【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】令和4年10月13日(2022.10.13)

【国際公開番号】WO2020/076720
【公表番号】特表2022-508757(P2022-508757A)
【公表日】令和4年1月19日(2022.1.19)
【年通号数】公開公報(特許)2022-009
【出願番号】特願2021-545355(P2021-545355)
【国際特許分類】
H04L 9/08(2006.01)
【ＦＩ】
Ｈ０４Ｌ 9/00 ６０１Ａ

【手続補正書】
【提出日】令和4年10月4日(2022.10.4)
【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】
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに通信可能に結合された少なくとも１つのメモリとを備えるシステムであって、
前記少なくとも１つのプロセッサは、
少なくとも１つのセットの秘密パーツの対応する各秘密パーツを、少なくとも１つの対応する対称鍵を使用して対応する単一暗号化秘密パーツに暗号化し、前記対応する単一暗号化秘密パーツを生成し、
対応する少なくとも１つの公開鍵を使用して、対応する各単一暗号化秘密パーツを、対応する二重暗号化秘密パーツに暗号化するように構成され、前記対応する少なくとも１つの公開鍵は、対応する公開／秘密鍵ペアに属し、
２以上の二重暗号化秘密パーツは、秘密を再構築するために使用される、システム。
【請求項２】
対応する各単一暗号化秘密パーツは、単一の公開鍵を使用して暗号化され、前記単一の公開鍵は、単一の公開／秘密鍵ペアに属し、
前記単一の公開／秘密鍵ペアは対応する秘密鍵も含む、請求項１に記載のシステム。
【請求項３】
前記少なくとも１つのプロセッサは、
おのおのが、前記対応する公開／秘密鍵ペアに属する、対応する少なくとも１つの秘密鍵を使用して、各二重暗号化秘密パーツを、前記対応する単一暗号化秘密パーツに復号し、
第２の公開／秘密鍵ペアに属する対応する第２の公開鍵を使用して、対応する単一暗号化秘密パーツのおのおのを再暗号化するようにさらに構成される、請求項１に記載のシステム。
【請求項４】
前記少なくとも１つのプロセッサは、各秘密パーツを、前記少なくとも１つの対応する対称鍵と、排他的ＯＲ（ＸＯＲ）することによって、各秘密パーツを暗号化して、前記対応する単一暗号化秘密パーツを生成するように構成される、請求項１に記載のシステム。

【請求項５】
各二重暗号化秘密パーツは、少なくとも１つの対称鍵と、前記対応する公開／秘密鍵ペアに属する公開鍵との両方を使用して暗号化される、請求項１に記載のシステム。
【請求項６】
各二重暗号化秘密パーツは、前記対応する公開／秘密鍵ペアに属する対応する公開鍵を使用して、２回暗号化される、請求項１に記載のシステム。
【請求項７】
各二重暗号化秘密パーツは、少なくとも１つの対称鍵と、対応するパーツホルダ公開／秘密鍵ペアに属する対応するパーツホルダ公開鍵との両方を使用して暗号化される、請求項１に記載のシステム。
【請求項８】
前記少なくとも１つのプロセッサは、
前記２以上の二重暗号化秘密パーツを受信し、
前記対応する公開／秘密鍵ペアに属する対応する秘密鍵を使用して、前記２以上の二重暗号化秘密パーツのおのおのを、前記対応する単一暗号化秘密パーツに復号し、
対応する各単一暗号化秘密パーツを、対応する秘密パーツに復号し、
ある数の対応する秘密パーツから、前記秘密を再構築するようにさらに構成され、前記数は、以前に前記秘密から作成された秘密パーツの総数のサブセットである、請求項１に記載のシステム。
【請求項９】
対応する各二重暗号化秘密パーツは、複数のパーツホルダのうちそれぞれのパーツホルダに分配され、
前記２以上の二重暗号化秘密パーツは、前記複数のパーツホルダのうち２以上のパーツホルダから受信される、請求項８に記載のシステム。
【請求項１０】
前記少なくとも１つのプロセッサは、
対称暗号化鍵である前記秘密を、複数の秘密パーツから再構築し、
前記対称暗号化鍵を用いてアクションを実行するようにさらに構成される、請求項１に記載のシステム。
【請求項１１】
前記アクションは、前記２以上の二重暗号化秘密パーツから再構築された前記秘密を使用する以下のアクション、すなわち、
第１のデータを暗号化すること、
第２のデータを復号すること、
トランザクションアドレスを生成すること、または
トランザクションに署名すること
のうちの少なくとも１つを備える、請求項１０に記載のシステム。
【請求項１２】
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサに通信可能に結合された少なくとも１つのメモリとを備えるシステムであって、
前記少なくとも１つのプロセッサは、
公開／秘密鍵ペアに属する少なくとも公開鍵を使用して暗号化された、複数の二重暗号化秘密パーツを受信し、
前記複数の二重暗号化秘密パーツのおのおのを、前記公開／秘密鍵ペアに属する秘密鍵を使用して、対応する単一暗号化秘密パーツに復号し、
少なくとも１つの対応する対称鍵を使用して、対応する各単一暗号化秘密パーツを、対応する秘密パーツに復号するように構成され、
秘密は、以前に前記秘密から作成された秘密パーツの総数のうちのサブセットである数の、対応する秘密パーツから再構築される、システム。

