(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6515246号
(P6515246)
(45)発行日　令和1年5月15日(2019.5.15)　(24)登録日　平成31年4月19日(2019.4.19)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E

請求項の数 47　(全 36 頁)

(21)出願番号　特願2018-516682(P2018-516682)
(86)(22)出願日　平成29年2月16日(2017.2.16)
(65)公表番号　特表2019-507510(P2019-507510A)
(43)公表日　平成31年3月14日(2019.3.14)
(86)国際出願番号　PCT/IB2017/050856
(87)国際公開番号　WO2017/145016
(87)国際公開日　平成29年8月31日(2017.8.31)
審査請求日　平成30年7月31日(2018.7.31)
(31)優先権主張番号　1603117.1
(32)優先日　平成28年2月23日(2016.2.23)
(33)優先権主張国　英国(GB)
(31)優先権主張番号　1619301.3
(32)優先日　平成28年11月15日(2016.11.15)
(33)優先権主張国　英国(GB)

早期審査対象出願

(73)特許権者　318001991
エヌチェーン　ホールディングス　リミテッド
NCHAIN HOLDINGS LIMITED
アンティグア・バーブーダ、　セントジョンズ、　４４　チャーチ　ストリート、　フィッツジェラルド　ハウス
Fitzgerald House, 44 Church Street, St. John's, Antigua and Barbuda (AG)
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】情報及び階層的で決定性の暗号化鍵のセキュアな交換のための共通秘密の決定

(57)【特許請求の範囲】
【請求項１】
第１のノードで、前記第１のノード及び第２のノードに共通の共通秘密を決定するコンピュータによって実現される方法であって、前記第１のノードは、準同型性を有する暗号化システムの第１の非対称暗号対に関連付けされ、前記第１の非対称暗号対は、第１のノードのマスター私有鍵及び第１のノードのマスター公開鍵を有し、前記第２のノードは、前記暗号化システムの第２の非対称暗号対に関連付けされ、前記第２の非対称暗号対は、第２のノードのマスター私有鍵及び第２のノードのマスター公開鍵を有し、前記第１のノードのマスター公開鍵は、前記第１及び第２のノードに共通の前記暗号化システムを利用した前記第１のノードのマスター私有鍵の暗号化に基づき、前記第２のノードのマスター公開鍵は、前記第１及び第２のノードに共通の前記暗号化システムを利用した前記第２のノードのマスター私有鍵の暗号化に基づき、前記方法は、
－少なくとも前記第１のノードのマスター私有鍵及び前記第１及び第２のノードに共通する決定性鍵に基づいて第１のノードの第２の私有鍵を決定するステップと、
－少なくとも前記第２のノードのマスター公開鍵及び前記共通の暗号化システムを利用した前記決定性鍵の暗号化に基づいて第２のノードの第２の公開鍵を決定するステップと、
－前記第１のノードの第２の私有鍵及び前記第２のノードの第２の公開鍵に基づいて前記共通秘密を決定するステップと、
を含み、

前記第２のノードは、第１のノードの第２の公開鍵及び第２のノードの第２の私有鍵に基づいて同じ共通秘密を有し、
－前記第１のノードの第２の公開鍵は、少なくとも、前記第１のノードのマスター公開鍵及び前記共通の暗号化システムを利用した前記決定性鍵の暗号化に基づき、
－前記第２のノードの第２の私有鍵は、少なくとも、前記第２のノードのマスター私有鍵及び前記決定性鍵に基づいている方法。
【請求項２】
前記決定性鍵はメッセージに基づく、請求項１に記載の方法。
【請求項３】
－前記メッセージ及び前記第１のノードの第２の私有鍵に基づいて第１の署名付きメッセージを生成するステップと、
－通信ネットワークを介して、前記第１の署名付きメッセージを前記第２のノードに送信するステップと、
を更に含み、
前記第１の署名付きメッセージは、前記第１のノードを認証するために、第１のノードの第２の公開鍵を用いて有効性を確認することができる、請求項２に記載の方法。
【請求項４】
－通信ネットワークを介して、前記第２のノードから第２の署名付きメッセージを受信するステップと、
－前記第２のノードの第２の公開鍵を用いて前記第２の署名付きメッセージの有効性を確認するステップと、
－前記第２の署名付きメッセージの有効性を確認した結果に基づいて、前記第２のノードを認証するステップと、
を更に含み、
前記第２の署名付きメッセージは、前記メッセージ又は第２のメッセージ、及び前記第２のノードの第２の私有鍵に基づいて生成された、請求項２又は３に記載の方法。
【請求項５】
－前記決定性鍵が基づく前記メッセージを生成するステップと、
－通信ネットワークを介して、前記メッセージを前記第２のノードに送信するステップと、
を更に含む、請求項２～４のいずれか１項に記載の方法。
【請求項６】
－通信ネットワークを介して、前記第２のノードから前記メッセージを受信するステップ、
を更に含む、請求項２～４のいずれか１項に記載の方法。
【請求項７】
－通信ネットワークを介して、別のノードから前記メッセージを受信するステップ、
を更に含む、請求項２～４のいずれか１項に記載の方法。
【請求項８】
－データストア、及び／又は前記第１のノードに関連付けられた入力インタフェースから前記メッセージを受信するステップ、
を更に含む、請求項２～４のいずれか１項に記載の方法。
【請求項９】
前記暗号化システムは楕円曲線暗号化（ＥＣＣ）システムであり、前記第１のノードのマスター公開鍵及び第２のノードのマスター公開鍵は、それぞれの第１のノードのマスター私有鍵及び第２のノードのマスター私有鍵と生成元との楕円曲線点乗算に基づく、請求項１～８のいずれか１項に記載の方法。
【請求項１０】
－通信ネットワークを介して、前記第２のノードのマスター公開鍵を受信するステップと、

