(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5419056号
(P5419056)
(45)発行日　平成26年2月19日(2014.2.19)　(24)登録日　平成25年11月29日(2013.11.29)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675B
H04L 9/30 (2006.01)　　H04L 9/00 663Z
H04L 9/08 (2006.01)　　H04L 9/00 601D

請求項の数 5　外国語出願　(全 18 頁)

(21)出願番号　特願2006-20935(P2006-20935)
(22)出願日　平成18年1月30日(2006.1.30)
(65)公開番号　特開2006-221161(P2006-221161A)
(43)公開日　平成18年8月24日(2006.8.24)
審査請求日　平成21年1月30日(2009.1.30)
(31)優先権主張番号　11/053,339
(32)優先日　平成17年2月8日(2005.2.8)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】Ｃａｒｔｉｅｒ対形成の暗号化適用

(57)【特許請求の範囲】
【請求項１】
プロセッサおよびメモリを少なくとも含むコンピュータにおいて暗号化処理を行う方法において、前記コンピュータは署名／暗号化モジュールを備え、前記方法は、
前記コンピュータにおいて、前記署名／暗号化モジュールが、２つの異なるアーベル多様体ＥおよびＥ’ならびにそれらの間の同種写像Φから、カルティエ対形成を生成するステップであって、
前記署名／暗号化モジュールにより、前記２つの異なるアーベル多様体の第１のアーベル多様体から第１の要素Ｐを決定するステップ、および
元のデータを第２のアーベル多様体にハッシュすることによって、前記２つの異なるアーベル多様体の前記第２のアーベル多様体から第２の要素Ｐ’を決定するステップであって、前記第１および第２のアーベル多様体は同一のアーベル多様体ではない、決定するステップを含み、
前記カルティエ対形成は、ｍを同種写像Φの次数ｍ、ｎを前記第１のアーベル多様体のねじれ点の数として、ｍ’＝ｍ$^{-1}$ｍｏｄｎの時に、ｍ’倍写像［ｍ’］に基づいて、前記点Ｑから前記点Ｐの反転を求めることによって求められ、
前記カルティエ対形成は、前記同種写像Φに対して、ＰはΦの核の中のアーベル多様体Ｅ上の点であり、Ｐ’は、双対$\widehat{\Phi}$の核の中のアーベル多様体Ｅ’上の点であり、ＱはΦ（Ｑ）＝Ｐ’の特性を持つ点とするとき、

e_{Φ}（Ｐ，Ｐ’）＝e_{m}（Ｐ，Ｑ）として定義され、

前記コンピュータにおいて、署名／暗号化モジュールが、前記アーベル多様体の第１のアーベル多様体から前記アーベル多様体の第２のアーベル多様体までの次数ｍの同種写像Φを決定する、生成するステップと、

前記コンピュータにおいて、前記署名／暗号化モジュールが、前記生成されたカルティエ対形成に基づいてデータを暗号化処理するステップであって、

乱数ｒから秘密鍵を生成するステップと、

署名者の公開鍵を前記秘密鍵の数ｒおよび前記第１の要素Ｐの関数として生成するステップと、

前記元のデータの結果のハッシュのｒ倍数として署名（シグネチャ）を計算するステップと

を含む、暗号化処理をするステップと

を備えることを特徴とする方法。

【請求項２】

前記暗号化処理は、署名プロトコルに基づくことを特徴とする請求項１に記載の方法。

【請求項３】

プロセッサおよびメモリを少なくとも含むコンピュータにおいて暗号化処理を行う方法において、前記コンピュータは署名／暗号化モジュールを備え、前記方法は、

前記コンピュータにおいて、前記署名／暗号化モジュールが、２つの異なるアーベル多様体ＥおよびＥ’ならびにそれらの間の同種写像Φから、カルティエ対形成を生成するステップであって、

前記署名／暗号化モジュールにより、前記２つの異なるアーベル多様体の第１のアーベル多様体から第１の要素Ｐを決定するステップ、および

元のデータを第２のアーベル多様体にハッシュすることによって、前記２つの異なるアーベル多様体の前記第２のアーベル多様体から第２の要素Ｐ’を決定するステップであって、前記第１および第２のアーベル多様体は同一のアーベル多様体ではない、決定するステップを含み、

前記カルティエ対形成は、ｍを同種写像Φの次数ｍ、ｎを前記第1のアーベル多様体のねじれ点の数として、ｍ´＝m^{-1}ｍｏｄｎの時に、ｍ´倍写像［ｍ´］に基づいて、前記点Ｑから前記点Ｐの反転を求めることによって求められ、

前記カルティエ対形成は、前記同種写像Φに対して、ＰはΦの核の中のアーベル多様体Ｅ上の点であり、Ｐ’は、双対$\widehat{\Phi}$の核の中のアーベル多様体Ｅ’上の点であり、ＱはΦ（Ｑ）＝Ｐ’の特性を持つ点とするとき、

e_{Φ}（Ｐ，Ｐ’）＝e_{m}（Ｐ，Ｑ）として定義され、

前記コンピュータにおいて、署名／暗号化モジュールが、前記アーベル多様体の第１のアーベル多様体から前記アーベル多様体の第２のアーベル多様体までの次数ｍの同種写像Φを決定する、生成するステップと、

前記コンピュータにおいて、前記署名／暗号化モジュールが、前記生成されたカルティエ対形成に基づいてデータを暗号化処理するステップであって、

Ｅ上の点Ｐを識別するステップと、

乱数ｒおよびＰのｒ倍数ｒ＊Ｐを生成するステップと、

公開鍵ｓ＊Ｐを取得するステップと、

識別ＩＤ、前記乱数ｒ、およびｓ＊Ｐに基づいて算出されたカルティエ対形成の関数として、データを暗号化して暗号化データを生成するステップとを含む、暗号化処理するステップ

を備えることを特徴とする方法。

【請求項４】

請求項１乃至３いずれかの方法を実行する、プロセッサによって実行可能なコンピュータプログラム命令を備えたことを特徴とするコンピュータ読取り可能記憶媒体。

【請求項５】
暗号化処理を行うコンピュータ装置において、
プロセッサと、
前記プロセッサに接続されたメモリと、
署名／暗号化モジュールとを備え、
前記メモリ上には
前記コンピュータ装置において前記署名／暗号化モジュールが、２つの異なるアーベル多様体ＥおよびＥ’ならびにそれらの間の同種写像Φから、カルティエ対形成を生成するステップであって、
前記署名／暗号化モジュールが前記２つの異なるアーベル多様体の第１のアーベル多様体から第１の要素Ｐを決定するステップ、および
元のデータを第２のアーベル多様体にハッシュすることにより、前記２つの異なるアーベル多様体の前記第２のアーベル多様体から第２の要素Ｐ’を決定するステップであって、前記第１および第２のアーベル多様体は同一のアーベル多様体ではない、決定するステップを含み、
前記カルティエ対形成は、ｍを同種写像Φの次数ｍ、ｎを前記第1のアーベル多様体のねじれ点の数として、ｍ´＝ｍ$^{-1}$ｍｏｄｎの時に、ｍ´倍写像［ｍ´］に基づいて、前記点Ｑから前記点Ｐの反転を求めることによって求められ、
前記カルティエ対形成は、前記同種写像Φに対して、ＰはΦの核の中のアーベル多様体Ｅ上の点であり、Ｐ’は、双対$\widehat{\Phi}$の核の中のアーベル多様体Ｅ’上の点であり、ＱはΦ（Ｑ）＝Ｐ’の特性を持つ点とするとき、
e_{Φ}（Ｐ，Ｐ’）＝e_m（Ｐ，Ｑ）として定義され、
前記コンピュータにおいて、署名／暗号化モジュールが、前記アーベル多様体の第１のアーベル多様体から前記アーベル多様体の第２のアーベル多様体までの次数ｍの同種写像Φを決定する、生成するステップと、
前記コンピュータ装置において前記署名／暗号化モジュールが、前記生成されたカルティエ対形成に基づいてデータを暗号化処理するステップであって、
署名者の公開鍵を前記秘密鍵の数ｒおよび前記第１の要素Ｐの関数として生成するステップと、
前記元のデータの結果のハッシュのｒ倍数として署名（シグネチャ）を計算するステップと
を含む、暗号化処理をするステップと
を有する方法を実行する、前記プロセッサによって実行可能なコンピュータプログラム命令を含むことを特徴とするコンピュータ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明のシステムおよび方法は、暗号化処理に関する。
【背景技術】
【０００２】
既存の対形成ベースの暗号化システムでは、例えば楕円曲線などの、アーベル多様体上の点において評価されるＷｅｉｌまたはＴａｔｅ対形成を使用する。固定の自然数ｍに対して、Ｗｅｉｌ対形成e_mは、入力として楕円曲線上の２つのｍねじれ点をとり、出力としてｍ乗根をとる双一次写像である。例えば、固定の自然数ｍに対して、Ｗｅｉｌ対形成e_mは、入力として楕円曲線上の２つのｍねじれ点をとり、出力としてｍ乗根をとる双一次写像である。
【０００３】
【非特許文献１】Katz et al., "Arithmetic Moduli of Elliptic Curves" Princeton University Press, 1985, pp. 87--91, or Cartier, "Isogenies and duality of abelian

