整数のモジュロｑであり、ｍは、モニック多項式である）にあるようなものであり得る。

【００２９】

［0046］本開示は、暗号文を複数のユーザに送信する方法及びシステムを提供する。暗号文を複数のユーザに送信する方法は、システムパラメータセットを生成することを含み得る。システムパラメータセットは、複数のユーザのうちのユーザの公開鍵に依存しないパラメータを含み得る。システムパラメータセットに少なくとも部分的に基づいて固定成分を生成し得る。複数のユーザの各公開鍵を使用して平文を暗号化することにより、複数の可変成分を生成し得る。暗号化は、リンドナー－ペイカート方式、超特異同種写像ディフィー－ヘルマンプロトコル及び同種写像に基づく公開鍵暗号化方式からなる群から選択される暗号化方式に基づき得る。固定成分及び可変成分を含む暗号文は、複数のユーザに送信され得る。暗号文は、少なくとも部分的に固定成分を使用して復号可能であり得る。暗号文は、マルチ暗号文であり得る。

【００３０】

［0047］本開示は、データベースを編成する方法及びシステムを提供する。データベースを編成する方法は、項数「ｍ」のツリー構造で複数の受信者を構造化することを含み得る。項数「ｍ」は、少なくとも２であり得る。圧縮暗号文更新は、複数の受信者の全て未満に送信され得る。

【００３１】

［0048］図２は、複数の暗号文を複数のユーザに送信する一例のプロセス２００のフローチャートである。動作２１０において、プロセス２００は、項数ｍのツリー構造で複数の受信者を構造化することを含み得る。項数は、ツリーのノードが有することができる子ノードの最大数であり得る。例えば、項数４のツリーは、１ノード当たり最大で４つの子ノードを有する。例は、項数２のツリーを示す図１０Ｄ及び項数４のツリーを示す図１０Ｅにおいて見られ得る。項数「ｍ」は、少なくとも約１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４、１５、１６、１７、１８、１９、２０、２１、２２、２３、２４、２５、５０、１００、２５０、５００、１，０００又は１，０００超であり得る。項数「ｍ」は、最大で約１，０００、５００、２５０、１００、５０、２５、２４、２３、２２、２１、２０、１９、１８、１７、１６、１５、１４、１３、１２、１１、１０、９、８、７、６、５、４、３、２、１又は１未満であり得る。項数「ｍ」は、上記の任意の２つの点によって画定される範囲中にあり得る。例えば、ツリーは、項数８～１６であり得る。複数の受信者は、ツリーの他のノードであり得る。ツリーの他のノードは、それら自体の子ノードを有し得る。例えば、図１０Ｅのノード１からの更新の複数の受信者は、ノード２、３及び４並びにノード１８、１９及び２０を含むノードであり得る。ツリー構造のノードは、そのノード又はそのノードの任意の子ノードの暗号化に使用される情報を収容するように構成され得る。

【００３２】

［0049］別の動作２２０において、プロセス２００は、複数の受信者の全て未満に圧縮暗号文更新を送信することを含み得る。送信は、ネットワークを経由する送信であり得る。ネットワークは、公衆ネットワーク（例えば、インターネット）又は私設ネットワーク（例えば、ローカルネットワーク）であり得る。圧縮暗号文更新は、本明細書の他の箇所に記載の方法及びシステムによって生成され得る。圧縮暗号文更新は、格子に基づく暗号化方式、同種写像に基づく暗号化方式等を使用して暗号化され得る。圧縮暗号文更新を送信するためのバイト数は、複数の受信者の各々に更新を送信するためのバイト数よりも少なくとも約１／１．１、１／１．２、１／１．３、１／１．４、１／１．５、１／１．６、１／１．７、１／１．８、１／１．９、１／２、１／２．５、１／３、１／３．５、１／４、１／４．５、１／５、１／５．５、１／６、１／６．５、１／７、１／７．５、１／８、１／８．５、１／９、１／９．５、１／１０、１／１１、１／１２、１／１３、１

／１４、１／１５、１／１６、１／１７、１／１８、１／１９、１／２０、１／２１、１／２２、１／２３、１／２４、１／２５又はそれ以上すくなくてもよい。圧縮暗号文更新を送信するためのバイト数は、複数の受信者の各々に更新を送信するためのバイト数よりも最大で約１／２５、１／２４、１／２３、１／２２、１／２１、１／２０、１／１９、１／１８、１／１７、１／１６、１／１５、１／１４、１／１３、１／１２、１／１１、１／１０、１／９．５、１／９、１／８．５、１／８、１／７．５、１／７、１／６．５、１／６、１／５．５、１／５、１／４．５、１／４、１／３．５、１／３、１／２．５、１／２、１／１．９、１／１．８、１／１．７、１／１．６、１／１．５、１／１．４、１／１．３、１／１．２、１／１．１又はそれ未満であってよい。

【００３３】

［0050］ 送信は、ツリー構造の各ノードに同じメッセージを送信することを含み得る。メッセージは、データベースのユーザの鍵の更新情報を含み得る。例えば、ユーザは、鍵更新をツリー構造の各ノードに送信することができる。別の例において、ユーザは、圧縮暗号文を使用して鍵更新をツリーの特定のレベルの各ノードに送信することができる。メッセージは、本明細書の他の箇所に記載されるようなメッセージ（例えば、テキストメッセージ、ソフトウェア更新、暗号鍵更新）であり得る。送信は、ツリー構造の各ノードに異なるメッセージを送信することを含み得る。例えば、異なる暗号化メッセージをユーザから複数の他のユーザの各々に送信することができる。送信は、幾つかの異なるメッセージをツリー構造のノード数未満のツリー構造の各ノードに送信することを含み得る。例えば、特定の深度の各ノードは、同じメッセージを受信することができる。この例では、項数４及び深度２のツリーは、同じ親ノードの子である３つのノードに送信される１つのメッセージ及び親ノードと親を共有するノードに送信される別のメッセージを有することができ、合計で６つの更新が送信される。この例において、暗号文圧縮方式を使用せずに送信される場合の１５の代わりに６つの更新を送信することにより、圧縮暗号文更新を送信するためのバイト数は、受信者の各々に更新を送信するためのバイト数の１／（１５／６）＝１／２．５である。別の例において、子ノードがノードのパス中の復号鍵にアクセスすることができる項数４及び深度２のツリーは、図１０Ｅのノード１７及び２１等の２つのノードにマルチ暗号文を送信することによって更新することができる。この例において、通信コストは、複数のノードの各ノードに更新を送信することと比較して１／（１５／２）＝１／７．５に改善することができる。送信は、ｄ個の暗号文をマルチ暗号文で送信することを含み得、ここで、$d = \log_m N$であり、式中、ｍは、ツリーの項数であり、Ｎは、受信者（例えば、ユーザ）ノードの数である。

【００３４】

［0051］ 本開示は、複数の暗号鍵及び複数のマルチ暗号文を含む暗号化更新を複数の受信者ノードに対して実行する方法及びシステムを提供する。複数の暗号鍵及び複数のマルチ暗号文を含む暗号化更新を複数の受信者ノードに対して実行する方法は、暗号化更新を受信することを含み得る。複数の暗号鍵のうちの１つ又は複数と、複数のマルチ暗号文の１つ又は複数の暗号文とを除去することにより、縮小暗号化更新を生成し得る。縮小暗号化更新は、複数の受信者ノードの受信者ノードに送信され得る。動作は、複数のノードのうちの１つ又は複数の他のノードについて繰り返され得る。

【００３５】

［0052］ 図３は、複数の暗号鍵及び複数のマルチ暗号文を含む暗号化更新を複数の受信者ノードに対して実行する一例のプロセス３００のフローチャートである。動作３１０において、プロセス３００は、暗号化更新を受信することを含み得る。暗号化更新は、複数の暗号鍵及び／又は複数のマルチ暗号文を含み得る。暗号化更新は、暗号鍵ペアの半分、暗号化メッセージ又は２進数若しくは１６進数文字列として表現可能な任意のデータ等の情報を含み得る。暗号化更新は、１つ又は複数の送信デバイスから受信され得る。１つ又は複数の送信デバイスは、計算デバイス（例えば、サーバ、モバイルデバイス、計算デバイス等）であり得る。例えば、ユーザのスマートフォンは、暗号化更新を送信することができる。暗号化更新は、適宜プログラムされたコンピュータ（例えば、サーバコンピュー

タ）によって受信され得る。例えば、ユーザのラップトップは、暗号鍵更新をセキュアメッセージングサーバに送信することができる。送信デバイスは、複数の受信者ノードと同じタイプであり得る。例えば、送信デバイスは、スマートフォンであり得、受信者ノードも同様にスマートフォンであり得る。送信デバイスは、複数の受信者ノードの少なくとも幾つかのノードと同じタイプであり得る。例えば、送信デバイスは、スマートフォンであり得、受信者ノードは、他のスマートフォン及びサーバノードであり得る。