－前記第１のノードに関連付けられたデータストアに、前記第２のノードのマスター公開鍵を記憶するステップと、
を更に含む、請求項１～９のいずれか１項に記載の方法。
【請求項１１】
－第１のノードにおいて、前記第１のノードのマスター私有鍵及び前記第１のノードのマスター公開鍵を作成するステップと、
－通信ネットワークを介して、前記第１のノードのマスター公開鍵を前記第２のノード及び／又は他のノードに送信するステップと、
－前記第１のノードに関連付けられた第１のデータストアに、前記第１のノードのマスター私有鍵を記憶するステップと、
を更に含む、請求項１～１０のいずれか１項に記載の方法。
【請求項１２】
－前記通信ネットワークを介して、前記第２のノードに、前記共通秘密を決定する方法のために共通の暗号化（ＥＣＣ）システムを用いることを示す通知を送信するステップ、
を更に含み、
前記第１のノードのマスター私有鍵及び前記第１のノードのマスター公開鍵を作成するステップは、
－前記共通の暗号化システムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて前記第１のノードのマスター私有鍵を作成するステップと、
－前記第１のノードのマスター私有鍵の暗号化に基づいて前記第１のノードのマスター公開鍵を決定するステップと、
を更に含む、請求項１１に記載の方法。
【請求項１３】
前記共通の暗号化システムは、共通の生成元による楕円曲線暗号化（ＥＣＣ）システムであり、前記第１のノードのマスター公開鍵（P_{1C}）は、前記第１のノードのマスター私有鍵（V_{1C}）と前記共通の生成元（Ｇ）との楕円曲線点乗算に基づき、

$$P_{1C}=V_{1C}\times G$$

に従って決定される、請求項１２に記載の方法。
【請求項１４】
－メッセージのハッシュの決定に基づいて前記決定性鍵（ＤＫ）を決定するステップ、
を更に含み、
前記第１のノードの第２の私有鍵（V_{2C}）を決定するステップは、

$$V_{2C}=V_{1C}+DK$$

による、前記第１のノードのマスター私有鍵（V_{1C}）及び前記決定性鍵（ＤＫ）のスカラー加算に基づき、
前記第２のノードの第２の公開鍵（P_{2S}）を決定するステップは、

$$P_{2S}=P_{1S}+DK\times G$$

による、前記決定性鍵（ＤＫ）と前記共通の生成元（Ｇ）との楕円曲線点乗算に楕円曲線点加算した第２のノードのマスター公開鍵（P_{1S}）に基づく、請求項１３に記載の方法。
【請求項１５】
前記決定性鍵は、以前の決定性鍵のハッシュを決定することに基づく、請求項１～１４のいずれか１項に記載の方法。
【請求項１６】
前記第１の非対称暗号対及び前記第２の非対称暗号対は、それぞれの以前の第１の非対称暗号対及び以前の第２の非対称暗号対の関数に基づく、請求項１～１５のいずれか１項に記載の方法。
【請求項１７】
対称鍵アルゴリズムを用いた第１のノードと第２のノードとの間のセキュアな通信の方法であって、