varieties", Ann. Math., vol. 71, 1960, p. 315-351

【発明の開示】

【発明が解決しようとする課題】

【０００４】

Ｃａｒｔｉｅｒ対形成の関数としてデータを暗号化処理するシステムおよび方法が説明される。

【課題を解決するための手段】

【０００５】

Ｃａｒｔｉｅｒ対形成の関数としてデータを暗号化処理するシステムおよび方法が説明される。１つの態様において、Ｃａｒｔｉｅｒ対形成は、２つの異なるアーベル多様体およびそれらの間の同種写像から生成される。データはＣａｒｔｉｅｒ対形成に基づいて暗号化処理される。

【０００６】

図中において、コンポーネント参照番号の左端の数字は、コンポーネントが最初に出現する特定の図を識別する。

【発明を実施するための最良の形態】

【０００７】

概要

Ｃａｒｔｉｅｒ対形成の暗号化適用のためのシステムおよび方法は、以下に図１から図５を参照して説明される。Ｃａｒｔｉｅｒ対形成はe_{Φ}（－、－）で示されるが、これは対形成が点の２つの異なる群からの要素ＰおよびＰ’において評価されることを示している。点の各群は、有限体F_q上で定義された２つの楕円曲線ＥおよびＥ’の１つからのものであり、ΦはＥからＥ’への同種写像（ｉｓｏｇｅｎｙ）である。これらの要素ＰおよびＰ’を識別する技法は、以下で図２を参照して説明される。楕円曲線Ｅから楕円曲線Ｅ’への同種写像Φは、群準同型であるＥからＥ’への写像であり、座標の有理関数により座標位置で与えられる。

【０００８】

ｍを同種写像の次数を示すものとすると、これはΦが可分である場合、Φの核（カーネル：ｋｅｒｎｅｌ）の大きさと等しい。ＰをΦの核内のＥ上の点とし、Ｐ’を双対同種写像

【０００９】

【数１】

$$\hat{\phi}$$

【００１０】

の核内のＥ’上の点とし、ＱをΦ（Ｑ）＝Ｐ’の特性を持つＥ上の点とすると、同種写像Φに関してＣａｒｔｉｅｒ対形成は以下のように定義される。e_{Φ}（Ｐ、Ｐ’）＝e_m（Ｐ、Ｑ）、ここで、e_m（Ｐ、Ｑ）は曲線Ｅ上のｍ次のＷｅｉｌ対形成である。Ｃａｒｔｉｅｒ対形成の特性は周知である（例えば、非特許文献１参照）。Ｃａｒｔｉｅｒ対形成はさらに、アーベル多様体の任意の同種写像に実施することもできる。したがってＣａｒｔｉｅｒ対形成を実施するためには、同種写像のもとで点の事前イメージを検出し、Ｗｅｉｌ対形成を評価すれば十分である（Ｃａｒｔｉｅｒ対形成を評価する例示的な手順は、以下で図２および図３を参照して説明される）。

【００１１】

Ｃａｒｔｉｅｒ対形成のシステムおよび方法または暗号化適用は、任意のタイプの対形成ベースの暗号プロトコルを使用して、データを暗号処理するために使用される。そのような暗号プロトコルには、例えば、識別ベースの暗号化を実施するために使用されるもの（例えば、プレーン、ブラインド、プロキシ、リング、拒否不可など）、暗号プロトコル（例えば、認証、ブロードキャスト、キーワード検索による暗号化など）、バッチシグニチャ、キーアグリーメント（ｋｅｙ　ａｇｒｅｅｍｅｎｔ）（プレーン、認証、グループ

など）、信頼当局および公開鍵証明、階層暗号方式、しきい値暗号方式およびシグニチャ、カメレオンハッシュ（ｃｈａｍｅｌｅｏｎ　ｈａｓｈ）およびシグニチャ、認証、アプリケーションおよびシステム、アクセス制御、キーアグリーメント、非対話式キー配布、クレデンシャル（例えば、匿名、秘匿、セルフブラインダブル（ｓｅｌｆ－ｂｌｉｎｄａｂｌｅ）など）、秘密ハンドシェーク、立証可能なセキュアシグニチャ（ｐｒｏｖａｂｌｙ　ｓｅｃｕｒｅ　ｓｉｇｎａｔｕｒｅｓ）、ショートシグニチャ、集合、リング、ならびに検証可能な暗号化シグニチャ、ブラインドおよび部分的ブラインドシグニチャ、プロキシシグニチャ、拒否不可シグニチャ、サイン暗号化（ｓｉｇｎ－ｃｒｙｐｔｉｏｎ）、マルチシグニチャおよびしきい値シグニチャ、限定ベリファイヤおよび指定ベリファイヤシグニチャ、しきい値暗号方式、階層および役割ベースの暗号方式、カメレオンハッシュおよびシグニチャ、検証可能な確率関数、強く遮断された暗号化（ｓｔｒｏｎｇｌｙ　ｉｎｓｕｌａｔｅｄ　ｅｎｃｒｙｐｔｉｏｎ）、侵入回復暗号化（ｉｎｔｒｕｓｉｏｎ－ｒｅｓｉｌｉｅｎｔ　ｅｎｃｒｙｐｔｉｏｎ）、証明書のないＰＫＣ、ａｌ、トレイター追跡（ｔｒａｉｔｏｒ　ｔｒａｃｉｎｇ）、などが含まれる。その結果、Ｃａｒｔｉｅｒ対形成の暗号化適用のためのシステムおよび方法は、楕円曲線またはアーベル多様体上の点において評価されたＷｅｉｌまたはＴａｔｅ対形成に基づいてそのような暗号プロトコルを各々実施する対形成ベースの暗号化システムに代替案を提供する。

【００１２】

Ｃａｒｔｉｅｒ対形成の暗号化適用のためのシステムおよび方法のさまざまな態様が詳細に説明される。

【００１３】

例示的なシステム

必須ではないが、Ｃａｒｔｉｅｒ対形成の暗号化適用のためのシステムおよび方法は、パーソナルコンピュータなどのコンピュータ装置によって実行されるコンピュータ実行可能命令（プログラムモジュール）の一般的な文脈に即して説明される。プログラムモジュールは一般に、特定のタスクを実行するかまたは特定の抽象データタイプを実施するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含んでいる。システムおよび方法は前述の文脈に即して説明されているが、以下に説明される動作およびオペレーションは、またハードウェアにおいて実施することができる。

