【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７部門第３区分
【発行日】平成29年7月6日(2017.7.6)

【公表番号】特表2016-526342(P2016-526342A)
【公表日】平成28年9月1日(2016.9.1)
【年通号数】公開・登録公報2016-052
【出願番号】特願2016-516248(P2016-516248)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｃ

【手続補正書】
【提出日】平成29年5月29日(2017.5.29)
【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】
第１のエンティティが完全なシークレットを所有していることを、前記完全なシークレットを第２のエンティティに送信することなく前記第２のエンティティに証明することによって、前記第１のエンティティでの前記第１のエンティティ自体の前記第２のエンティティに対する認証方法であって、
前記第１のエンティティでユーザーからの入力を受信することであって、前記完全なシークレットが少なくとも第１の因子及び第２の因子に分割され、前記入力が前記シークレットの前記第２の因子に関係する、受信することと、
前記第１のエンティティで少なくとも前記第１の因子及び前記入力から前記完全なシークレットを再構築することと、
前記第１のエンティティで前記再構築された完全なシークレットを使用して計算を実行し、前記計算の前記結果を前記第２のエンティティに送信することであって、前記結果が前記第２のエンティティでペアリング計算に対する入力を提供する、計算を実行し、前記計算の前記結果を送信することと、
を含む方法。
【請求項２】
前記完全なシークレットが、前記第１の因子及び前記第２の因子を備えた２つの因子に分割され、前記入力が前記第２の因子の予想値を含み、前記完全なシークレットが前記第１の因子及び前記入力から再構築される、請求項１に記載の方法。
【請求項３】
前記シークレットが代数曲線上の点に相当し、前記ペアリング計算が前記代数曲線上のペアリングを備える、請求項２に記載の方法。
【請求項４】
前記第１のエンティティでの前記計算が、前記代数曲線上で別の点を得るために、前記第１のエンティティで、前記シークレットに相当する点、または前記シークレットに相当する少なくとも１つの点から導出される点を前記代数曲線上で乗算することをさらに含み、前記計算の前記結果を前記第２のエンティティに送信することが、その別の点の前記座標を送信することを含む、請求項３に記載の方法。
【請求項５】

前記第１のエンティティの前記シークレットが信頼機関によって発行され、前記第１のエンティティの前記アイデンティティ及び前記信頼機関によって記憶されるマスターシークレットに基づく、請求項３または４に記載の方法。
【請求項６】
前記代数曲線が楕円曲線であって、
第１のエンティティで乱数値を生成することであって、ｘがｑよりも小さい、生成することと、
前記第１のエンティティでＡ＝Ｈ$_1$（ＩＤ$_\alpha$）を計算することであって、上式でＩＤ$_\alpha$は前記第１のエンティティと関連付けられる前記アイデンティティであり、Ｈ$_1$は前記楕円曲線上の点に前記アイデンティティをハッシュするハッシュ関数である、計算することと、
前記第１のエンティティで前記曲線上で別の点Ｕ＝ｘＡを計算し、ＩＤ$_\alpha$及びＵを前記第２のエンティティに送信することと、
前記第２のエンティティで生成される乱数値ｙを受信することであって、ｙがｑよりも小さく、前記再構築された完全なシークレットを使用して前記第１のエンティティで前記計算を実行し、前記結果を前記第２のエンティティに送信することが、新しい点Ｖ＝－（ｘ＋ｙ）（（ｓ－α）Ａ＋αＡ）を計算し、前記第２のエンティティにＶを送信することを含み、前記第１の因子が（ｓ－α）Ａを備え、前記入力が値αを備え、前記クライアントシークレットｓＡが信頼機関によって発行され、前記クライアントアイデンティティに相当する前記点Ａをマスターシークレットｓで乗算することによって前記信頼機関によって得られ、前記ペアリング計算がマッピング
$$G_1 \times G_2 \rightarrow G_T$$
を備え、上式でＧ$_1$及びＧ$_2$が別個であり、ｑが群Ｇ$_1$、Ｇ$_2$、及びＧ$_T$の位数である、受信すること、
をさらに含む、請求項３に記載の方法。
【請求項７】
前記第１のエンティティで時間許可証を受信することをさらに含み、前記再構築された完全なシークレットを使用する前記計算が、前記第２のエンティティに送信するための前記結果を得るために前記時間許可証も使用し、前記時間許可証が前記信頼機関によって発行され、前記時間許可証が、前記第１のエンティティが前記プロトコルを完了する資格のある期間から導出される、請求項５に記載の方法。
【請求項８】
前記第１のエンティティで時間許可証を受信することをさらに含み、前記再構築されたシークレットを使用する前記計算が、前記第２のエンティティに送信するための前記結果を得るために前記時間許可証も使用し、前記時間許可証が前記信頼機関によって発行され、前記時間許可証が、前記第１のエンティティが前記プロトコルを完了する資格のある期間及び追加データから導出される、請求項５に記載の方法。
【請求項９】
前記ペアリング計算が前記第１のエンティティを認証するための前記第２のエンティティでの計算の部分を形成し、前記方法が、前記入力が前記第２の因子に一致しなかったことを示す応答を前記第２のエンティティから受信すること、及び前記第１のエンティティに再び認証を試すように要請することをさらに含む、請求項３から８のいずれか１つに記載の方法。
【請求項１０】
前記方法がさらに、前記第２のエンティティが前記第１のエンティティを認証できるようにするために前記計算の前記結果を送信することに応えて、前記第２のエンティティから応答を受信し、前記応答のデータ値から前記第１のエンティティで暗号鍵を導出することを含み、前記応答の前記データ値が前記ペアリング計算のペアリングの前記結果から得られる、請求項３から８のいずれか１つに記載の方法。
【請求項１１】