【００３６】

［0053］暗号化更新は、墨塗り署名を用いて署名され得る。墨塗り署名は、署名を損なわずに又は１つ若しくは複数のデータブロックを発効させずに、暗号化更新中の１つ又は複数のデータブロックに対する動作を許容するように構成され得る。動作は、書き換え、修正、削除、追加等、又はそれらの任意の組合せであり得る。例えば、墨塗り署名を用いて署名された複数の暗号文を含むマルチ暗号文は、署名を維持しながら、複数の暗号文の暗号文を削除させることができる。ユーザ又は暗号化更新を生成するシステムは、署名に影響せずに変更可能な暗号化更新の部分、署名に影響せずに可能な動作等、又はそれらの任意の組合せを示し得る。例えば、システムは、署名に影響せずに削除可能なデータブロックを示すことができる。暗号文は、格子に基づく暗号化方式を使用して暗号化され得る。１つ又は複数の暗号文は、本明細書の他の箇所で記載のように暗号化された（例えば、格子に基づく暗号化方式を使用して生成され、同種写像に基づく暗号化方式を使用して生成された）暗号文であり得る。墨塗り署名は、偽造不可能、変更不可能又はそれらの組合せであり得る。墨塗り署名は、プライベート、トランスペアレント、アカウンタブル又はそれらの任意の組合せであり得る。墨塗り署名は、代わりに、削除可能署名であり得る。墨塗り署名は、マークルツリーに基づき得る。

【００３７】

［0054］別の動作３２０において、プロセス３００は、複数の暗号鍵の１つ又は複数と複数のマルチ暗号文の１つ又は複数の暗号文とを除去することにより、縮小暗号化更新を生成することを含み得る。除去は、署名に影響せずに実行され得る。墨塗り署名は、複数の暗号鍵及び複数のマルチ暗号文の１つ又は複数の除去を促進し得る。例えば、墨塗り署名を用いた暗号化更新は、署名に影響せずに変更することができる一方、墨塗り署名を用いない暗号化更新は、署名に影響せずに変更することができない。除去は、暗号化更新の受信者によって実行され得る。例えば、ホストサーバは、ユーザから受信した更新からブロックを除去することができる。除去は、暗号鍵の１つ若しくは複数及び／又はマルチ暗号文の１つ若しくは複数の暗号文を除去することを含み得る。１つ又は複数の暗号文は、その１つ又は複数の暗号文を必要としない受信者ノードへの更新から除去され得る。例えば、ノードＡ、Ｂ及びＣの更新を含むマルチ暗号文では、サーバは、Ａに送信される縮小暗号化更新からＢ及びＣの更新を除去することができる。１つ又は複数の暗号文の除去は、受信者ノードに送信される更新サイズを低減し得る。複数のノードに送信されるバイト数は、複数の受信者ノードの各ノードに更新を送信するために使用され得るバイト数と比較して少なくとも約１／ｎに低減され得、ここで、ｎは、複数のノード中のノード数である。複数のノードに送信されるバイト数は、複数の受信者ノードの各ノードに更新を送信するために使用し得るバイト数と比較して最大で約１／ｎに低減され得、ここで、ｎは、複数のノード中のノード数である。複数のノードに送信されるバイト数は、複数の受信者ノードの各ノードに更新を送信するために使用され得るバイト数と比較して少なくとも約１／１．１、１／１．２、１／１．３、１／１．４、１／１．５、１／１．６、１／１．７、１／１．８、１／１．９、１／２、１／２．５、１／３、１／３．５、１／４、１／４．５、１／５、１／５．５、１／６、１／６．５、１／７、１／７．５、１／８、１／８．５、１／９、１／９．５、１／１０、１／１１、１／１２、１／１３、１／１４、１／１５、１／１６、１／１７、１／１８、１／１９、１／２０、１／２１、１／２２、１／２３、１／２４、１／２５又はそれ以上低減され得る。複数のノードに送信されるバイト数は、複数の受信者ノードの各ノードに更新を送信するために使用され得るバイト数と比較して最大で約１／２５、１／２４、１／２３、１／２２、１／２１、１／２０、１／

１９、１／１８、１／１７、１／１６、１／１５、１／１４、１／１３、１／１２、１／１１、１／１０、１／９．５、１／９、１／８．５、１／８、１／７．５、１／７、１／６．５、１／６、１／５．５、１／５、１／４．５、１／４、１／３．５、１／３、１／２．５、１／２、１／１．９、１／１．８、１／１．７、１／１．６、１／１．５、１／１．４、１／１．３、１／１．２、１／１．１又はそれ未満に低減され得る。

【００３８】

［0055］ 別の動作３３０において、プロセス３００は、縮小暗号化更新を複数の受信者ノードの受信者ノードに送信することを含み得る。受信者ノードは、暗号化更新を復号し得る。受信者ノードは、１つの暗号鍵及び１つの暗号文を受信し得る。マルチ暗号文の１つ又は複数の暗号文は、複数のノードの全てに送信されなくてよい。例えば、３つのノードを有するシステムでは、マルチ暗号文中に３つの暗号文を有する更新は、３つの単一の暗号文更新に分割することができる。この例において、各ノードは、３つのうちの１つの特定の暗号文を受信することができ、したがってマルチ暗号文の全ての暗号文が複数のノードの全てのノードに送信されるわけではない。縮小暗号文は、公衆ネットワーク（例えば、インターネット）、プライベートネットワーク（例えば、仮想プライベートネットワーク（ＶＰＮ）、ローカルネットワーク）等を経由して送信され得る。縮小暗号文は、依然として有効な署名を含み得る。

【００３９】

［0056］ 別の動作３４０において、プロセス３００は、複数のノードのうちの１つ又は複数の他のノードについて動作３２０～３３０を繰り返すことを含み得る。動作３４０は、複数のノードの各ノードに対して略同時に実行され得る。動作３４０は、暗号鍵更新をサーバ全体に提供し得る。各ノードは、複数の暗号鍵のうちの１つの暗号鍵と、マルチ暗号文のうちの１つの暗号文とを含む縮小暗号化更新を受信し得る。例えば、サーバは、複数の暗号鍵及びマルチ暗号文を単一の暗号鍵及び単一の暗号文に縮小してノードに送信することができる。複数のノードの各ノードは、複数のノードの他の各ノードから、複数の暗号鍵のうちの異なる暗号鍵と、マルチ暗号文のうちの異なる暗号文とを含む縮小暗号化更新を受信し得る。例えば、暗号化更新（Ｕ，$Ｖ_1$，$Ｖ_2$）の場合、ノード１は、（Ｕ，$Ｖ_1$）を受信することができ、ノード２は、（Ｕ，$Ｖ_2$）を受信することができる。受信者ノードは、１つ又は複数の子ノードを有し得る。子ノードは、ツリー構造の子ノードであり得る。子ノードは、したがって、１つ又は複数の追加の子ノードを有し得る。例えば、図１０Ｅのノード５、６、７及び８は、ノード１８の子ノードであり得る。子ノードは、受信者ノードに記憶された１つ又は複数のパラメータへのアクセスを有し得る。子ノードは、子ノードのパス中の各受信者ノードの復号鍵にアクセス可能であり得る。

【００４０】

［0057］ 図４Ａ～図４Ｃは、リンドナー－ペイカート（ＬＰ）枠組みの一例を示す。リンドナー－ペイカート枠組みの更なる詳細は、Richard Lindner及びChris Peikertによる「Better key sizes (and attacks) for LWE-based encryption」；In Aggelos Kiayias, editor, CT-RSA 2011, volume 6558 of LNCS, pages 319-339. Springer, Heidelberg, February 2011に見出すことができ、これは、全体的に参照により援用される。ＬＰ枠組みは、幾つかの暗号化方式を解釈するための枠組みとして使用され得る。ＬＰ枠組みは、本明細書において暗号文圧縮方法を説明するための好都合な枠組みを提供し得る。図４Ａは、暗号鍵ｅｋ及び復号鍵ｄｋの生成に使用することができる一例の関数keygen()を示す。Ｄ＊関数は、本明細書の他の箇所に記載されるような確率分布関数であり得ある。確率分布を使用して無作為性を導入するにあたり、ＬＰ枠組みは、量子コンピュータに基づく攻撃に対してより強靭になり得る。確率分布を使用して複数のパラメータＡ、Ｓ及びＥを生成することができ、結合してパラメータＢを形成することができる。ここでは正方行列として示されているが、パラメータＡは、非正方であり得る。方式は、他の行列（例えば、Ｓ、Ｅ）の寸法を適合することによって機能的なままであり得る。図４Ｂにおいて、図４Ａの式において生成されたパラメータを使用してメッセージｍｓｇを暗号化し得る。暗号化メッセージは、Ｖによって表され得る一方、公開鍵に関連しない１つ

又は複数のシステムパラメータは、Ｕによって表され得る。暗号文は、Ｕ及びＶの両方を含み得る。例えば、符号化メッセージと共に幾つかのシステムパラメータを連結して、単一の暗号文にすることができる。図４Ｃは、図４Ｂにおいて生成された暗号文の復号プロセスを示す。