【００１４】

図１は、Ｃａｒｔｉｅｒ対形成の暗号化適用のための例示的なシステム１００を示している。システム１００は、通信ネットワーク１０３を経由して第２のコンピュータ装置１０４に結合されている第１のコンピュータ装置１０２を含んでいる。通信ネットワーク１０３は、オフィス、企業規模のコンピュータネットワーク、イントラネット、およびインターネットで普及しているような、ローカルエリアネットワーク（ＬＡＮ）および一般的なワイドエリアネットワーク（ＷＡＮ）通信環境の任意の組み合わせを含むことができる。第１のコンピュータ装置１０２および第２のコンピュータ装置１０４は、パーソナルコンピュータ、ラップトップ、サーバ、ハンドヘルドまたはモバイルコンピュータ装置（例えば、携帯電話、携帯情報端末）などのような任意のタイプのコンピュータ装置を表している。

【００１５】

コンピュータ装置１０２は、プログラムモジュール１０６（１つまたは複数）およびプログラムデータ１０８を含んでいる。プログラムモジュール１０６は、例えば署名／暗号化モジュール１１０および他のプログラムモジュール１１１を含んでいる。署名／暗号化モジュール１１０は、Ｃａｒｔｉｅｒ対形成１１２の関数として元のデータをそれぞれ署名または暗号化する。そのような元のデータは、「他のデータ」１１４の各部分として示されている。署名／暗号化モジュール１１０によってそれぞれ署名または暗号化された元のデータは、暗号化または署名されたデータ１１６として示されている。つまり、暗号化処理されたデータ１２２は、署名／暗号化モジュール１１０がＣａｒｔｉｅｒ対形成１１２の関数として元のデータを暗号により署名する場合に署名され、暗号化処理されたデー

タ１２２は、署名／暗号化モジュール１１０がＣａｒｔｉｅｒ対形成１１２の関数として元のデータを暗号化する場合に暗号化される。Ｃａｒｔｉｅｒ対形成１１２を生成し、Ｃａｒｔｉｅｒ対形成１１２を使用して元のデータを暗号化処理（つまり、それぞれ署名または暗号化）するために、署名／暗号化モジュール１１０によって実施される例示的な技法は、以下で図２から図４を参照して説明される。署名／暗号化モジュール１１０が元のデータを暗号により署名する場合、説明のために、署名／暗号化モジュール１１０を署名モジュール１１０と呼ぶ。同様に、署名／暗号化モジュール１１０が元のデータを暗号化する場合、署名／暗号化モジュール１１０を暗号化モジュール１１０と呼ぶ。

【００１６】

図１の第２のコンピュータ装置１０４はさらに、Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理するためのプログラムモジュールおよびプログラムデータを含んでいる。例えば、プログラムモジュールは、Ｃａｒｔｉｅｒ対形成に基づいて暗号化処理されたデータ１２２を検証または復号化するための検証／復号化モジュール１１８を含んでいる。つまり、暗号化処理されたデータ１２２がＣａｒｔｉｅｒ対形成１１２の関数として署名された場合、検証／復号化モジュール１１８は暗号化処理されたデータ１２２を検証し、検証／復号化モジュール１１８はＣａｒｔｉｅｒ対形成１１２の関数として暗号化されている暗号化処理されたデータ１２２を復号化する。暗号化処理されたデータ１２２は、第１のコンピュータ装置１０２によって第２のコンピュータ装置１０４に伝達された署名または暗号化されたデータ１１６を表している。暗号化処理されたデータ１２２をＣａｒｔｉｅｒ対形成１２０の関数としてそれぞれ検証または復号化する例示的な技法は、以下に図２から図４を参照して説明される。説明のために、検証／復号化モジュール１１８が署名されたデータ１２２を暗号により検証する場合、検証／復号化モジュール１１９を検証モジュール１１８と呼ぶ。同様に、検証／復号化モジュール１１８がデータ１２２を復号化する場合、検証／復号化モジュール１１８を復号化モジュール１１８と呼ぶ。

【００１７】

Ｃａｒｔｉｅｒ対形成の例示的な生成および暗号化適用

図２は、Ｃａｒｔｉｅｒ対形成の暗号化適用のための例示的な手順２００を示している。説明および例示的な説明のために、手順２００のオペレーションは図１のコンポーネントに関して説明される。この目的のために、コンポーネント参照番号の左端の数字は、コンポーネントが最初に出現する特定の図を識別する。

【００１８】

ブロック２０２において、署名／暗号化モジュール１１０（図１）は、有限体F_qにわたる第１の楕円曲線Ｅ上の点の群から第１の要素を識別する。具体的には、第１の要素ＰはＥ（F_q）内の点として定義され、Ｅはアーベル多様体または楕円曲線１２４として図１に示される。この第１の要素Ｐは、ＥからＥ’の同種写像Φの核内にある必要がある。

【００１９】

ブロック２０４において、署名／暗号化モジュール１１０（図１）は、有限体F_qにわたる第２のアーベル多様体または楕円曲線Ｅ’（同種写像ΦによりＥに関連している）上の点の群から第２の要素を判別する。Ｅ’は図１に示されている。具体的には、第２の要素Ｐ’は、実施される特定の暗号化適用の関数としての双対同種写像

【００２０】

【数２】

$$\hat{\phi}$$

【００２１】

の核内のＥ’（F_q）上の点である。例えば、Ｃａｒｔｉｅｒ対形成１１２に基づいて例示的な暗号化署名方式を説明する図３を参照して以下で説明されるように、要素Ｐ’は第２の楕円曲線Ｅ’にハッシュされたメッセージＭとして定義することができるが、これが最終的にメッセージＭの署名に使用される。もう１つの例において、Ｐ’は、メッセージＭが点Ｐ’の倍数として楕円曲線Ｅ’にハッシュされるように選択された点であってもよ

い。

【００２２】

ブロック２０６において、署名／暗号化モジュール１１０は、暗号により処理されたデータ（つまり署名または暗号化されたデータ１１６）を生成するために、ＰおよびＰ’によって定義されたＣａｒｔｉｅｒ対形成１１２の関数として元のデータを署名または暗号化する。ブロック２０８において、検証／復号化モジュール１１８はそれぞれ、署名または暗号化されたデータ１１６を復号化または検証する。説明のために、署名または暗号化されたデータ１１６は、暗号化処理されたデータ１２２としてコンピュータ装置１０４内に示されている。ブロック２０８の復号化または検証機能は、Ｃａｒｔｉｅｒ対形成１２０の関数として実行される。データを処理（例えば、署名または暗号化、および同様に検証または復号化）するためにブロック２０６およびブロック２０８において選択された特定の対形成ベースの暗号学アルゴリズムは、目的および実施のために選択された特定の対形成ベースの暗号アルゴリズムの関数である。ただし、例示的な説明のために、署名／暗号化モジュール１１０がＣａｒｔｉｅｒ対形成１１２を使用して元のデータを署名する手順、および検証／復号化モジュール１１８がＣａｒｔｉｅｒ対形成１２０を使用して署名済みデータ１１６を検証する手順は、図３を参照して以下に説明される。もう１つの例において、Ｃａｒｔｉｅｒ対形成１１２を使用して元のデータを暗号化し、Ｃａｒｔｉｅｒ対形成１２０に基づいて暗号化されたデータ１２２を復号化する識別ベースの暗号化（ＩＢＥ）手順は、図４を参照して以下に説明される。ここでそのような例示的な実施態様について説明する。

【００２３】

Ｃａｒｔｉｅｒ対形成に基づくデータの例示的な暗号による署名

図３は、Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化により署名して検証するための例示的な手順３００を示している。説明および例示的な説明のために、手順３００のオペレーションは図１のコンポーネントに関して説明される。この目的のために、コンポーネント参照番号の左端の数字は、コンポーネントが最初に出現する特定の図を識別する。

【００２４】

手順３００の例示的な暗号化実施態様において、署名／暗号化モジュール１１０は署名モジュールである。署名モジュール１１０は、任意の対形成ベースの暗号化署名プロトコルを実施する。例えば、Ｃａｒｔｉｅｒ対形成１１２が決定されると、対形成１１２は、可能な対形成ベースの署名および検証暗号化アルゴリズムのいずれかを使用してデータをそれぞれ署名および検証するために使用される。１つの実施態様において、例えば、署名モジュール１００は、以下のようなデジタル署名プロトコルを実施する。