前記暗号鍵を導出することが、前記データ値を前記第２のエンティティにとって未知の値乗し、前記結果をハッシュして前記暗号鍵を得ることを含み、前記方法がさらに、前記暗号鍵を使用して、前記第２のエンティティへのメッセージを暗号化し、前記第２のエンティティから受信されるメッセージを解読することを含む、請求項１０に記載の方法。
【請求項１２】
前記第２の因子がＰＩＮを備える、請求項１から１１のいずれか１つに記載の方法。
【請求項１３】
装置が完全なシークレットを所有していることを、他のエンティティに該シークレットを明らかにすることなく、前記他のエンティティに提供することによって前記装置自体を前記他のエンティティに認証するための前記装置であって、
メモリ上に命令を記憶させる少なくとも１つのメモリと、
前記装置で、ユーザーから入力を受信することであって、前記完全なシークレットが少なくとも第１の因子及び第２の因子に分割され、前記入力が前記シークレットの前記第２の因子に関係する、受信する動作と、
前記装置で、すくなくとも前記第１の因子及び前記第２の因子からシークレットを再構築する動作と、
前記再構築されたシークレットを使用して前記装置で計算を実行し、前記他のエンティティに前記計算の前記結果を送信することであって、前記結果がペアリング計算への入力を提供する、計算を実行し、結果を送信する動作と、
を実行するための前記命令を実行するようにプログラミングされた少なくとも１台のプロセッサと、
を備える装置。
【請求項１４】
前記再構築されたシークレットを使用する前記計算が、前記他のエンティティに送信するための前記結果を得るために前記装置で受信される時間許可証も使用し、前記時間許可証が信頼機関によって発行され、前記時間許可証が、前記装置が前記プロトコルを完了する資格のある期間から導出される、請求項１３に記載の装置。
【請求項１５】
前記少なくとも１つのメモリが、前記計算の前記結果を前記他のエンティティに送信することに応えて、前記装置で、前記他のエンティティから受信されるメッセージのデータ値から暗号鍵を導出するための命令をさらに含み、前記応答の前記データ値が前記ペアリング計算のペアリングの前記結果から得られる、請求項１３または１４に記載の装置。
【請求項１６】
クライアントデバイス自体を認証側エンティティに対して、前記クライアントデバイスがシークレットを所有していることを、前記エンティティに前記シークレットを送信することなく証明することによって認証するための前記クライアントデバイスのためのコンピュータプログラムであって、前記クライアントデバイスの１台または複数のプロセッサによって実行されるときに、前記１台または複数のプロセッサに請求項１から１２のいずれか１つに記載の方法を実行させる命令を備える、コンピュータプログラム。
【請求項１７】
第１のエンティティの第２のエンティティに対する多因子ゼロ知識証明認証を実行するコンピュータによって実装される方法。
【請求項１８】
前記方法が前記認証を実行するためにペアリングベースの暗号法を使用する、請求項１７に記載のコンピュータによって実装される方法。
【請求項１９】
前記第１のエンティティが別個のエンティティによって発行され、楕円曲線上の点に相当し、前記第１のエンティティで少なくとも１つの第１の因子及び少なくとも１つの第２の因子に分割されたシークレットと関連付けられ、前記方法がさらに、前記第１のエンティティに記憶される少なくとも前記第１の因子、及びユーザーから受信される少なくとも