【００４１】

［0058］ ＬＰ枠組みを改良するために、ＬＰ枠組みに幾つかの変更を行い得る。１つの変更は、生成器に通して１つ又は複数の要素を再編纂することができるシードとして要素の１つ又は複数を表すことにより、図４Ａ～図４Ｃの要素（例えば、Ａ、Ｓ、Ｅ、Ｂ、Ｒ、Ｅ’、Ｅ’’、Ｕ及びＶ）のよりコンパクトな表現を可能にすることであり得る。生成器は、疑似乱数生成器であり得る。例えば、Ａは、乱数生成器に入力されると、完全行列Ａを生成するシードとして表すことができる。シードは、別の要素であり得る。例えば、公開鍵ｅｋは、要素Ａのシードとして使用することができる。別の例において、平文メッセージｍｓｇを要素Ｓのシードとして使用することができる。圧縮は、要素の１つ又は複数に適用され得る。圧縮は、非可逆的又は可逆的であり得る。例えば、非可逆的圧縮は、下位ビットを落とすことにより、要素Ｂ、Ｕ及びＶに適用することができる。圧縮の適用は、要素のサイズ、したがって要素が関わる任意の更新のサイズを低減し得る。

【００４２】

［0059］ 図４Ｄは、１人又は複数の受信者に送信される単一のメッセージの暗号文圧縮の一実装形態の擬似コードの一例を示す。各ユーザｋで共通のＡ要素を採用することにより、Ａ要素の数を１／ｋに低減し得る。Ａ要素のこの再使用は、シードからＡを生成することと同等であり得る。Ａを再使用することにより、同じＲ及びＥ’は、ｋユーザの各々で使用され得る。これらの２つの変更を図４Ｂの復号プロセスに適用することにより、マルチ暗号文を生成する新しいプロセスが続き得る。マルチ暗号文は、ｋ人の別個のユーザへの同じメッセージｍｓｇを同時に暗号化し得る。マルチ暗号文（Ｕ、V_i）は、図４Ｃと同じ復号アルゴリズムを使用して、ｋ人のユーザの各ユーザｉによって復号され得る。ｋ人のユーザの各々に対してシステムパラメータＵを再使用することにより、マルチ暗号文の総通信コストは、｜Ｕ｜＋｜Ｖ｜であり得、ここで、｜ｘ｜は、ｘのバイトサイズであり得る。逆に、ｋ個の暗号文を送信することの総通信コストは、ｋ・（｜Ｕ｜＋｜Ｖ｜）であり得る。多くのユーザｋがいる場合、マルチ暗号文の使用は、総通信コストを約

【数１】

$$\frac{|U|+|V|}{|V|}$$

分の１に低減し得る。総通信コストの削減は、｜Ｕ｜＞＞｜Ｖ｜の場合、より高くなり得る。種々の暗号化方式での性能の改善は、図８に見られ得る。

【００４３】

［0060］ 一例において、図４Ｄのプロセスは、１つ又は複数のシステムパラメータＡ、ｋ人のユーザの各ユーザｉへの１つ又は複数の暗号鍵$ek_i = B_i$及び共通メッセージｍｓｇを提供することで開始し得る。図４Ｄのプロセス例は、分布関数からパラメータＲ及びＥ’を生成することで開始し得る。パラメータＲ、Ｅ’及びＡ（例えば、各ユーザに再使用可能なシステムパラメータ）は、Ｕ←ＲＡ＋Ｅ’であるように結合され得る。パラメータＵは、複数のユーザの各ユーザによって使用可能な情報（例えば、ユーザの公開鍵に依存しない情報）を含み得る。ｋ人のユーザの各ユーザｉについて、パラメータE_i''を別の分布関数から生成し得、$V_i \leftarrow RB_i + E_i'' + \mathrm{Encode}(msg)$ように使用し得る。これは、ｉ$V_i$を生成し得、これは、次いで、ｍｃｔｘｔ：＝（Ｕ，$V_0$，．．．，$V_{k-1}$）であるようにパラメータＵと連結することができ、ここで、ｍｃｔｘｔは、マルチ暗号文であり得る。マルチ暗号文は、Ｕのサイズにｖのサイズのｋ倍を加えたものに等しいサイズを有し得る。

【００４４】

［0061］ 図５Ａは、１人又は複数の受信者に送信される１つ又は複数のメッセージでの

暗号文圧縮の一実装形態の疑似コード例を示す。図５Ａの例は、図４Ｄの例のマルチメッセージ類似物であり得る。図５Ａにおいて、図４Ｄの単一メッセージｍｓｇは、ｋ人のユーザの各ユーザｉで異なるメッセージmsg_iで置換され得る。プロセスは、他の点で同様であり得、本明細書の他の箇所に記載されるものと同様の傾向に従い得る。違いは、各メッセージmsg_iが異なるサイズを有し得るため、｜Ｖ｜が一定でないことがあることである。

【００４５】

[0062] 図５Ｂ～図５Ｄは、超特異同種写像鍵暗号化（ＳＩＫＥ）公開鍵暗号化方式の一実装形態の擬似コード例を示す。図５Ｂ～図５Ｄは、ＳＩＫＥ提出パッケージの一環として、National Institute of Standards and Technologyにより２０１９年３月３１日に発行されたDavid JaoらによるSupersingular Isogeny Key Encapsulation specification（参照により本明細書に援用される）に記載のＳＩＫＥ方式に基づき得る点で図４Ａ～図４Ｃと異なり得る。図５Ｂにおいて、秘密（又は復号鍵）Ｓを生成するために、鍵空間K_Aのランダムメンバーを選択し得る。次いで、同種写像アルゴリズムisogenを使用してＳの同種写像を計算して、Ｐ、即ち公開（又は暗号）鍵を生成し得る。図５Ｃにおいて、s_Bを鍵空間K_Bから生成することができる。そこから同種写像アルゴリズムisogenにより計算されたs_Bの同種写像から、パラメータＵ（例えば、ユーザの公開鍵に依存しないパラメータ）を生成することができる一方、別の同種写像アルゴリズムであるisoexは、暗号鍵Ｐ及びs_Bから共有鍵ｊを生成することができ、共有鍵ｊを生成するプロセスは、図９に更に詳細に見ることができる。関数Ｈは、共有鍵ｊをビット文字列に写像することができ、次いでメッセージｍｓｇへの排他的ＯＲ演算子を用いてこれに作用してＶを返し得る。暗号文は、方程式ｃｔｘｔ：＝（Ｕ，Ｖ）に示すようにＵ及びＶを連結することによって生成され得る。復号プロセスは、図５Ｄに見出され得、同じ同種写像アルゴリズムisoexは、パラメータＵ及び復号鍵Ｓを利用して同じ共有鍵ｊを生成し得、したがってそれを使用してＶからメッセージｍｓｇを復号し得る。

【００４６】

[0063] 図６Ａは、１人又は複数の受信者に送信された１つのメッセージのＳＩＫＥ公開鍵暗号化方式での暗号文圧縮の一実装形態の擬似コード例を示す。図６Ａのコードは、図４Ｄの例のＳＩＫＥ類似物であり得る。違いは、図６Ａが、図５Ｂ～図５Ｄに記載のような同種写像に基づく暗号化方式での暗号文圧縮の一実装形態を示すことであり得る。図５Ｃと図６Ａとの間のプロセスの違いは、幾人かのユーザｋがそれぞれメッセージｍｓｇを受信することであり得る。パラメータＵは、ユーザ非依存であり得る（例えば、特定のユーザに関連するいかなるパラメータにも依存しない）。したがって、Ｕは、ｋ人のユーザの各ユーザｉに対して再使用され得る。パラメータＶは、ユーザ非依存でなくてもよく（例えば、特定のユーザに関連するパラメータに依存する）、したがって、各ユーザは、異なるV_iを有し得る。図５Ｃと同様のプロセスに従うが、代わりに複数の暗号鍵P_iを有して、マルチ暗号文$mctxt:=(U, V_0, \ldots, V_{k-1})$を生成することができる。ｋ人のユーザの各ユーザｉは、図５Ｄのプロセスを使用して、マルチ暗号文の暗号文（Ｕ，V_i）を復号し得る。全てのユーザに１つのパラメータを有することにより、マルチ暗号文のサイズは、ｋ・｜Ｕ｜分の１に低減することができ、したがってアルゴリズムが実行されている計算デバイスの効率を改善することができる。

【００４７】

[0064] 図６Ｂは、１人又は複数の受信者に送信された１つ又は複数のメッセージのＳＩＫＥ公開鍵暗号化方式での暗号文圧縮の一実装形態の擬似コード例を示す。図６Ｂの例は、図６Ａの例のマルチメッセージング類似物であり得る。図６Ｂにおいて、図６Ａの単一メッセージｍｓｇは、ｋ人のユーザの各ユーザｉで異なるメッセージmsg_iで置換され得る。各ユーザｉは、マルチ暗号文（$U, V_0, \ldots, V_{k-1}$）の暗号文（Ｕ，V_i）を復号可能であり得る。図６Ｂの例のセキュリティは、図５Ａの例のセキュリティよりも高いレベルであり得る。