【００２５】

図３およびブロック３０２を参照すると、署名モジュール１１０は２つの楕円曲線またはアーベル多様体ＥおよびＥ’間の次数ｍの同種写像Φを決定する。ブロック３０４において、署名モジュール１１０は、同種写像Φの核内のＥ（F_q）の第１の要素Ｐを決定する。ブロック３０６において、署名モジュール１１０は、パブリックハッシュ関数ｈを使用してメッセージＭを第２の楕円曲線Ｅ’にハッシュすることにより第２の要素Ｐ’を決定する。つまり、Ｐ’はメッセージ Ｍのハッシュｈ（Ｍ）、ｈ（Ｍ）として定義され、ハッシュ関数ｈは、メッセージスペース｛０、１｝*から双対同種写像

【００２６】

【数３】

$$\hat{\phi}$$

【００２７】

の核であるＥ’（F_q）の部分群への関数である。説明のため、Ｍのハッシュは「他のデータ」１１４の個別の部分として示されている。このようにして、各点ＰおよびＰ’のそれぞれの群は、特定の暗号化署名方式で実施するために指定される。

【００２８】

ブロック３０８において、署名モジュール１１０は、乱数の整数ｒを取得する。これは、署名者の秘密鍵である。署名者の秘密鍵は、元のデータを署名して関連付けられている署名済みデータ１１６を検証することを望む２人の関係者（例えばアリスとボブ）の文脈に即して生成される。ブロック３１０において、署名モジュール１１０は、署名者の公開鍵を、ｒ＊Ｐで表される点Ｐのｒ倍数として生成する。ここでｒは署名者の秘密鍵である。ブロック３１２において、署名モジュール１１０は、元のデータ（この例ではメッセージＭ）の署名σ１２６を、メッセージＭの結果のハッシュのｒ倍数、つまりσ＝ｒ＊ｈ（Ｍ）として計算する。説明のため、同種写像Φ、乱数ｒは「他のデータ」１１４の個別の部分として示されている。

【００２９】

ブロック３１４において、プログラムモジュール１０６（例えば、署名モジュール１１０または異なるプログラムモジュール）は、点ＰおよびＰのｒ倍数とハッシュ関数ｈと共にσ＝ｒ＊ｈ（Ｍ）１２６を公開鍵１２８として公開する。同種写像および２つのアーベル多様体もまた、システムの公開鍵情報の一部である。ブロック３１６において、プログラムモジュール１０６は、ネットワークで結ばれた第２のコンピュータ装置１０４などの第２のエンティティに、検証のためにメッセージＭ（署名済みデータ１１６として示される）および署名σ１２６を伝達する。（第１のコンピュータ装置１０２および第２のコンピュータ装置１０４に関連付けられている両関係者には周知であるセットアップデータは、２つの楕円曲線１２４、同種写像、点Ｐ、およびハッシュ関数ｈを含んでいる。点ｒ＊Ｐは、署名者の公開鍵１２８である）。

【００３０】

ブロック３１８において、検証モジュール１１８は、暗号化処理されたデータ１２２としてコンピュータ装置１０４内で表される受信メッセージＭとその対応する署名σを、Ｍをハッシュしてｅ$_{\Phi}$（ｒ＊Ｐ、ｈ（Ｍ））を計算し、それをｅ$_{\Phi}$（Ｐ、σ）と比較することによって検証する。これらが等しい場合、暗号化処理データ１２２（署名済みメッセージＭ）は検証済みである。それ以外の場合は、署名済みの元のデータの完全性（ｉｎｔｅｇｒｉｔｙ）は破損している。

【００３１】

Ｃａｒｔｉｅｒ対形成の評価

この節では、特定の場合に、検証／復号化モジュール１１８（例えばブロックを参照）のオペレーションがどのようにＣａｒｔｉｅｒ対形成１２０を明示的に計算できるかを示す。具体的には、この節では、同種写像の次数が素数であり、楕円曲線の群の位数に互いに素であるか、または多くとも次数の二乗で群の位数が割り切れる場合、Ｃａｒｔｉｅｒ対形成を計算する方法を説明する。ここでは、実質的に暗号化プロトコルの関心事のすべての場合を扱う。これは通常、素数の群位数、または大きい素数に２または３のような小さい余因数を乗じたものと等しい群位数を持つことが望ましいからである。１つの実施態様において、これらのオペレーションは図３のブロック３１８のオペレーションを説明する。もう１つの実施態様において、これらのオペレーションは図４のブロック４０８およびブロック４１６のオペレーションを説明する。

【００３２】

φ：Ｅ$_{1}$→Ｅ$_{2}$を有限体ｋにわたる楕円曲線の同種写像とする。最初に、同種写像を反転させる、つまりＱ∈Ｅ$_{2}$を与えられてφ（Ｐ）＝Ｑとなるような$P \in E_1$を求める計算タスクを検討する。反転イメージは、φが同形でない限り一意ではない。ｍ倍写像は：［ｍ］：Ｅ→Ｅにマップする。

【００３３】

【数４】

$$n = \acute{e}E(k)$$

【００３４】

とする。すると、Ｅ上のすべてのｋ－有理点はｎ－ねじれ点である。ｍが任意の整数であ

る場合、Ｅ（ｋ）上で［ｍ］＝［ｍ　ｍｏｄ　ｎ］である。ｇｃｄ（ｍ、ｎ）＝１であると仮定する。これはつまり、［ｍ］がＥ（ｋ）の順列を与えるということである。ｍ’≡ｍ－１ｍｏｄ　ｎである場合、ｍ’倍写像［ｍ’］は反転を与える。なぜなら、［ｍ’］ｏ［ｍ］＝［ｍ’ｍ］＝［ｍ’ｍ　ｍｏｄ　ｎ］＝［１］だからである。

【００３５】

簡単にするために、ｇｃｄ（ｍ、ｎ）≠１の場合、ｍ＝１で素数と仮定する。ＰをＥ（ｋ）上の点とする。すると［ｎ／ｌ］［ｌ］（Ｐ）＝［ｎ］（Ｐ）となり、［ｌ］のイメージは指数ｎ／ｌのＥ（ｋ）の部分群である。特に、Ｅ（ｋ）が巡回群である場合、Ｉｍ［ｌ］はサイズｎ／ｌの部分群である。たとえこの場合でも、問題は解決することができる。問題は、同種写像のもとで点のプリイメージを見つけることである。ｇｃｄ（ｎ／ｌ、ｌ）＝１であると仮定する。部分群Ｉｍ［ｌ］で、［ｌ］倍写像は順列であり、したがってこれは反転を有する。正確に言えば、ｌ’≡ｌ－１ｍｏｄ　ｎ／ｌである場合、［ｌ’］Ｐはｌ－ｍａｐによる乗算を介してＰに写像するＩｍ［ｌ］内の点である。証明は同様であり、Ｑ＝［ｌ’］Ｐである場合、［ｎ／ｌ］Ｑ＝Ｏでありかつ［ｌ］Ｑ＝［ｌｌ’］Ｐ＝Ｐであることに留意されたい。次に、ｌ２｜｜ｎかつＥ［ｌ］⊆Ｅ（ｋ）である場合を検討する。ｌ｜ｍおよびｇｃｄ（ｍ／ｌ、ｌ）＝１に対して