前記第２の因子から前記完全なシークレットを、前記第１のエンティティで再構築することと、前記再構築された完全なシークレットを使用して計算を実行し、前記第２のエンティティに前記計算の結果を送信することと、前記第１のエンティティを認証するために計算で前記第１のエンティティから受信される前記結果を前記第２のエンティティで使用することとを含み、前記第１のエンティティでの前記計算が非ペアリング計算であり、前記第２のエンティティでの前記計算がペアリング計算である、請求項１８に記載の方法。
【請求項２０】
前記第２のエンティティが、前記別個のエンティティによって発行される独自のシークレットも記憶し、前記第２のエンティティのシークレットが前記楕円曲線上の点に相当し、前記方法がさらに、
前記第１のエンティティから受信される前記結果をその入力の１つとして採る第１のペアリング、及び前記第２のエンティティのシークレットに相当する前記曲線上の前記点をその入力の１つとして採る第２のペアリングを含むペアリングの積を前記第２のエンティティで実行することと、
前記ペアリングの前記積の前記結果に基づいて前記第１のエンティティを認証するかどうかを判断することと、
を含む、請求項１９に記載の方法。
【請求項２１】
請求項１７から２０のいずれか１つに記載の方法を使用してクライアントを認証することを含み、前記第１のエンティティの前記認証中に計算されるペアリングの前記結果からセッション暗号鍵を導出することをさらに含む、認証鍵共有実行方法。
【請求項２２】
前記第２のエンティティが、前記ペアリングの前記結果から導出される値を前記第１のエンティティに送信することと、前記第１のエンティティが前記受信された値から前記鍵を導出することとをさらに含む、請求項２１に記載の方法。
【請求項２３】
装置で、クライアントからデータを受信することであって、前記データが前記装置に対して前記クライアントを認証する認証試行の部分として提供され前記クライアントが複数の因子に分割された実際のシークレットと関連付けられ、前記データが前記実際のシークレットの再構築を試行するために前記クライアントで使用される複数の因子から導出された、受信することと、
前記データを導出するために使用される前記複数の因子の内の前記因子の内の１つが、前記実際のシークレットの前記複数の因子の内の対応する因子に対して異なると判断し、前記差異の前記範囲を決定することと、
前記差異と関連付けられるエラー値を決定することと、
前記クライアントのいくつかの認証試行について結合されたエラー値の値が所定の最大エラー値を超えないと判断することに応えて、前記クライアントに再び認証を試行するように要請することと、
を含む、コンピュータによって実装される方法。
【請求項２４】
メモリの上に命令を記憶させる少なくとも１つのメモリと、
装置に対してクライアントを認証するための認証試行の部分として前記クライアントからデータを受信することであって、前記クライアントが複数の因子に分割されたシークレットと関連付けられ、前記受信されたデータが前記実際のシークレットの再構築を試行するために前記クライアントで使用される複数の因子から導出された、データを受信する動作と、
記装置で、前記データを導出するために使用される前記複数の因子の前記因子の内の１つが前記実際のシークレットの前記複数の因子の対応する因子に対して異なっていると判断し、前記差異の前記範囲を決定する動作と、
前記差異と関連付けられるエラー値を決定する動作と、