【００４８】

[0065] 図１２Ａ～図１２Ｃは、可換性超特異同種写像ディフィー－ヘルマン（ｃＳＩＤＨ）公開鍵暗号化方式の一実装形態の疑似コード例を示す。ｃＳＩＤＨ方式に関する更なる詳細は、Wouter Castryck、Tanja Lange、Chloe Martindale、Lorenz Panny及びJoost Renesによる「CSIDH: An Efficient Post-Quantum Commutative Group Action」、編者Thomas Peyrin及びSteven D. Galbraith、Advances in Cryptology - ASIACRYPT 2018, pages 395-427. Springer International Publishing, 2018に見出され得、これは、全体的に参照により援用される。アルゴリズムは、EI Gamal方式に基づき得る。手短に言えば、ｃＳＩＤＨ方式は、ｃＳＩＤＨ方式が可換であり得る一方、ＳＩＤＨ方式（そのうちのＳＩＫＥは、一実装形態であり得る）は、そうでないことがある点でＳＩＤＨ方式と異なり得る。可換性は、１つ又は複数の動作が実行される順序に対して不変であり得る。例えば、整数乗算は、（２＊３）＊４＝２＊（３＊４）に示されるように可換である。可換でない演算は、非可換であり得る。ｃＳＩＤＨ方式は、素数ｐに基づき得る。素数は、大きい素数（例えば、１，０００，０００よりも大きい値の素数）であり得る。素数のサイズ（例えば、ビット長）は、ｃＳＩＤＨ方式のセキュリティを定義し得る。素数は、$p = 4 \cdot l_1 \cdot l_2 \cdot \ldots \cdot l_r - 1$の形態であり得、式中、$l_i$は、小さい別個の奇数の素数であり得る。素数ｐは、セットS_pを定義し得、これは、楕円曲線方程式$y^2 = x^3 + A \cdot x^2 + x$が、厳密にｐ個の解を有する全ての要素Ａを含むような有限場F_pのサブセットであるように選択され得る。別の群Ｇは、

【数２】

$$Z[\sqrt{-p}]$$

のイデアル類群から生じ得、これは、Ｃｌ（Ｏ）として示され得る。群の要素は、イデアルと呼ばれ得、「α」で表され得る。したがって、可換性群作用は、Ｃｌ（Ｏ）×Ａ→Ａであるように定義され得、式中、Ａは、全ての係数のセットＡ∈F_pであり得る。これは、群Ｃｌ（Ｏ）の要素が同種写像を介して楕円曲線に対して作用し得ることを意味し得る。これにより、ＳＩＤＨの場合と同様に、ある曲線から別の曲線への秘密変換が可能になり得る。そのような演算は、図１２Ａ～図１２Ｄを含め、本明細書において［α］Ｅと示され得る。

【００４９】

[0066] セットアップフェーズにおいて、鍵交換の１人又は複数の当事者（例えば、アリス及びボブ）は、上述したように大きい素数ｐ並びに有限場F_p及び整数Ｂにわたる開始楕円曲線$E_0 : y^2 = x^3 + x$について合意し得る。図１２Ａに示す等の鍵生成フェーズにおいて、第１の当事者（例えば、アリス）は、範囲［－Ｂ，Ｂ］＝Ｍ、即ち別個にサンプリングされた整数のｎタプルをサンプリングし得る。整数は、イデアル類

【数３】

$$[a] = \left(l_1^{e_1}, \ldots, l_n^{e_n}\right) \in \mathrm{Cl}(O)$$

を表し得、式中、l_iは、別個の素イデアルであり得る。公開鍵は、楕円曲線［α］$E_0 : y^2 = x^3 + A \cdot x^2 + x$の係数Ａ∈$F_p$であり得る。

【００５０】

[0067] 図１２Ｂは、図１２Ａにおいて生成されたパラメータを使用し得る符号化アルゴリズムの擬似コード例を示す。アルゴリズムKeygenは、図１２Ａのアルゴリズムであり得る。アルゴリズムKeygenは、ユーザの暗号鍵に依存しないか、ユーザ非依存であるか、又は両方である追加のパラメータＵを生成し得る。図１２Ａの［ａ］及びE_Aと同じ方法でパラメータ［ｂ］及びE_Aも生成され得る。パラメータE_Rは、１人又は複数の当事者間で共有される秘密であり得る。パラメータE_Rは、以下により生成され得る：［ａ］［ｂ］E_0＝［ｂ］［ａ］E_0＝E_R。E_Rは、$y^2 = x^3 + R \cdot x^2 + x$の形態であり得、これは、Ｃｌ（Ｏ）の可換性に起因して全当事者（例えば、アリス及びボブ）で同じ

であり得る。メッセージ及び共有秘密E_Rのハッシュに適用される排他的ＯＲ演算を使用してＶを生成し得る。パラメータＵ及び暗号化メッセージＶの連結により、暗号文ｃｔｘｔ：＝（Ｕ，Ｖ）を生成し得る。暗号文は、図１２Ｃに示すように復号され得る。パラメータE_Uは、パラメータE_Aと同様に生成し得る。

【００５１】

［0068］図１２Ｄは、１人又は複数の受信者に送信される単一メッセージの暗号文圧縮の一実装形態の擬似コード例を示す。図１２Ｄの要素は、図１２Ｂの要素と同じであり得る。単一の受信者の代わりに、図１２Ｄのアルゴリズムは、同じメッセージｍｓｇを複数のユーザｋに送信するように構成され得る。複数のユーザｋの各ユーザｉについて、A_i暗号鍵から異なるE_{A_i}を生成し得る。暗号化方式は、ｉユーザの各々について図１２Ｂでのように続き得、したがってkV_i暗号化メッセージを生成し得る。本明細書の他の箇所で論じられる方法と同じ方法で、暗号化メッセージは、ユーザ非依存であるパラメータＵと連結されて、マルチ暗号文を生成することができる。マルチ暗号文は、本明細書の他の箇所に記載のように墨塗り署名を用いて署名され得る。マルチ暗号文方式の使用は、鍵生成及び鍵交換動作で実行される類群作用計算に関連する演算を低減することにより、コンピュータの性能を改善し得る。類群作用演算は、アルゴリズムの最も計算的にコストのかかる部分であり得、マルチ暗号文方式は、鍵生成を１回実行し得、アルゴリズムの計算コストを半減する。ｃＳＩＤＨ方式を使用したマルチメッセージマルチ暗号文方式は、ＳＩＤＨ又は格子に基づく方式に基づくものよりもセキュアであり得る。ｃＳＩＤＨ方式を使用したマルチメッセージマルチ暗号文方式は、暗号文識別不能性（ＩＮＤ－ＣＰＡ）セキュアであり得る。

【００５２】

［0069］図１２Ｄは、マルチメッセージ方式で実施することもできる。複数のユーザｋのｉユーザの各々で単一のメッセージｍｓｇの代わりに、動作６において複数のメッセージmsg_iを提供することができる。このマルチメッセージマルチ暗号文において、各V_iは、異なるメッセージを含むことができる。

【００５３】

［0070］種々の暗号化方式に関して本明細書に記載したが、本明細書に記載のマルチ暗号文を生成し、使用する方法及びシステムは、特定の暗号化方式に限定されない。本明細書に記載の方法及びシステムは、選択平文攻撃（ＣＰＡ）に対して強靭であり得る。例えば、暗号化される複数の平文を送信し、暗号化された暗号文を受信する能力を有する攻撃者は、秘密鍵を特定することができない。本明細書に記載の方法及びシステムは、１つ又は複数の一般的変換の適用によって選択暗号文攻撃（ＣＣＡ）に対して強靭にされ得る。変換は、一度に複数の受信者を扱うように適合され得る。適合された変換は、復号失敗に対して強靭であり得る。適合された変換は、量子ランダムオラクルモデル（ＱＲＯＭ）においてセキュリティ証明を有し得る。

【００５４】

コンピュータシステム

［0071］本開示は、本開示の方法を実施するようにプログラムされたコンピュータシステムを提供する。図１１は、本明細書の他の箇所に記載の方法を実施するようにプログラム又は他の方法で構成されたコンピュータシステム１１０１を示す。コンピュータシステム１１０１は、例えば、マルチ暗号文の生成、マルチ暗号文を含むメッセージ／更新の配布等の本開示の種々の態様を調整することができる。コンピュータシステム１１０１は、ユーザの電子デバイスであり得るか、又は電子デバイスからリモートに配置されるコンピュータシステムであり得る。電子デバイスは、モバイル電子デバイスであり得る。コンピュータシステム１１０１は、非古典的コンピュータシステム（例えば、量子コンピュータシステム）であり得る。

【００５５】

［0072］コンピュータシステム１１０１は、中央演算処理装置（ＣＰＵ、本明細書ではまた「プロセッサ」及び「コンピュータプロセッサ」）１１０５を含み、ＣＰＵ１１０５

は、シングルコア若しくはマルチコアプロセッサ又は並列処理用の複数のプロセッサであり得る。コンピュータシステム１１０１は、メモリ若しくはメモリロケーション１１１０（例えば、ランダムアクセスメモリ、読み取り専用メモリ、フラッシュメモリ）、電子記憶ユニット１１１５（例えば、ハードディスク）、１つ若しくは複数の他のシステムと通信するための通信インターフェース１１２０（例えば、ネットワークアダプタ）及びキャッシュ、他のメモリ、データストレージ及び／又は電子ディスプレイアダプタ等の周辺デバイス１１２５も含む。メモリ１１１０、記憶ユニット１１１５、インターフェース１１２０及び周辺デバイス１１２５は、マザーボード等の通信バス（実線）を通してＣＰＵ１１０５と通信する。記憶ユニット１１１５は、データを記憶するためのデータ記憶ユニット（又はデータリポジトリ）であり得る。コンピュータシステム１１０１は、通信インターフェース１１２０を用いてコンピュータネットワーク（「ネットワーク」）１１３０に動作可能に結合することができる。ネットワーク１１３０は、インターネット、インターネット及び／又はエクストラネット、又はインターネットと通信するイントラネット及び／又はエクストラネットであり得る。幾つかの場合、ネットワーク１１３０は、電気通信ネットワーク及び／又はデータネットワークである。ネットワーク１１３０は、１つ又は複数のコンピュータサーバを含むことができ、それによりクラウド計算等の分散計算を可能にすることができる。ネットワーク１１３０は、場合によりコンピュータシステム１１０１を用いてピアツーピアネットワークを実装することができ、コンピュータシステム１１０１に結合されたデバイスがクライアント又はサーバとして挙動できるようにし得る。