【００３６】

【数５】

$$E(k) \cong (Z/mZ) \times (Z/mdZ)$$

【００３７】

となる。ｌ’≡ｌ-1ｍｏｄ（ｎ／ｌ２）とする。ここで

【００３８】

【数６】

$$(n/l^2) = \frac{m^2 d}{l^2}$$

【００３９】

である。写像［ｌ］は、群として以下の式と同形体であるＥ（ｋ）上のｌ－ｍａｐの乗算のイメージの順列である。

Ｚ／（ｍ／ｌ）ＺｘＺ／（ｍｄ／ｌ）Ｚ

Ｑ＝［ｌ’］Ｐとすると、［ｌ］Ｑ＝［ｌｌ’］Ｐかつ

【００４０】

【数７】

$$ll' \equiv 1 \bmod \frac{m^2 d}{l^2}$$

【００４１】

となるので、ｌｌ’≡１ｍｏｄ　ｍ／ｌさらにｍｏｄ　ｍｄ／ｌとなる。したがって［ｌ］Ｑ＝［ｌ］Ｐ＝Ｐである。

【００４２】

φ：$E_1 \rightarrow E_2$を同種写像とし、

【００４３】

【数８】

$$\hat{\phi}$$

【００４４】

を双対とし、$P \in E_2$とする。ｍ＝ｄｅｇφと設定する。すると、

【００４５】

【数９】

$$[1/m]_{E_1} \hat{\phi}(P)$$

【００４６】
はＰの反転である。ここで、前節に従い、
【００４７】
【数１０】
$[1/m]_{E_1}$

【００４８】
によりE_1の［ｍ］写像倍を反転する手順を意味する。これは、以下の式から導かれる。
【００４９】
【数１１】
$$[1/\mathrm{m}]_{E_1}\hat{\phi}(P)=[1/m]_{E_1}\hat{\phi}\phi(Q)\ \text{where}\ P=\phi(Q)=[1/\mathrm{m}]_{E_1}[m]_{E_1}Q=\mathrm{Q}.$$

【００５０】
このようにして、同種写像は、
【００５１】
【数１２】
$\hat{\phi}$

【００５２】
を評価するために使用される回数で、反転される。
【００５３】
例示的なアプリケーション
φ：$E_1 \rightarrow E_2$を同種写像とする。すると、以下の双一次対形成がある。
【００５４】
【数１３】
$$e_{\phi}:\ker\phi\times\ker\hat{\phi}\rightarrow\mu_{\deg\phi}.$$

【００５５】
この対形成は、以下の有用な特性を満足させる。
e_{ϕ}（Ｐ、φ（Ｑ））＝$e_{\deg\phi}$（Ｐ、Ｑ）
ここで、右辺の数量は、ｄｅｇφ－ねじれ点のＷｅｉｌ対形成である。写像
【００５６】
【数１４】
$$\phi:E_1[\deg]\rightarrow\ker\hat{\phi}$$

【００５７】
が（核ｋｅｒφについて）主観的（ｓｕｂｊｅｃｔｉｖｅ）であるためである。この識別は、e_{ϕ}対形成を評価するために使用される。
【００５８】
ｄｅｇφ＝１を素の次数の同種写像とする。E_1［ｌ］⊆E_1（ｋ）であり、l^3で
【００５９】
【数１５】
$\acute{e}E_1(k)$

【００６０】
が割り切れないと仮定する。すると、
【００６１】
【数１６】
$$(P,Q)\in\ker\phi\times\ker\hat{\phi}$$

【００６２】
が与えられ、Ｑがφ：Ｅ$_1$［ｌ］→Ｅ$_2$のイメージ内にあるので、同種写像φは前述のように、Ｑに写像する点Ｒ∈Ｅ$_1$［ｌ］を求めるために反転される。ｅφ（Ｐ、Ｑ）の値を求めるためにＷｅｉｌ対形成ｅ$_1$（Ｐ、Ｒ）が計算される。これにより、Ｃａｒｔｉｅｒ対形成を計算するために同種写像φ
【００６３】
【数１７】

$$\hat{\phi}$$

【００６４】
の１回の評価で確率的多項式時間アルゴリズムが導かれる。φしか手元にない場合でも
【００６５】
【数１８】

$$e_{\phi}(P,Q) = e_{\hat{\phi}}(Q,P)^{-1}$$

【００６６】
であることを使用することによってｅ$_\phi$（Ｐ、Ｑ）を評価できることに注目し、後者を計算するためにφを計算する。
【００６７】
【数１９】

$$\hat{\phi}$$

【００６８】
を計算する必要はない。特に、
【００６９】
【数２０】

$$\hat{\phi}$$

【００７０】
またはφは効率的に評価することができる。このようにして、システム１００のシステムおよび方法は、Ｃａｒｔｉｅｒ対形成１１２を計算するための効率的なアルゴリズムを提供する。
【００７１】
例示的な識別ベースの暗号化
図４は、Ｃａｒｔｉｅｒ対形成に基づく識別ベース暗号化（ＩＢＥ）のためのシステム１００の例示的な手順４００を示している。データを暗号化および復号化するために選択された特定の対形成ベースのＩＢＥアルゴリズムは、任意であり、実施態様のために選択された特定の暗号学体系の機能である。例えば、Ｃａｒｔｉｅｒ対形成１１２が決定されると、対形成は、可能な対形成ベースのＩＢＥ暗号化アルゴリズムのいずれかを使用して元のデータをそれぞれ暗号化するために使用される。説明のために、手順４００のオペレーションは図１のコンポーネントに関して説明される。コンポーネント参照番号の左端の数字は、コンポーネントが最初に出現する特定の図を識別する。
【００７２】
ブロック４０２において、公開鍵生成プログラム（ＰＫＧ）は、パブリックパラメータとして、有限体Ｆ$_q$にわたる２つのアーベル多様体ＥおよびＥ’、同種写像Φ、ＥからＥ’の次数ｍを生成する。１つの実施態様において、公開鍵生成プログラムは、署名／暗号化モジュール１１０によって実施される（図１）。もう１つの実施態様において、公開鍵生成プログラムは、「別のプログラムモジュール」１１１である。ブロック４０４において、公開鍵生成プログラムは、Φの核内のＥ１２４上の点Ｐを生成するが、これもパブリックである。ブロック４０６において、公開鍵生成プログラムは、主秘密鍵としてランダ

ム整数ｓを生成し、点ｓ＊Ｐを公開する（公開鍵１２８）。１つの実施態様において、ブロック４０６で、公開鍵生成プログラムはさらに、２つの暗号ハッシュ関数h_1およびh_2をパブリックに指定する。例示的な説明のため、ハッシュ関数は図１の「他のデータ」１１４のそれぞれの部分として示されている。ハッシュ関数h_1は、ビットストリングをとり、これらを双対同種写像の核内のＥ’１２４上の点Ｐにハッシュする。ハッシュ関数h_2は、有限体$Fq^{\ddagger}$の乗法群内のｍを割り切れる位数の要素をとり、これらをシステムのメッセージの長さと等しい長さ（ｈ）のビットストリングにハッシュする。したがって、公開鍵生成プログラムによって使用可能になるシステムのパブリック情報は（Ｅ、Ｅ’、F_q、Φ、Ｐ、ｓ＊Ｐ、h_1、h_2、ｎ）である。

【００７３】

識別ＩＤ（例えば、復号モジュール１１８などの暗号化メッセージの受信側）は、以下のようにＰＫＧ（公開鍵権限）から識別に対応する秘密鍵を抽出することができる。公開鍵生成プログラムは、h_1（ＩＤ）＝Q_{ID}を計算し、メッセージを受信したＩＤに秘密鍵ｓ＊Q_{ID}を送信して戻す。ＰＫＧは、メッセージを受信したＩＤに復号鍵ｓ＊ＱＩＤを送信して戻す。

【００７４】

ブロック４０８において、署名／暗号化モジュール１１０は、h_1（ＩＤ）＝Q_{ID}を計算することによりメッセージ（例えば元のデータ）を識別ＩＤに暗号化し、ランダム整数ｒ、モジュロｍを選択する。署名／暗号化モジュール１１０は、Q_{ID}とのｓ＊ＰのＣａｒｔｉｅｒ対形成１１２、g_{ID}＝ｅΦ（ｓ＊Ｐ、Q_{ID}）を計算する。署名／暗号化モジュール１１０は、暗号化データ（または暗号文）１１６を生成するために、メッセージＭを暗号化する。したがって、データは、識別ＩＤおよび算出されたＣａｒｔｉｅｒ対形成の関数として暗号化される。１つの実施態様において、識別ＩＤは、例えばビットストリングとして表されるような、人の電子メールアドレスである。例えば、ビットストリングＩＤは、第２のアーベル多様体（双対同種写像の核内）上の点にハッシュされる。この点をＱ＿ＩＤと呼ぶ。次に、暗号化プログラム１１０は、システムのグローバル公開鍵（ＰＫＧによって保守される）とのＱ＿ＩＤのＣａｒｔｉｅｒ対形成１１２を計算する。その対形成の値は、ｇ＿ＩＤと呼ばれる。算出されたＣａｒｔｉｅｒ対形成に関して、暗号化プログラム１１０は、対形成を評価するためにｓ＊Ｐを使用するが、さらにランダムｒを生成してｒ＊Ｐを送信する。