【請求項１３】
各二重暗号化秘密パーツは、
対称鍵、または、前記公開／秘密鍵ペアに属する前記公開鍵を使用して、対応する各秘密パーツが、前記対応する単一暗号化秘密パーツに暗号化される第１段階と、
対応する公開／秘密鍵ペアに属する前記公開鍵を使用して、前記対応する単一暗号化秘密パーツが、それぞれの二重暗号化秘密パーツに暗号化される第２段階と
を備える２段階を使用して暗号化された、請求項１２に記載のシステム。
【請求項１４】
前記少なくとも１つのプロセッサは、秘密パーツの前記総数のうち前記数から再構築された前記秘密を使用して、以下のアクション、すなわち、
第１のデータを暗号化すること、
第２のデータを復号すること、
トランザクションアドレスを生成すること、または
トランザクションに署名すること
のうちの少なくとも１つを実行するようにさらに構成される、請求項１２に記載のシステム。
【請求項１５】
前記少なくとも１つのプロセッサは、対応する各単一暗号化秘密パーツを、前記少なくとも１つの対応する対称鍵と、排他的ＯＲ（ＸＯＲ）することによって、対応する各単一暗号化秘密パーツを復号して、前記対応する秘密パーツを生成するように構成される、請求項１２に記載のシステム。
【請求項１６】
前記複数の二重暗号化秘密パーツが、複数のパーツホルダから受信される、請求項１２に記載のシステム。
【請求項１７】
第１の秘密パーツおよび第２の秘密パーツのための前記少なくとも１つの対応する対称鍵は同一である、請求項１または１２に記載のシステム。
【請求項１８】
第１の秘密パーツおよび第２の秘密パーツのための前記少なくとも１つの対応する対称鍵は異なる、請求項１または１２に記載のシステム。
【請求項１９】
秘密パーツを、複数のパーツホルダに安全に配布するための方法であって、
少なくとも１つの対称鍵を使用して、少なくとも１つのセットの秘密パーツの各秘密パーツを、対応する単一暗号化秘密パーツに暗号化するステップと、
対応する公開／秘密鍵ペアに属する対応する少なくとも１つの公開鍵を使用して、対応する各単一暗号化秘密パーツを、対応する二重暗号化秘密パーツに暗号化するステップと、
各二重暗号化秘密パーツを、それぞれのパーツホルダに配布するステップとを備え、
２つ以上の二重暗号化秘密パーツは、秘密を再構築するために使用される、方法。
【請求項２０】
資産暗号化鍵を再構築する方法であって、
公開／秘密鍵ペアに属する少なくとも公開鍵を使用して暗号化された複数の二重暗号化秘密パーツを受信するステップと、
前記公開／秘密鍵ペアに属する秘密鍵を使用して、前記複数の二重暗号化秘密パーツのそれぞれを、対応する単一暗号化秘密パーツに復号化するステップと、
少なくとも1つの対応する対称鍵を使用して、対応する各単一暗号化秘密パーツを、対応する秘密パーツに復号化するステップとを備え、
秘密は、前記秘密から以前に作成された秘密パーツの総数のうちのサブセットである数の、対応する秘密パーツから再構築される、方法。
【手続補正２】

【補正対象書類名】明細書
【補正対象項目名】０００２
【補正方法】変更
【補正の内容】
【０００２】
[0002]本出願は、以下の同時係属中の米国特許出願に関連しており、これらは、参照により本明細書に組み込まれる。
[0003]「ＥＮＣＲＹＰＴＥＤ ＡＳＳＥＴ ＥＮＣＲＹＰＴＩＯＮ ＫＥＹ ＰＡＲＴＳ ＡＬＬＯＷＩＮＧ ＦＯＲ ＡＳＳＥＭＢＬＹ ＯＦ ＡＮ ＡＳＳＥＴ ＥＮＣＲＹＰＴＩＯＮ ＫＥＹ ＵＳＩＮＧ Ａ ＳＵＢＳＥＴ ＯＦ ＴＨＥ ＥＮＣＲＹＰＴＥＤ ＡＳＳＥＴ ＥＮＣＲＹＰＴＩＯＮ ＫＥＹ ＰＡＲＴＳ」（暗号化された資産暗号化鍵パーツのサブセットを使用して資産暗号化鍵のアセンブリを可能にする暗号化された資産暗号化鍵パーツ）と題され、本書と同日付で出願され、参照により本明細書に組み込まれる米国特許出願第１６／５９５，０２０号（代理人整理番号２７０．０３０ＵＳ０１）。