－請求項１～１６のいずれか１項に記載の方法によって共通秘密を決定するステップと、
－前記共通秘密に基づいて対称鍵を決定するステップと、
－前記対称鍵を用いて、第１の通信メッセージを暗号化された第１の通信メッセージに暗号化するステップと、
－通信ネットワークを介して、前記暗号化された第１の通信メッセージを前記第１のノードから前記第２のノードに送信するステップと、
を含む、方法。
【請求項１８】
－通信ネットワークを介して、前記第２のノードから暗号化された第２の通信メッセージを受信するステップと、
－前記対称鍵を用いて、前記暗号化された第２の通信メッセージを第２の通信メッセージに復号するステップと、
を更に含む、請求項１７に記載の方法。
【請求項１９】
第１のノードと第２のノードとの間のオンライントランザクションを行う方法であって、
－請求項１～１６のいずれか１項に記載の方法によって共通秘密を決定するステップと、
－前記共通秘密に基づいて対称鍵を決定するステップと、
－前記対称鍵を用いて、第１のトランザクションメッセージを暗号化された第１のトランザクションメッセージに暗号化するステップと、
－通信ネットワークを介して、前記暗号化された第１のトランザクションメッセージを前記第１のノードから前記第２のノードに送信するステップと、
－通信ネットワークを介して、前記第２のノードから暗号化された第２のトランザクションメッセージを受信するステップと、
－前記対称鍵を用いて、前記暗号化された第２のトランザクションメッセージを第２のトランザクションメッセージに復号するステップと、
を含む方法。
【請求項２０】
第１のノードで、第２のノードと共通の共通秘密を決定するためのデバイスであって、前記第１のノードは、第１のノードのマスター私有鍵及び第１のノードのマスター公開鍵を有する第１の非対称暗号対に関連付けられ、前記第２のノードは、第２のノードのマスター私有鍵及び第２のノードのマスター公開鍵を有する第２の非対称暗号対に関連付けられ、前記デバイスは、前記共通秘密を決定するために請求項１～１９のいずれか１項に記載の方法を行うための第１の処理デバイスを備えているデバイス。
【請求項２１】
第１のノードと第２のノードとの間のセキュアな通信又はセキュアなオンライントランザクションを行うためのデバイスであって、
－請求項１７～１９のいずれか１項に記載の方法を行う
ための第１の処理デバイスを備えているデバイス。
【請求項２２】
前記第１のノードのマスター私有鍵のうちの１つ又は複数を記憶するための第１のデータストアを更に備えている請求項２０又は２１に記載のデバイス。
【請求項２３】
前記第１のデータストアは、前記第１のノードのマスター公開鍵、前記第２のノードのマスター公開鍵、及びメッセージのうちの１つ又は複数を更に記憶する、請求項２２に記載のデバイス。
【請求項２４】
通信ネットワークを介して、メッセージ、前記第１のノードのマスター公開鍵、前記第

２のノードのマスター公開鍵、第１の署名付きメッセージ、第２の署名付きメッセージ、共通の暗号化システムを用いることを示す通知のうちの１つ又は複数を送信及び／又は受信するための通信モジュールを更に備えている請求項２０～２３のいずれか１項に記載のデバイス。

【請求項２５】

前記共通の暗号化システムは、共通の生成元を備えた楕円曲線暗号化（ＥＣＣ）システムである、請求項２４に記載のデバイス。

【請求項２６】

第１のノードと第２のノードとの間の共通秘密を決定するためのシステムであって、

－前記第１のノードは、準同型性を有する暗号化システムの第１の非対称暗号対に関連付けされ、前記第１の非対称暗号対は、第１のノードのマスター私有鍵及び第１のノードのマスター公開鍵を有し、

－前記第２のノードは、前記暗号化システムの第２の非対称暗号対に関連付けされ、前記第２の非対称暗号対は、第２のノードのマスター私有鍵及び第２のノードのマスター公開鍵を有し、前記第１のノードのマスター公開鍵は、前記第１及び第２のノードに共通の前記暗号化システムを利用した前記第１のノードのマスター私有鍵の暗号化に基づき、前記第２のノードのマスター公開鍵は、前記第１及び第２のノードに共通の前記暗号化システムを利用した前記第２のノードのマスター私有鍵の暗号化に基づき、