【００７５】

ブロック４１０において、署名／暗号化モジュール１１０は暗号文ｃ＝（Ｕ、Ｖ）を送信する。ここでＵ＝ｒ＊ＰかつＶ＝Ｍ＋h_2（g_{ID}^{r}）であり、「＋」符号はリモートコンピュータ装置１０４へのビットストリングの２進加算を示す。ブロック４１２において、および暗号化されたデータ１１６（コンピュータ装置１０４に関して暗号化データ１２２として示される）の受信に応じて、復号化モジュール１１８は、暗号化データ１２２に対応する秘密鍵ｓ＊Q_{ID}をＰＫＧ（公開鍵権限）から抽出する。ブロック４１４において、復号化モジュール１１８は、Ｕおよびｓ＊Q_{ID}のＣａｒｔｉｅｒ対形成１２０、h_{ID}＝e_{Φ}（Ｕ、ｓ＊Q_{ID}）を計算するために秘密鍵を使用する。ブロック４１６において、復号化モジュール１１８は、暗号化されたデータ１２２をＭ＝Ｖ＋h_2（h_{ID}）として復号化する。

【００７６】

例示的なオペレーティング環境

図５は、Ｃａｒｔｉｅｒ対形成に基づくデータの暗号化処理が全体としてまたは部分的に実施される適切なコンピューティング環境の例を示している。例示的なコンピューティング環境５００は、図１の例示的なシステムおよび図２～図４の例示的なオペレーションに適切なコンピューティング環境の一例に過ぎず、本明細書に説明されているシステムおよび方法の使用の範囲または機能に関していかなる制限を示唆することも意図するものではない。さらに、コンピューティング環境５００は、コンピューティング環境５００に示された１つのコンポーネントまたはその組み合わせに対して依存関係または必要条件を有

するものと解釈すべきではない。

【００７７】

本明細書に説明されている方法およびシステムは、数多くの他の一般的用途または特殊用途のコンピューティングシステム、環境、または構成で動作可能である。使用に最適なさまざまな既知のコンピューティングシステム、環境、および／または構成の例には、パーソナルコンピュータ、サーバーコンピュータ、マイクロプロセッサシステム、マイクロプロセッサベースのシステム、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、上記のシステムまたは装置のいずれかを含む分散コンピューティング環境などが含まれるが、これらに限定されることはない。フレームワークのコンパクトまたはサブセットバージョンもまた、ハンドヘルドコンピュータまたは他のコンピュータ装置のような、リソースが制限されているクライアントにおいて実装することができる。本発明は、タスクが通信ネットワークを通じてリンクされたリモート処理装置によって実行される分散コンピューティング環境においても実施される。分散コンピューティング環境において、プログラムモジュールは、ローカルおよびリモートの記憶装置に配置することができる。

【００７８】

図５を参照すると、Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理する例示的なシステムは、例えば図１のシステム１００を実装するコンピュータ５１０の形態の汎用コンピュータ装置を含んでいる。以下で説明されているコンピュータ５１０の態様は、図１のコンピュータ装置１０２および／または１０４の例示的な実施態様である。コンピュータ５１０のコンポーネントは、処理装置５２０（１つまたは複数）、システムメモリ５３０、およびシステムメモリを含むさまざまなシステムコンポーネントを処理装置５２０に接続するシステムバス５２１を含むことができるが、これらに限定されることはない。システムバス５２１は、メモリバスまたはメモリコントローラ、周辺バス、およびさまざまなバスアーキテクチャのいずれかを使用するローカルバスを含む、任意のタイプのバス構造であってもよい。限定的ではなく例示的に、そのようなアーキテクチャは、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、ＥＩＳＡバス、ＶＥＳＡローカルバス、およびメザニンバスとも呼ばれるＰＣＩバスを含むことができる。

【００７９】

コンピュータ５１０は通常、各種のコンピュータ読取り可能媒体を含んでいる。コンピュータ読取り可能媒体は、コンピュータ５１０がアクセスでき、揮発性および不揮発性媒体、取り外し可能および固定式の媒体を含む任意の使用可能な媒体であってもよい。一例として、コンピュータ読取り可能媒体は、コンピュータ記憶媒体および通信媒体を備えることができるが、これらに限定されることはない。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュールおよびその他のデータなどの情報のストレージのための任意の方法または技術において実装された揮発性および不揮発性の、取り外し可能および固定式の媒体を含んでいる。コンピュータストレージ媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリその他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤ（デジタル多用途ディスク）、またはその他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ、またはその他の磁気記憶装置、あるいは所望の情報を格納するために使用することができ、コンピュータ５１０によってアクセスすることができる他の媒体を含んでいるが、これらに限定されることはない。

【００８０】

通信媒体は通常、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを搬送波または搬送メカニズムのような変調データ信号で組み入れ、任意の情報伝達媒体を含んでいる。「変調データ信号」という用語は、その信号において信号の情報を符号化するように、その１つまたは複数の特性を設定または変更された信号を意味する。例えば、通信媒体は、有線ネットワークまたは直接配線接続のような有線媒体、および音響、ＲＦ、赤外線など無線媒体を含むが、これらに限定されることはない。上記

の任意の組み合わせも、コンピュータ読取り可能媒体の範囲に含まれる。

【００８１】

システムメモリ５３０は、読み取り専用メモリ（ＲＯＭ）５３１およびランダムアクセスメモリ（ＲＡＭ）５３２のような揮発性メモリおよび／または不揮発性メモリの形態でコンピュータ記憶媒体を含んでいる。起動時などにコンピュータ５１０内の構成要素間の情報の転送を助ける基本ルーチンを含むＢＩＯＳ（基本入出力システム）５３３は通常、ＲＯＭ５３１に格納される。ＲＡＭ５３２は通常、処理装置５２０によって即時アクセス可能および／または現在操作中のデータおよび／またはプログラムモジュールを含んでいる。限定的ではなく例示的に、図５では、オペレーティングシステム５３４、アプリケーションプログラム５３５、その他のプログラムモジュール５３６、およびプログラムデータ５３７を示している。

【００８２】

コンピュータ５１０は、他の取り外し可能／固定式、揮発性／不揮発性のコンピュータ記憶媒体を含めることもできる。ほんの一例として、図５では、固定の不揮発性磁気媒体との間の読み取りまたは書き込みを行なうハードディスクドライブ５４１、取り外し可能の不揮発性磁気ディスク５５２との間の読み取りまたは書き込みを行なう磁気ディスクドライブ５５１、およびＣＤ－ＲＯＭまたはその他の光媒体などの取り外し可能の不揮発性光ディスク５５６との間の読み取りまたは書き込みを行なう光ディスクドライブ５５５を示している。例示的なオペレーティング環境において使用することができる他の取り外し可能／固定、揮発性／不揮発性コンピュータ記憶媒体は、磁気テープカセット、フラッシュメモリカード、ＤＶＤ、デジタルビデオテープ、固体ＲＡＭ、固体ＲＯＭなどを含むが、これらに限定されることはない。ハードディスクドライブ５４１は通常、インタフェース５４０などの固定式メモリインタフェースを通じてシステムバス５２１に接続され、磁気ディスクドライブ５５１および光ディスクドライブ５５５は通常、インタフェース５５０などの取り外し可能メモリインタフェースによってシステムバス５２１に接続される。