【００５６】

［0073］ ＣＰＵ１１０５は、プログラム又はソフトウェアで実装することができる一連の機械可読命令を実行することができる。命令は、メモリ１１１０等のメモリロケーションに記憶され得る。命令は、ＣＰＵ１１０５に向けられ得、続けて本開示の方法を実施するようにＣＰＵ１１０５をプログラム又は他の方法で構成することができる。ＣＰＵ１１０５によって実行される動作の例は、フェッチ、デコード、実行及びライトバックを含むことができる。

【００５７】

［0074］ ＣＰＵ１１０５は、集積回路等の回路の一部分であり得る。システム１１０１の１つ又は複数の他の構成要素は、回路に含まれ得る。場合により、回路は、特定用途向け集積回路（ＡＳＩＣ）である。

【００５８】

［0075］ 記憶ユニット１１１５は、ドライバ、ライブラリ及び保存されたプログラム等のファイルを記憶することができる。記憶ユニット１１１５は、ユーザデータ、例えばユーザ選好及びユーザプログラムを記憶することができる。場合により、コンピュータシステム１１０１は、イントラネット又はインターネットを通してコンピュータシステム１１０１と通信するリモートサーバに配置される等、コンピュータシステム１１０１から外部の１つ又は複数の追加のデータ記憶ユニットを含むことができる。

【００５９】

［0076］ コンピュータシステム１１０１は、ネットワーク１１３０を通して１つ又は複数のリモートコンピュータシステムと通信することができる。例えば、コンピュータシステム１１０１は、ユーザのリモートコンピュータシステムと通信することができる。リモートコンピュータシステムの例には、パーソナルコンピュータ（例えば、ポータブルＰＣ）、スレート又はタブレットＰＣ（例えば、Apple（登録商標）iPad、Samsung（登録商標Galaxy Tab）、電話、スマートフォン（例えば、Apple（登録商標）iPhone、Android対応デバイス、Blackberry（登録商標））又は個人情報端末がある。ユーザは、ネットワーク１１３０を介してコンピュータシステム１１０１にアクセスすることができる。

【００６０】

［0077］ 本明細書に記載されるような方法は、例えば、メモリ１１１０又は電子記憶ユニット１１１５等のコンピュータシステム１１０１の電子記憶ロケーションに記憶された機械（例えば、コンピュータプロセッサ）実行可能コードによって実装することができる

。機械実行可能又は機械可読コードは、ソフトウェアの形態で提供することができる。使用中、コードは、プロセッサ１１０５によって実行することができる。場合により、コードは、記憶ユニット１１１５から検索され、プロセッサ１１０５によるアクセスを容易にするためにメモリ１１１０に記憶することができる。状況により、電子記憶ユニット１１１５を除外することができ、機械実行可能命令は、メモリ１１１０に記憶される。

【００６１】

［0078］ コードは、予めコンパイルされて、コードを実行するように適合されたプロセッサを有する機械と併用されるように構成することができるか、又は実行時中にコンパイルすることができる。コードは、コードを予めコンパイルされて又はコンパイルされたままで実行できるように選択することができる。

【００６２】

［0079］ コンピュータシステム１１０１等、本明細書に提供されるシステム及び方法の態様は、プログラミングで実装することができる。本技術の種々の態様は、典型的には、機械（又はプロセッサ）実行可能コード及び／又は一種の機械可読媒体で搬送又は実装される関連データの形態の「製品」又は「製造品」と考えることができる。機械実行可能コードは、メモリ（例えば、読み取り専用メモリ、ランダムアクセスメモリ、フラッシュメモリ）又はハードディスク等の電子記憶ユニットに記憶することができる。「ストレージ」型媒体は、非一時的記憶をソフトウェアプログラミングに随時提供され得る種々の半導体メモリ、テープドライブ、ディスクドライバ等のコンピュータの有形メモリ、プロセッサ等、又は関連するモジュールのいずれか又は全てを含むことができる。ソフトウェアの全て又は部分は、ときにインターネット又は種々の他の電気通信ネットワークを通して通信し得る。そのような通信は、例えば、あるコンピュータ又はプロセッサから別のコンピュータ又はプロセッサに、例えば管理サーバ又はホストコンピュータからアプリケーションサーバのコンピュータプラットフォームにソフトウェアをロードできるようにし得る。したがって、ソフトウェア要素を運び得る別のタイプの媒体には、ローカルデバイス間の物理的インターフェースにわたり、有線及び光陸戦ネットワークを通して及び種々のエアリンクを介して使用される等の光学、光波、電波及び電磁波がある。有線又は無線リンク、光リンク等のそのような波動を搬送する物理的要素も、ソフトウェアを運ぶ媒体として見なすことができる。本明細書で使用される場合、非一時的有形「記憶」媒体に限定される場合を除き、コンピュータ又は機械「可読媒体」等の用語は、実行のためにプロセッサに命令を提供することに関わる任意の媒体を指す。

【００６３】

［0080］ したがって、コンピュータ実行可能コード等の機械可読媒体は、限定ではく、有形記憶媒体、搬送波媒体又は物理的伝送媒体を含む多くの形態をとり得る。不揮発性記憶媒体には、例えば、図面に示されるデータベース等の実装に使用され得る等、任意のコンピュータ等における任意の記憶装置等の光ディスク又は磁気ディスクがある。揮発性記憶媒体には、そのようなコンピュータプラットフォームのメインメモリ等の動的メモリがある。有形伝送媒体は、コンピュータシステム内のバスを構成するワイヤを含め、同軸ケーブル、銅線及び光ファイバを含む。搬送波伝送媒体は、無線（ＲＦ）及び赤外線（ＩＲ）データ通信中に生成される等の電気信号若しくは電磁信号又は音波若しくは光波の形態をとり得る。したがって、一般的な形態のコンピュータ可読媒体には、例えば、フロッピーディスク、フレキシブルディスク、ハードディスク、磁気テープ、他の任意の磁気媒体、ＣＤ－ＲＯＭ、ＤＶＤ若しくはＤＶＤ－ＲＯＭ、他の任意の光媒体、パンチカード紙テープ、穴のパターンを有する他の任意の物理的記憶媒体、ＲＡＭ、ＲＯＭ、ＰＲＯＭ及びＥＰＲＯＭ、フラッシュＥＰＲＯＭ、他の任意のメモリチップ若しくはカートリッジ、データ若しくは命令を輸送する搬送波、そのような搬送波を輸送するケーブル若しくはリンク又はコンピュータがプログラミングコード及び／又はデータを読み取ることができる他の任意の媒体がある。これらの形態のコンピュータ可読媒体の多くは、１つ又は複数の命令の１つ又は複数のシーケンスを実行のためにプロセッサに搬送することに関わり得る。

【００６４】

［0081］コンピュータシステム１１０１は、例えば、プログラミングインターフェースを提供するためにユーザインターフェース（ＵＩ）１１４０を含む電子ディスプレイ１１３５を含むことができるか、又はそれと通信することができる。ＵＩの例には、限定ではなく、グラフィカルユーザインターフェース（ＧＵＩ）及びウェブに基づくユーザインターフェースがある。

【００６５】

［0082］本開示の方法及びシステムは、１つ又は複数のアルゴリズムとして実装することができる。アルゴリズムは、中央演算処理装置１１０５によって実行されると、ソフトウェアによって実装することができる。アルゴリズムは、例えば、本明細書に記載のような１つ又は複数の暗号化アルゴリズムを実装することができる。