前記クライアントのいくつかの認証試行について結合されたエラー値が所定の最大エラー値を超えないと判断することに応えて、前記クライアントに再び認証を試行するように要請する動作と、
を実行するための前記命令を実行するようにプログラミングされる少なくとも１台のプロセッサと、
を備える装置。
【請求項２５】
１台または複数のプロセッサによって実行されるときに、前記プロセッサに請求項２３に記載の方法を実施させる命令を備えるコンピュータプログラム。
【請求項２６】
コンピュータによって実装される、第１のエンティティでの第２のエンティティへの情報の、前記第２のエンティティに前記実際の情報を送信することのない通信方法であって、前記情報が少なくとも１つの第１の因子及び少なくとも１つの第２の因子に分割されるシークレットと関連付けられ、前記方法が、
少なくとも前記第１の因子及びダミーの第２の因子をダミーシークレットに結合することであって、前記ダミーの第２の因子は、前記第２のエンティティに通信される前記情報に相当する値分、前記第２の因子に対して異なる、結合することと、
前記再構築されたダミーシークレットを使用して前記第１のエンティティで計算を実行し、前記第２のエンティティに前記計算の前記結果を送信することであって、前記結果が前記第２のエンティティで計算に使用されて、前記ダミーの第２の因子と前記第２の因子の前記差異を決定する、計算を実行し、結果を送信することと、
を含む、方法。
【請求項２７】
前記計算が楕円曲線上の暗号ペアリングを含み、前記シークレットが曲線上の点である、請求項２６に記載の方法。
【請求項２８】
前記情報がメッセージの一部を形成し、前記メッセージの各部が少なくとも２つの因子に分割されるシークレットと関連付けられ、前記方法がさらに、少なくとも１つの第１の因子及び少なくとも１つのダミー因子を、前記メッセージの各部のためのダミーシークレットに結合し、前記第２のエンティティが前記メッセージをアセンブルするために、前記ダミーシークレットに基づく計算の前記結果を前記第２のエンティティに送信することをさらに含む、請求項２６または２７に記載の方法。
【請求項２９】
コンピュータによって実装される、第２のエンティティに対する第１のエンティティの認証方法であって、
前記第１のエンティティが、複数の因子に分割される第１のエンティティのシークレットと関連付けられ、前記方法が、前記複数の因子から再構築される前記第１のエンティティのシークレットから導出されるデータに基づいて、バイリニアマッピングを使用して計算を実行し、前記第１のエンティティが前記計算の結果に基づいて前記第１のエンティティのシークレットを所有していたに違いないかどうかを、前記第２のエンティティで判断することをさらに含む、方法。
【請求項３０】
前記シークレットの前記複数の因子から前記第１のエンティティで前記シークレットを再構築することと、
バイリニアマッピングに対する入力を導出するために前記再構築されたシークレットを使用することであって、前記計算を実行することが、前記第２のエンティティと関連付けられるデータに基づいて第１の入力及び第２の有力として前記入力を採る第１のバイリニアマッピングを計算すること、及び前記第１のエンティティと関連付けられるデータに基づく第１の入力、及び第２のエンティティのシークレットから導出される第２の入力データを採る第２のバイリニアマッピングを計算することを含み、前記第１のエンティティの

シークレットが前記第１のエンティティと関連付けられる前記データから構築され、前記第２のエンティティのシークレットが前記第２のエンティティと関連付けられる前記データから構築され、前記マッピングの前記結果、前記マッピングの前記結果から導出される値が、前記第２のエンティティによって、前記第１のエンティティがそのシークレットを所有しているかどうかを判断するために使用できる、使用することと、
をさらに含む、請求項２９に記載の方法。
【請求項３１】
前記計算が、前記第１のバイリニアマッピング及び前記第２のバイリニアマッピングに相当する２つのペアリングを実現するマルチペアリングを実行し、前記マルチペアリングの前記結果が所定値に等しいかどうかを判断することを含む、請求項３０に記載の方法。