【００８３】

図５に示されている前述のドライブおよびそれに伴うコンピュータ記憶媒体は、コンピュータ５１０のコンピュータ可読命令、データ構造、プログラムモジュール、およびその他のデータのストレージを提供する。例えば、図５において、ハードディスクドライブ５４１は、オペレーティングシステム５４４、アプリケーションプログラム５４５、その他のプログラムモジュール５４６、およびプログラムデータ５４７を格納するように示されている。これらのコンポーネントは、オペレーティングシステム５３４、アプリケーションプログラム５３５、その他のプログラムモジュール５３６、およびプログラムデータ５３７と同じにすることも、または異なるものにすることもできることに留意されたい。アプリケーションプログラム５３５は、例えば図１のコンピュータ装置１０２または１０４のプログラムモジュールを含んでいる。プログラムデータ５３７は、例えば図１のコンピュータ装置１０２または１０４のプログラムデータを含んでいる。オペレーティングシステム５４４、アプリケーションプログラム５４５、その他のプログラムモジュール５４６、およびプログラムデータ５４７は、少なくともそれらが異なるコピーであることを示すために本明細書において異なる符号を付けてある。

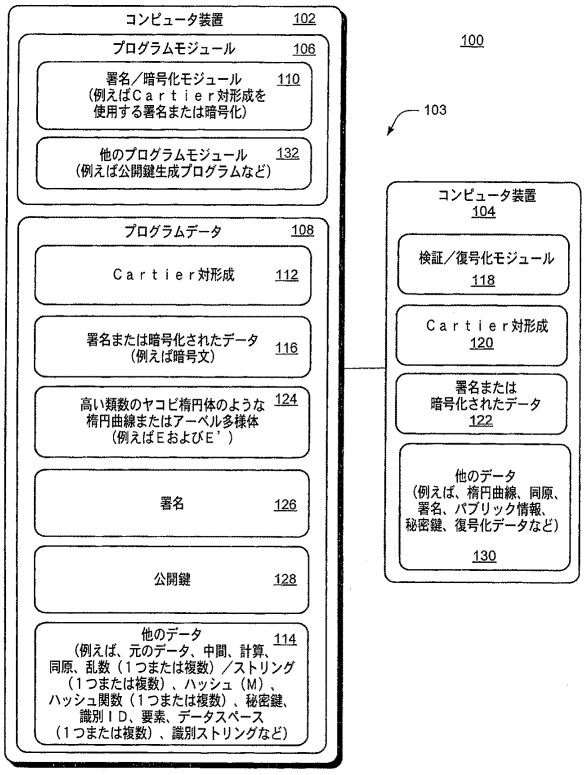
【００８４】

ユーザは、キーボード５６２および一般にマウス、トラックボールまたはタッチパッドと呼ばれるポインティングデバイス５６１などの入力装置を介してコンピュータ５１０にコマンドおよび情報を入力することができる。他の入力装置（図示せず）としては、マイクロフォン、ジョイスティック、ゲームパッド、衛星放送用パラボラアンテナ、スキャナなどを含むことができる。上記およびその他の入力装置は、システムバス５２１に接続されているユーザ入力インタフェース５６０を介して処理装置５２０に接続されることが多いが、パラレルポート、ゲームポート、またはＵＳＢなど他のインタフェースおよびバス構造によって接続することもできる。

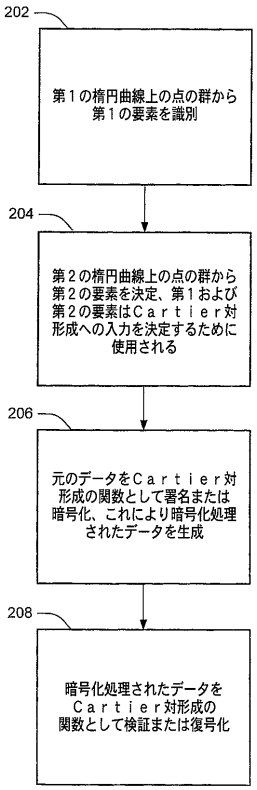
【００８５】
モニタ５９１またはその他の種類の表示装置も、ビデオインタフェース５９０などのインタフェースを介してシステムバス５２１に接続することができる。モニタに加えて、コンピュータは、出力周辺インタフェース５９５を介して接続できるプリンタ５９６およびオーディオデバイス（１つまたは複数）５９７などの他の周辺出力装置を含むこともできる。
【００８６】
コンピュータ５１０は、リモートコンピュータ５８０など、１つまたは複数のリモートコンピュータへの論理接続を使用するネットワーク化された環境において動作する。１つの実施態様において、リモートコンピュータ５８０は、図１のコンピュータ装置１０２またはネットワークコンピュータ１０４を表す。リモートコンピュータ５８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイスまたはその他の共通ネットワークノードであってもよく、その特定の実施態様の機能として、上記でコンピュータ５１０に関連して説明されている要素の多くまたはすべてを含むことができるが、図５においては記憶装置５８１のみが示されている。図５に示されている論理接続は、ローカルエリアネットワーク（ＬＡＮ）５８１およびワイドエリアネットワーク（ＷＡＮ）５７３を含んでいるが、他のネットワークを含むこともできる。そのようなネットワーク環境は、オフィス、企業規模のコンピュータネットワーク、イントラネット、およびインターネットで一般化している。
【００８７】
ＬＡＮネットワーク環境に使用される場合、コンピュータ５１０はネットワークインタフェースまたはアダプタ５７０を介してＬＡＮ５７１に接続される。ＷＡＮネットワーク環境に使用される場合、コンピュータ５１０は通常、モデム５７２またはインターネットなどのＷＡＮ５７３にわたる通信を確立するための他の手段を含んでいる。モデム５７２は、内蔵または外付けであってもよく、ユーザ入力インタフェース５６０または他の適切なメカニズムを介してシステムバス５２１に接続することができる。ネットワーク化された環境において、コンピュータ５１０に関連して示されるプログラムモジュール、またはその部分は、リモート記憶装置に格納することもできる。限定的ではなく例示的に、図５では、リモートアプリケーションプログラム５８５を記憶装置５８１に常駐するものとして示している。示されているネットワーク接続が例示的なものであり、コンピュータ間の通信リンクを確立する他の手段を使用することもできる。
【００８８】
結論
Ｃａｒｔｉｅｒ対形成の暗号化アプリケーションのためのシステムおよび方法を構造的機能および／または方法論的オペレーションもしくは作用に特有の表現で説明してきたが、添付の特許請求の範囲に定義されている実施態様が説明されている特定の機能または作用に必ずしも限定されないことを理解されたい。例えば、署名／暗号化モジュール１１０（図１）および検証／復号化モジュール１１８（図１）は、異なるそれぞれのコンピュータ装置（つまり装置１０２および１０４）上に示されており、もう１つの実施態様において、これらのプログラムモジュールに関連付けられている論理は単一のコンピュータ装置１０２上で実施することができる。したがって、システム１００の特定の機能およびオペレーションは、特許請求された対象を実施する例示的な形態として開示されている。
【図面の簡単な説明】
【００８９】
【図１】Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理する例示的なシステムを示す図である。
【図２】Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理する例示的な手順を示す図である。
【図３】Ｃａｒｔｉｅｒ対形成に基づいてデータに暗号化により署名して検証する例示的な手順を示す図である。

【図４】Ｃａｒｔｉｅｒ対形成を使用して識別ベースの暗号化を実施する例示的な手順を示す図である。
【図５】Ｃａｒｔｉｅｒ　ｐａｉｒｉｎｇに基づくデータの暗号化処理が全体としてまたは部分的に実施される適切なコンピューティング環境の例を示す図である。