【実施例】

【００６６】

例

［0083］以下の例は、本明細書に記載の特定のシステム及び方法の例示であり、限定を意図しない。

【００６７】

例１　－　更新サイズの現実世界での改善

［0084］図７Ａ～図７Ｃは、種々の鍵暗号化メカニズムの更新サイズｖｓ群サイズプロットの例を示す。図７Ａ～図７Ｃに示す例は、本明細書の他の箇所に記載の方法及びシステムの実施を介して達成することができるコンピュータシステムの機能の改善を示す。図７Ａ～図７Ｃに示す各群サイズについて、更新サイズを最小化するようにツリーの項数を選択した。図７Ａは、Kyber512鍵暗号化メカニズムを使用する複数の異なる状況での更新サイズのプロットを示す。１行目である送信者鍵（ｃ）は、圧縮が適用された状態の、送信者鍵方式の群サイズの関数としての更新サイズを示し、群サイズに等しい項数、したがって深度１が図２のプロセス２００で使用された、圧縮されたツリーＫＥＭ方式として考えることもできる。送信者鍵方式の一例は、単一のノードが更新を各受信ノードに送信する図１０Ｃに見出すことができる。２行目であるツリーＫＥＭは、図１０Ｄに示される等の非圧縮方式の効率をトレースする。ツリーＫＥＭ方式を使用した更新の初期コストは、圧縮送信者鍵方式よりも高いが、群サイズは、効率を上げるため、ツリーＫＥＭ方式を使用することの利得が大きい場合がある。３行目に示すように、圧縮ツリーＫＥＭ（例えば、ツリーＫＥＭ（ｃ））方式の適用により、更なる改善を実現することができる。圧縮ツリーＫＥＭ方式は、暗号文圧縮が更新プロセスで使用される図２のプロセス２００の一実装形態であり得る。圧縮ツリーＫＥＭ方式は、２よりも大きい全ての群サイズで標準ツリーＫＥＭ方式から改善された性能を示すと共に、群サイズが６４を超えて大きくなると、圧縮送信者鍵からの顕著な改善も示す。したがって、暗号文対応圧縮ツリーＫＥＭ方式は、全ての群サイズで更新サイズ、したがって更新を使用するシステムの性能を改善することができ、群が大きくなるほど、提供される改善が大きくなる。

【００６８】

［0085］同様に、図７Ｂ及び図７Ｃは、追加の鍵カプセル化メカニズム（ＫＥＭ）における暗号文圧縮方式を使用することによって表される改善を示し、改善の普遍性を示す。図７Ｂは、FrodoKEM640KEMの場合のプロットである一方、図７Ｃは、ＳＩＫＥ／p434KEMの場合の更新サイズｖｓ群サイズを示す。図７Ｃのコールアウト７７０、７８０及び７９０は、図の凡例を明確にするために提示されている。各図では、圧縮ツリーＫＥＭ方式の性能は、常に非圧縮ツリーＫＥＭ方式よりも良好であり、より大きい群サイズで圧縮送信者鍵方式よりも良好である。圧縮送信者鍵方式と圧縮ツリーＫＥＭ方式との間の相違の場所は、各方式のシステムパラメータ、暗号文及びマルチ暗号文の相対サイズに依存し得る。例えば、FrodoKEM640は、ＳＩＫＥ／p434よりも、暗号文のバイトサイズと比較して相対的に大きいシステムパラメータバイトサイズを有することができ、したがって圧縮送信者鍵と圧縮ツリーＫＥＭとの間の相違を見るためにより大きい群サイズをとる。

【００６９】

［0086］図８は、マルチ暗号文方式が使用される場合、複数の異なるＫＥＭ方式で可能な漸近利得係数を示す。｜Ｕ｜値は、システムパラメータ（例えば、ユーザの公開鍵に依存しないパラメータ）であり得る。｜Ｕ｜値は、図４Ａ～図４Ｄ及び図５Ａ～図５Ｄにおけるパラメータｕのサイズに対応することができる。マルチ暗号文方式の使用は、これらのパラメータが転送される回数、したがって転送し得るデータ量を低減することができる。｜Ｖ｜値は、ユーザの公開鍵に依存するパラメータ（例えば、暗号化メッセージ、種々の他の鍵）のサイズであり得る。｜Ｕ｜サイズと｜Ｖ｜サイズとを結合することにより、｜ｃｔｘｔ｜カラムを生成することができ、このカラムは、完全に古典的な暗号文のサイズを示す。追加の｜Ｖ｜パラメータを添付する代わりに｜Ｕ｜パラメータを再使用することにより、２受信者のマルチ暗号文のサイズは、｜Ｕ｜＋２｜Ｖ｜であり得る一方、２受信者の古典的な暗号文は、２｜Ｕ｜＋２｜Ｖ｜であり得る。｜ｃｔｘｔ｜／｜Ｖ｜を計算することにより、漸近利得係数を特定することができ、この係数は、本明細書の他の箇所に記載のようなマルチ暗号文方法及びシステムを実施することによって得ることができる最大効率係数を示し得る。図８に見られるように、本明細書に記載の方法は、暗号鍵更新を送信するための通信帯域幅要件を低減することにより、実際の効率利得をコンピュータシステムに付与することができる。更に、図８は、多様な異なる暗号化方式へのマルチ暗号文方式の広範囲の適用可能性を示すことができる。

【００７０】

例２　－　データベース構造と暗号文圧縮との相互作用

［0087］図１０Ａ～図１０Ｅは、暗号文圧縮と併せて使用し得る複数のプロトコルの例を示す。図１０Ａは、ブロードキャスト使用事例の一例である。ブロードキャスト使用事例において、ユーザＡは、情報を１人又は複数の受信者、この例では６人の受信者に出力することができる。情報が機密である場合、情報に何らかの暗号化を施すことがＡにとっての需要であり得る。出力は、ネットワーク（例えば、インターネット）、ブロードキャスト媒体（例えば、光波、無線波）等を経由し得る。図１０Ｂは、サーバ支援メッセージング方式を示す。ユーザＡは、ＡがサーバＳに送信する、１人又は複数の他のユーザを宛先としたメッセージを有する。１人又は複数のユーザは、ユーザＡがメッセージを送信するときにオンラインでないことがあるため、メッセージは、常にオンラインであるサーバＳに送信され得る。この例において、送信されるデータ量は、メッセージの意図される受信者数に基づいて急速に成長することができる。マルチ暗号文を使用すると、サーバＳを出る負荷を低減することができる。６人の受信者の例において、ユーザＡが、ユーザ非依存の０．５メガバイト（ＭＢ）のシステムパラメータと、ユーザ非依存でない０．５ＭＢの暗号化メッセージとを含む１ＭＢメッセージを送信する場合、標準暗号文システムは、Ａに６ＭＢの情報をサーバに送信させ（６ユーザ×１メッセージ当たり１ＭＢ）、次いで、サーバは、６つの６ＭＢメッセージを送出する（ユーザのメッセージへの任意の変更は、書名を損なう恐れがあるため）。マルチ暗号文方式の場合、ユーザＡは、３．５ＭＢメッセージをサーバに送信し（０．５ＭＢのシステムパラメータ及び３ＭＢの暗号化メッセージ）、サーバは、６ＭＢメッセージを用いて各受信者を更新することができ、合計通信節減は、２．５ＭＢである。マルチ暗号文方式と併せて墨塗り署名を使用する場合、ユーザＡは、３．５ＭＢメッセージをサーバに送信することができ、サーバは、複数のユーザの各ユーザに意図されない情報を除去することができ、それにより６つの１ＭＢメッセージを送信することができ、合計通信節減は、３２．５ＭＢである。明らかなように、マルチ暗号文と墨塗り署名との組合せは、メッセージの送信に必要とされる帯域幅の大きい低減をもたらすことができる。

【００７１】

［0088］図１０Ｃ及～図１０Ｅは、マルチ暗号文及び墨塗り署名と同等の異なるツリー構造として見ることができる。図１０Ｃは、暗号鍵を更新するユーザが更新を群中の他の各ユーザに送信する送信者鍵方式の一例である。この構造は、項数Ｎのツリーであり、ここで、Ｎは、群のメンバ数である。これは、図１０Ｄのツリーと対比することができ、図１０Ｄのツリーは、代わりに、同数の受信者ノードを有するが、代わりに項数２のツリー

に配置される。ユーザが暗号鍵更新等のメッセージを送信者鍵方式で送信する場合、ユーザは、Ｎ－１メッセージ、図１０Ｃの例では７つのメッセージを送信する。図１０Ｄのツリーでは、各ノードは、そのパス中のノード（例えば、ノード１へのパスは、ノード１０１０である）の復号鍵を知ることができる。各ノードは、そのノードのパス中の復号鍵を知ることができるため、鍵を更新するユーザは、ユーザのパス中の全てのノードを更新し、それには、更新を共通パス中のノードに送信する必要がある。図１０Ｄの例において、ノード１について、パスではノード１０１０であり、共通パスではノード１０２０である。これは、ｄ個の公開鍵及びｄ個の暗号文の送信に繋がり、ここで、$d = \log_2 N$である。したがって、ツリー構造は、通信コストが$\log_m N$対Ｎ－１として拡大縮小するため、送信者鍵構造よりもスケーラブルである。

