【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成21年3月19日(2009.3.19)

【公開番号】特開2006-221161(P2006-221161A)
【公開日】平成18年8月24日(2006.8.24)
【年通号数】公開・登録公報2006-033
【出願番号】特願2006-20935(P2006-20935)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６２０Ｚ

【手続補正書】
【提出日】平成21年1月30日(2009.1.30)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
２つの異なるアーベル多様体およびそれらの間の同原から、Ｃａｒｔｉｅｒ対形成を生成するステップと、
前記Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理するステップと、
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、署名プロトコルまたは識別ベースの暗号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】
Ｃａｒｔｉｅｒ対形成を生成する前記ステップは、
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と、
前記２つの異なるアーベル多様体の第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ことと、
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項４】
Ｃａｒｔｉｅｒ対形成を生成する前記ステップは、
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と、
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ことと、
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記Ｃａｒｔｉｅｒ対形成は、第１の要素Ｐおよび第２の要素Ｐ’を備え、暗号化処理する前記ステップは、
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の同原Φを決定するステップと、

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倍数として署名を計算するステップと、
前記元のデータを署名して、暗号化処理されたデータを生成するステップと、
前記暗号化処理されたデータを前記同原、前記暗号化処理されたデータのハッシュ、前記署名、および前記第１の要素と前記署名者の公開鍵の関数として検証するステップと、
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記２つの異なるアーベル多様体はそれぞれＥおよびＥ’を備え、
ＥからＥ’までの次数ｍの同原Φを生成するステップと、
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Ｃａｒｔｉｅｒ対形成の関数として暗号化データを生成するためにデータを暗号化するステップと、
をさらに備えることを特徴とする請求項１に記載の方法。
【請求項７】
前記暗号化データは、受信側エンティティの秘密鍵から決定されるＣａｒｔｉｅｒ対形成の関数として復号化できることを特徴とする請求項６に記載の方法。
【請求項８】
２つの異なるアーベル多様体およびそれらの間の同原からＣａｒｔｉｅｒ対形成を生成し、
前記Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理する
ために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ることを特徴とするコンピュータ読取り可能媒体。
【請求項９】
請求項２乃至７いずれかに記載の方法を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さらに備えることを特徴とする請求項８に記載のコンピュータ読取り可能媒体。
【請求項１０】
プロセッサと、
前記プロセッサに接続されたメモリであって、前記メモリは、
２つの異なるアーベル多様体およびそれらの間の同原からＣａｒｔｉｅｒ対形成を生成し、
前記Ｃａｒｔｉｅｒ対形成に基づいてデータを暗号化処理する、
ために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と、
を備えたことを特徴とするコンピュータ装置。
【請求項１１】
前記メモリは、請求項２乃至７いずれかに記載の方法を前記プロセッサに実行させることが可能なコンピュータプログラム命令をさらに含むことを特徴とする請求項１０に記載のコンピュータ装置。