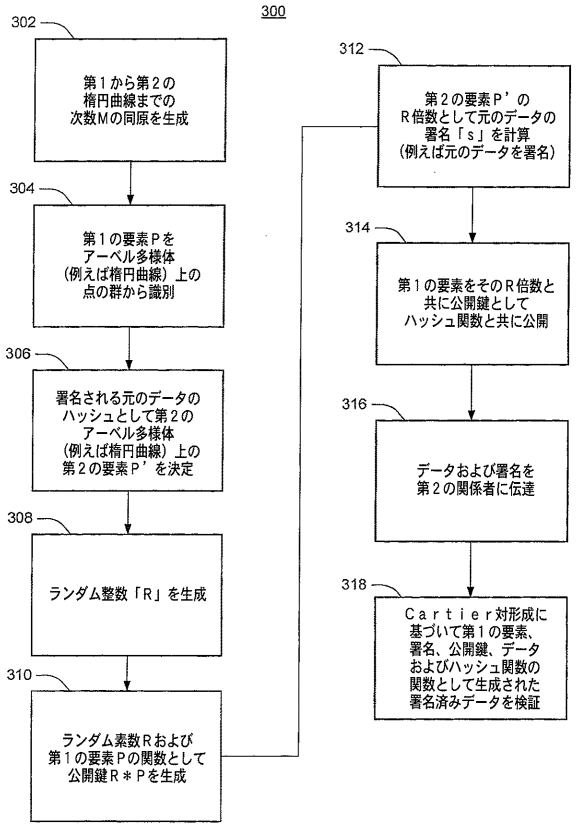
【図１】



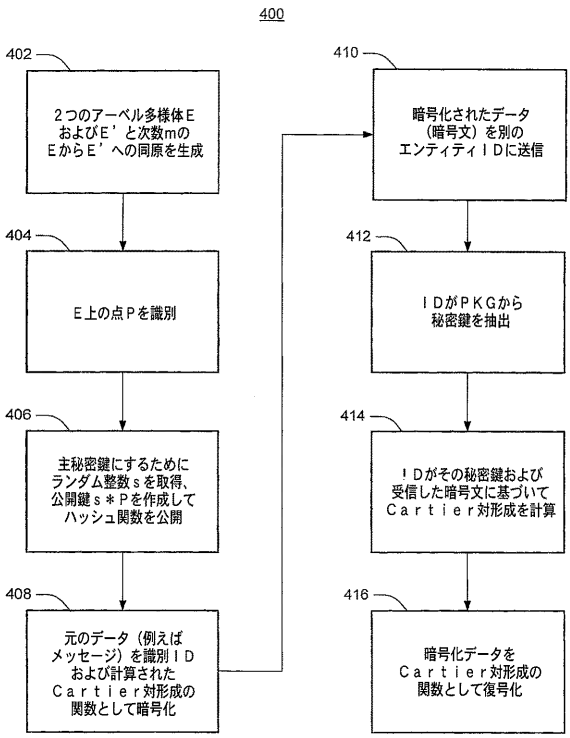
【図２】



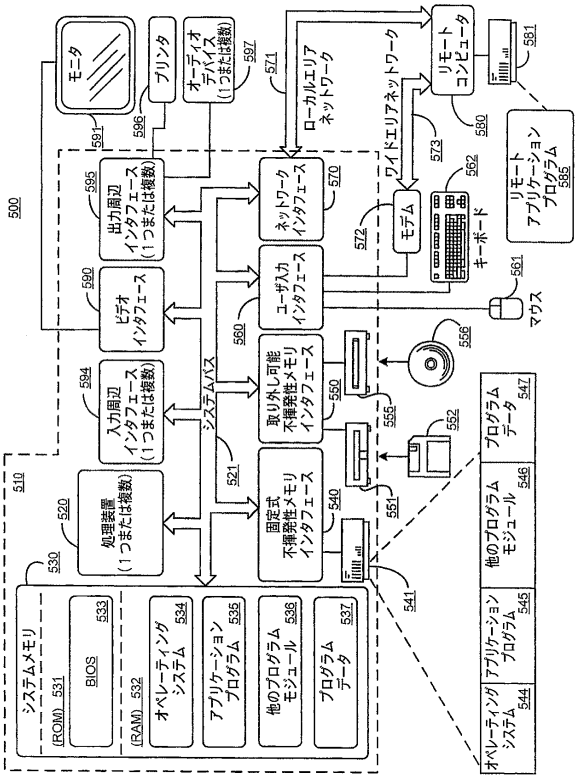
【図３】


300
302
第１から第２の楕円曲線までの次数Ｍの同原を生成
304
第１の要素Ｐをアーベル多様体（例えば楕円曲線）上の点の群から識別
306
署名される元のデータのハッシュとして第２のアーベル多様体（例えば楕円曲線）上の第２の要素Ｐ’を決定
308
ランダム整数「Ｒ」を生成
310
ランダム素数Ｒおよび第１の要素Ｐの関数として公開鍵Ｒ＊Ｐを生成
312
第２の要素Ｐ’のＲ倍数として元のデータの署名「ｓ」を計算（例えば元のデータを署名）
314
第１の要素をそのＲ倍数と共に公開鍵としてハッシュ関数と共に公開
316
データおよび署名を第２の関係者に伝達
318
Ｃａｒｔｉｅｒ対形成に基づいて第１の要素、署名、公開鍵、データおよびハッシュ関数の関数として生成された署名済みデータを検証

【図４】


400
402
２つのアーベル多様体ＥおよびＥ’と次数ｍのＥからＥ’への同原を生成
404
Ｅ上の点Ｐを識別
406
主秘密鍵にするためにランダム整数ｓを取得、公開鍵ｓ＊Ｐを作成してハッシュ関数を公開
408
元のデータ（例えばメッセージ）を識別ＩＤおよび計算されたＣａｒｔｉｅｒ対形成の関数として暗号化
410
暗号化されたデータ（暗号文）を別のエンティティＩＤに送信
412
ＩＤがＰＫＧから秘密鍵を抽出
414
！Ｄがその秘密鍵および受信した暗号文に基づいてＣａｒｔｉｅｒ対形成を計算
416
暗号化データをＣａｒｔｉｅｒ対形成の関数として復号化

【図５】


500
モニタ
591
プリンタ
596
オーディオデバイス（１つまたは複数）
597
ローカルエリアネットワーク
571
リモートコンピュータ
580
581
ワイドエリアネットワーク
573
リモートアプリケーションプログラム
585
出力周辺インタフェース（１つまたは複数）
595
ネットワークインタフェース
570
モデム
572
562
キーボード
561
マウス
ビデオインタフェース
590
ユーザ入力インタフェース
560
システムバス
521
入力周辺インタフェース（１つまたは複数）
594
取り外し可能不揮発性メモリインタフェース
550
556
555
551
固定式不揮発性メモリインタフェース
540
541
処理装置（１つまたは複数）
520
530
510
システムメモリ
(ROM) 531
BIOS 533
(RAM) 532
オペレーティングシステム 534
アプリケーションプログラム 535
他のプログラムモジュール 536
プログラムデータ 537
オペレーティングシステム 544
アプリケーションプログラム 545
他のプログラムモジュール 546
プログラムデータ 547

フロントページの続き

(72)発明者　デニス　エックス．チャールズ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　クリスティン　イー．ローター
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

審査官　中里　裕正

(56)参考文献　特表２００５－５００７４０（ＪＰ，Ａ）
米国特許出願公開第２００５／００１８８５０（ＵＳ，Ａ１）
イアン・Ｆ・ブラケ他，楕円曲線暗号，株式会社ピアソン・エデュケーション，２００１年１２月２０日，p.45-49
Blake, I. F. et al., Elliptic Curves in Cryptography, Cambridge University Press, １９９９年, p.42-46
Silverman, J. H., The Arithmetic of Elliptic Curves, Springer-Verlag New York, Inc., １９８６年, p.107
Tate, J. and Oort, F., Group schemes of prime order, Annales scientifiques de L'E.N.S. serie, １９７０年, tome 3, no 1, p.1-21
Garefalakis, T., The Generalized Weil Pairing and the Discrete Logarithm Problem on Elliptic Curves, Lecture Notes in Computer Science, ２００２年, Vol.2286, p.118-130

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３０
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）