【００７２】

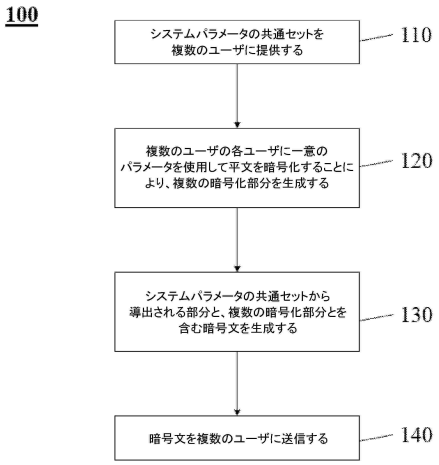
[0089] 図１０Ｅは、マルチ暗号文方式を使用することによって可能になる項数４を有する、項数がより大きいツリー構造の一例である。図１０Ｄのツリーと同様に、各ノードは、そのパス中のノードの復号鍵を知り、したがってユーザ１が更新を送信する場合、$d = \log_4 N$（この例では＝２）であるｄ個の復号鍵及び（ｍ－１）＊ｄ（ここで、ｍは、ユーザ数であり、この例では（ｍ－１）＊ｄ＝６である）個のマルチ暗号文を送信する。送信されるマルチ暗号文の数は、１レベル当たり１であり得る。マルチ暗号文は、１レベル当たり（ｍ－１）個の他のノードを更新するために（ｍ－１）個の暗号文を含み得る。図１０Ｄの例において、ノード１からの最初のマルチ暗号文更新は、ノード２、３及び４への暗号文を含むことができ、２番目のマルチ暗号文更新は、ノード１８、１９及び２０への暗号文を含むことができる。マルチ暗号文は、各受信者ノードに送信される前に、マルチ暗号文を変更できるようにする墨塗り書名を用いて書名することもできる。例えば、ノード２、３及び４へのマルチ暗号文更新は、他の２つのノードへの更新ではなく、関連する更新を含むように変更することができる。

【００７３】

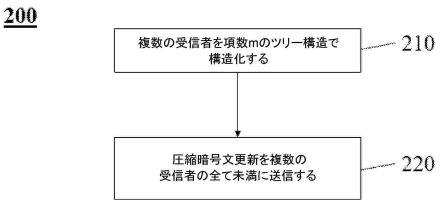
[0090] 本発明の好ましい実施形態を本明細書に示し、説明したが、そのような実施形態が単なる例として提供されることが当業者に明らかであろう。本発明は、本明細書内で提供される特定の例によって限定されることを意図されない。本発明について上記の本明細書を参照して説明したが、本明細書における実施形態の説明及び例示は、限定の意味での解釈を意図されない。本発明から逸脱することなく、多くの変形形態、変更形態及び置換形態が当業者に想到されるであろう。更に、本発明の全ての態様は、多様な条件及び変数に依存する、本明細書に記載された特定の図、構成又は相対的割合に限定されないことが理解されるものとする。本発明の実施にあたり、本明細書に記載の本発明の実施形態への種々の代替形態を採用し得ることを理解されたい。したがって、本発明は、あらゆるそのような代替の変更形態、変形形態又は均等物も包含することが企図される。以下の特許請求の範囲は、本発明の範囲を規定し、これらの請求項及びそれらの均等物内の方法及び構造は、それによって包含されることが意図される。

【図面】

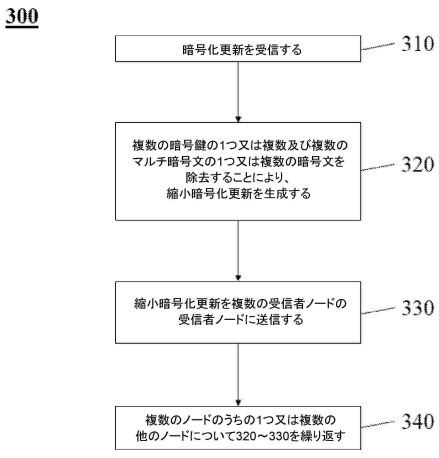
【図１】



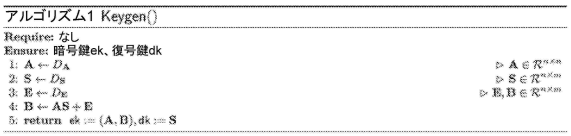
【図２】



【図３】



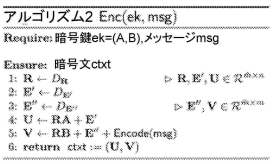
【図４Ａ】


アルゴリズム1 Keygen()

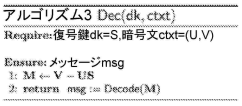
Require: なし
Ensure: 暗号鍵ek、復号鍵dk

1: $\mathbf{A} \leftarrow D_{\mathbf{A}}$ ▷ $\mathbf{A} \in \mathcal{R}^{n \times n}$
2: $\mathbf{S} \leftarrow D_{\mathbf{S}}$ ▷ $\mathbf{S} \in \mathcal{R}^{n \times m}$
3: $\mathbf{E} \leftarrow D_{\mathbf{E}}$ ▷ $\mathbf{E}, \mathbf{B} \in \mathcal{R}^{n \times m}$
4: $\mathbf{B} \leftarrow \mathbf{AS} + \mathbf{E}$
5: return $\mathrm{ek} := (\mathbf{A}, \mathbf{B}), \mathrm{dk} := \mathbf{S}$

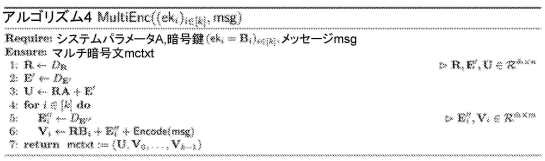
【図４Ｂ】



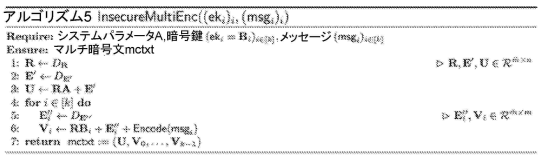
【図４Ｃ】



【図４Ｄ】



【図５Ａ】



【図５Ｂ】

アルゴリズム6 Keygen()

Require: なし
Ensure: 暗号鍵ek,復号鍵dk

1: $\mathbf{S} \xleftarrow{R} \mathcal{K}_A$
2: $\mathbf{P} \leftarrow \mathrm{isogen}(\mathbf{S})$
3: **return** ek := $\mathbf{P}$, dk := $\mathbf{S}$

【図５Ｃ】

アルゴリズム7 Enc(ek, msg)

Require: 暗号鍵ek=P,
メッセージmsg
Ensure: 暗号文ctxt

1: $s_B \xleftarrow{R} \mathcal{K}_B$
2: $\mathbf{U} \leftarrow \mathrm{isogen}(s_B)$
3: $j \leftarrow \mathrm{isoex}(\mathbf{P}, s_B)$
4: $\mathbf{V} \leftarrow \mathrm{msg} \oplus \mathbf{H}(j)$
5: **return** ctxt := $(\mathbf{U}, \mathbf{V})$

【図５Ｄ】

アルゴリズム8 Dec(dk, ctxt)

Reqire: 復号鍵dk=S,
暗号文ctxt=(U,V)
Ensure: メッセージmsg

1: $j \leftarrow \mathrm{isoex}(\mathbf{U}, \mathbf{S})$
2: **return** msg := $\mathbf{V} \oplus \mathbf{H}(j)$

【図６Ａ】

アルゴリズム9 MultiEnc($(\mathrm{ek}_i)_{i\in[k]}$, msg)

Require: 暗号鍵ek_i=$\mathbf{P}_i$,メッセージmsg
Ensure: マルチ暗号文mctxt

1: $s_B \xleftarrow{R} \mathcal{K}_B$
2: $\mathbf{U} \leftarrow \mathrm{isogen}(s_B)$
3: **for** $i \in [k]$ **do**
4: $\quad j_i \leftarrow \mathrm{isoex}(\mathbf{P}_i, s_B)$
5: $\quad \mathbf{V}_i \leftarrow \mathrm{msg} \oplus \mathbf{H}(j_i)$
6: **return** mctxt := $(\mathbf{U}, \mathbf{V}_0, \ldots, \mathbf{V}_{k-1})$

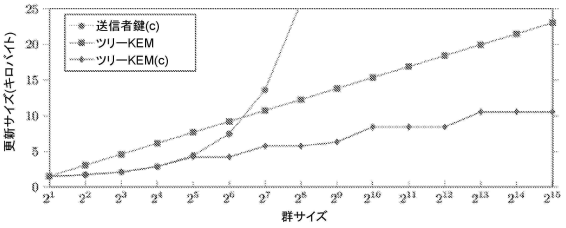
【図６Ｂ】

アルゴリズム10 MultiEnc($\{\mathsf{ek}_i\}_{i\in[k]}$, msg)

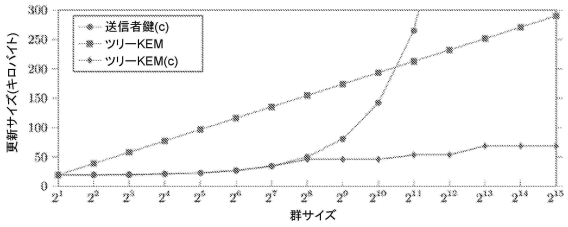
Require: 暗号鍵ek_i=P_i,メッセージmsg
Ensure: マルチ暗号文mctxt

$s_B \xleftarrow{R} \mathcal{K}_B$
$\mathbf{U} \leftarrow \mathsf{isogen}(s_B)$
for $i \in [k]$ **do**
  $j_i \leftarrow \mathsf{isoex}(\mathbf{P}_i, s_B)$
  $\mathbf{V}_i \leftarrow \mathsf{msg}_i \oplus \mathbf{H}(j_i)$
return mctxt := $(\mathbf{U}, \mathbf{V}_0, \ldots, \mathbf{V}_{k-1})$

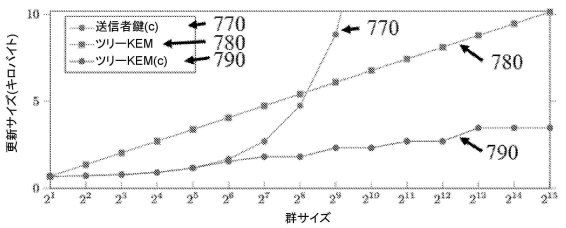
【図７Ａ】



【図７Ｂ】



【図７Ｃ】



【図８】

方式	|U|	|V|	|ctxt|	漸近利得係数
Round5 R5ND_1KEMb	429	110	539	4.9
Round5 R5ND_3KEMb	756	74	830	11.22
Round5 R5ND_5KEMb	940	142	1 082	7.62
LightSaber	640	96	736	7.67
Saber	960	128	1 088	8.5
FireSaber	1 280	192	1 472	7.67
NewHope-512-CPA-KEM	896	192	1 088	5.67
NewHope-1048-CPA-KEM	1 792	384	2 176	5.67
Kyber-512	640	96	736	7.67
Kyber-768	960	128	1 088	8.5
Kyber-1024	1 408	160	1 568	9.8
FrodoKEM-640	9 600	120	9 720	81
FrodoKEM-976	15 616	128	15 744	123
FrodoKEM-1344	21 504	128	21 632	169
SIKE/p434	330	16	346	21.63
SIKE/p503	378	24	402	16.75
SIKE/p751	564	32	596	18.63
SIKE/p434-圧縮	196	16	209	12.25
SIKE/p751-圧縮	331	32	363	10.34

【図９】

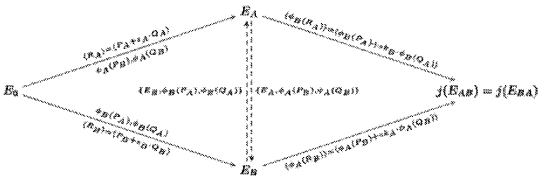


FIG. 9

【図１０Ａ】

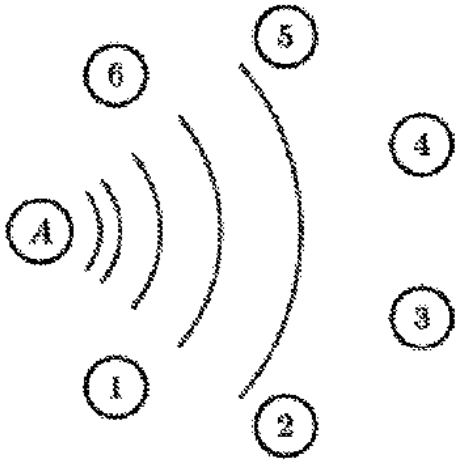


FIG. 10A

【図１０Ｂ】

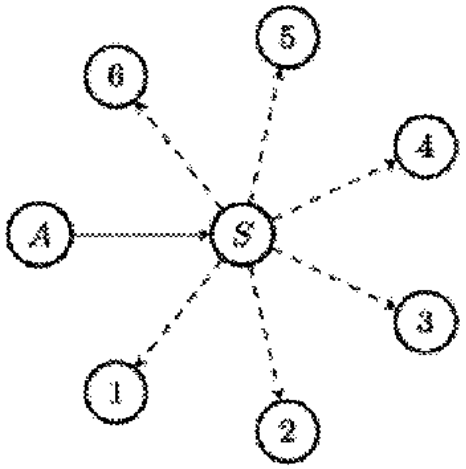


FIG. 10B

【図１０Ｃ】

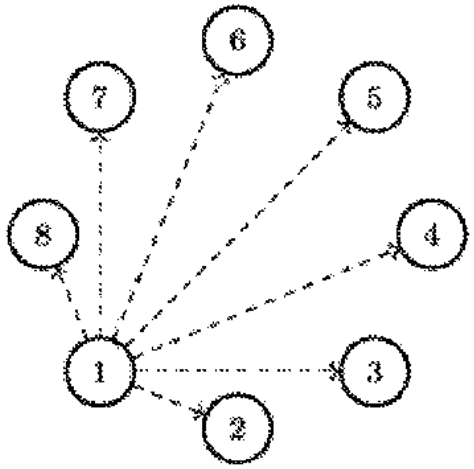


FIG. 10C

【図１０Ｄ】

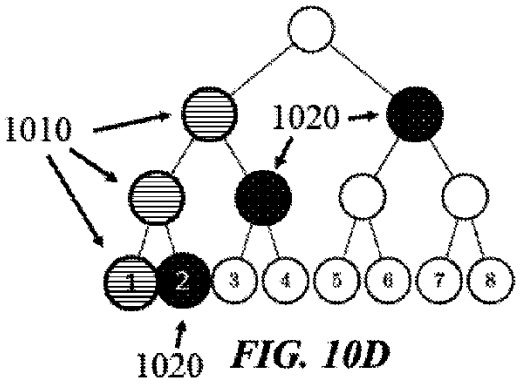


FIG. 10D

【図１０Ｅ】

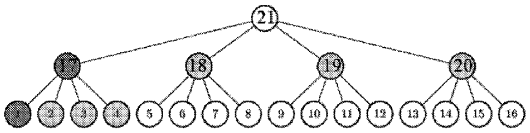


FIG. 10E

【図１１】

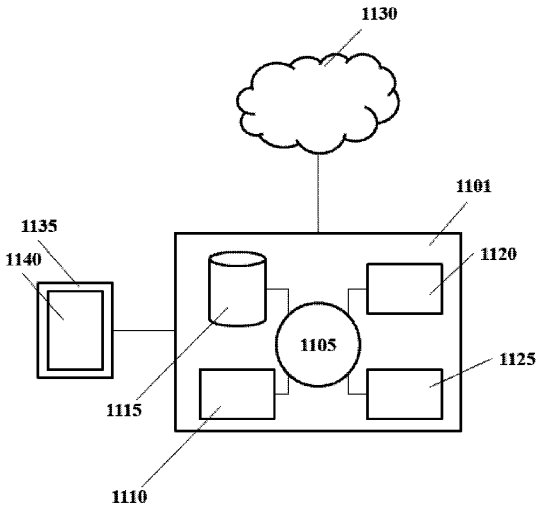


FIG. 11

【図１２Ａ】

アルゴリズム11 Keygen()

Require: なし
Ensure: 暗号鍵ek,復号鍵dk
1: $(e_1, \ldots, e_n)$ sampled randomly from $\mathcal{M}$
2: $[a] = (\mathbb{U}_1^a, \ldots, \mathbb{U}_n^a)$
3: $E_A \leftarrow [a] \cdot E_0$
4: **return** ek := $\mathbf{A}$, dk := $(e_1, \ldots, e_n)$

【図１２Ｂ】

アルゴリズム12 Enc(ek, msg)

Require: 暗号鍵ek=A,
メッセージmsg
Ensure: 暗号文ctxt
1: $(\mathbf{U}, \{e_1, \ldots, e_n\}) \leftarrow$ Keygen()
2: Compute [b] and E_A
3: $E_R \leftarrow [b]E_A$
4: $\mathbf{V} \leftarrow$ msg $\oplus \mathbf{H}(R)$
5: **return** ctxt := $(\mathbf{U}, \mathbf{V})$

【図１２Ｃ】

アルゴリズム13 Dec(dk, ctxt)

Require: 復号鍵dk=(e_1,$\cdots$,e_n)
暗号文ctxt=(U,V)
Ensure: メッセージmsg
1: Compute [a] from dk and E_U from $\mathbf{U}$
2: $E_R \leftarrow [a]E_U$
3: **return** msg := $\mathbf{V} \oplus \mathbf{H}(s)$

【図１２Ｄ】

アルゴリズム14 MultiEnc($(\mathrm{ek}_i)_{i\in[k]}$, msg)

Require: i∈[l,k]でのk個の暗号鍵ek_i=A_iのリスト,メッセージmsg
Ensure: マルチ暗号文mctxt
1: $(\{e_1, \ldots, e_n\}, \mathbf{U}) \leftarrow$ Keygen()
2: Construct [b]
3: **for** $i \in [k]$ **do**
4: Construct E_{A_i} from A_i
5: $E_{R_i} \leftarrow [b]E_{A_i}$
6: $\mathbf{V}_i \leftarrow$ msg $\oplus \mathbf{H}(R_i)$
7: **return** mctxt := $(\mathbf{U}, \mathbf{V}_1, \ldots, \mathbf{V}_k)$

フロントページの続き

イギリス国，オックスフォードシャー オーエックス２ ７エイチティー オックスフォード バンベリー ロード ２６７ プラマ ハウス ピーキューシールド エルティーディー
(72)発明者 カツマタ，シュウイチ
イギリス国，オックスフォードシャー オーエックス２ ７エイチティー オックスフォード バンベリー ロード ２６７ プラマ ハウス ピーキューシールド エルティーディー
(72)発明者 クファトコフスキ，クリス
イギリス国，オックスフォードシャー オーエックス２ ７エイチティー オックスフォード バンベリー ロード ２６７ プラマ ハウス ピーキューシールド エルティーディー

審査官 平井 誠
(56)参考文献 国際公開第２００８／０８７７３４（WO，Ａ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０９Ｃ １／００－５／００
Ｈ０４Ｌ ９／００－４０