前記システムは、

－前記第１のノードに関連付けられた第１の処理デバイスであって、

－少なくとも前記第１のノードのマスター私有鍵及び前記第１及び第２のノードに共通の決定性鍵に基づいて第１のノードの第２の私有鍵を決定し、

－少なくとも前記第２のノードのマスター公開鍵及び前記共通の暗号化システムを利用した前記決定性鍵の暗号化に基づいて第２のノードの第２の公開鍵を決定し、

－前記第１のノードの第２の私有鍵及び前記第２のノードの第２の公開鍵に基づいて前記共通秘密を決定する

ように構成される、第１の処理デバイスと、

－前記第２のノードに関連付けられた第２の処理デバイスであって、

－少なくとも、前記第１のノードのマスター公開鍵及び前記共通の暗号化システムを利用した前記決定性鍵の暗号化に基づいて第１のノードの第２の公開鍵を決定し、

－少なくとも、前記第２のノードのマスター私有鍵及び前記決定性鍵に基づいて第２のノードの第２の私有鍵を決定し、

－前記第１のノードの第２の公開鍵及び第２のノードの第２の私有鍵に基づいて前記共通秘密を決定する

ように構成される、第２の処理デバイスと、

を備え、

前記第１の処理デバイス及び前記第２の処理デバイスは同じ共通秘密を決定するシステム。

【請求項２７】

前記決定性鍵はメッセージに基づき、前記第１の処理デバイスは、

－前記メッセージ及び前記第１のノードの第２の私有鍵に基づいて第１の署名付きメッセージを作成し、

－通信ネットワークを介して、前記第１の署名付きメッセージを前記第２のノードに送信する

ように更に構成され、

前記第２の処理デバイスは、

－前記第１の署名付きメッセージを受信し、

－前記第１のノードの第２の公開鍵を用いて前記第１の署名付きメッセージの有効性を確認し、

－前記有効性を確認された前記第１の署名付きメッセージの結果に基づいて前記第１の

ノードを認証する
ように更に構成されている請求項２６に記載のシステム。
【請求項２８】
前記第２の処理デバイスは、
－前記メッセージ又は第２のメッセージ、及び前記第２のノードの第２の私有鍵に基づいて第２の署名付きメッセージを作成し、
－前記第２の署名付きメッセージを前記第１のノードに送信する
ように更に構成され、
前記第１の処理デバイスは、
－前記第２の署名付きメッセージを受信し、
－前記第２のノードの第２の公開鍵を用いて前記第２の署名付きメッセージの有効性を確認し、
－前記有効性を確認された第２の署名付きメッセージの結果に基づいて前記第２のノードを認証する
ように更に構成されている請求項２６又は２７に記載のシステム。
【請求項２９】
前記第１の処理デバイスは、
－前記決定性鍵が基づく前記メッセージを作成し、
－前記メッセージを送信する
ように構成され、
前記第２の処理デバイスは、
－前記メッセージを受信する
ように構成される、請求項２６～２８のいずれか一項に記載のシステム。
【請求項３０】
メッセージは、別のノードによって作成され、前記第１の処理デバイスは、
－前記メッセージを受信する
ように構成され、
前記第２の処理デバイスは、
－前記メッセージを受信する
ように構成される、請求項２６～２９のいずれか一項に記載のシステム。
【請求項３１】
システムデータストア及び／又は入力インタフェースを更に備え、前記第１の処理デバイス及び前記第２の処理デバイスは、前記システムデータストア及び／又は入力インタフェースから、メッセージ又は第２のメッセージを受信する、請求項２６～３０のいずれか１項に記載のシステム。
【請求項３２】
前記第１の処理デバイスは、前記システムデータストア及び／又は入力デバイスから前記第２のノードのマスター公開鍵を受信し、前記第２の処理デバイスは、前記システムデータストア及び／又は入力デバイスから前記第１のノードのマスター公開鍵を受信する、請求項３１に記載のシステム。
【請求項３３】
前記暗号化システムは、楕円曲線暗号化（ＥＣＣ）システムであり、前記第１のノードのマスター公開鍵、第２のノードのマスター公開鍵は、それぞれの第１のノードのマスター私有鍵及び第２のノードのマスター私有鍵と生成元との楕円曲線点乗算に基づく、請求項２６～３２のいずれか１項に記載のシステム。
【請求項３４】
－前記第１のノードのマスター私有鍵を記憶するための、前記第１のノードに関連付けられた第１のデータストアと、
－前記第２のノードのマスター私有鍵を記憶するための、前記第２のノードに関連付けられた第２のデータストアと、

を更に備える、請求項２６～３３のいずれか１項に記載のシステム。
【請求項３５】
前記第１の処理デバイスは、
－前記第１のノードのマスター私有鍵及び前記第１のノードのマスター公開鍵を作成し、
－前記第１のノードのマスター公開鍵を送信し、
－前記第１のノードのマスター私有鍵を前記第１のデータストアに記憶するように構成され、
前記第２の処理デバイスは、
－前記第２のノードのマスター私有鍵及び前記第２のノードのマスター公開鍵を作成し、
－前記第２のノードのマスター公開鍵を送信し、
－前記第２のノードのマスター私有鍵を前記第２のデータストアに記憶するように構成されている
請求項３４に記載のシステム。
【請求項３６】
－前記第１のデータストアは、前記第２のノードのマスター公開鍵を受信して記憶し、
－前記第２のデータストアは、前記第１のノードのマスター公開鍵を受信して記憶する、
請求項３４又は３５のいずれかに記載のシステム。
【請求項３７】
前記第１の処理デバイスは、
－共通の暗号化システムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて前記第１のノードのマスター私有鍵を作成し、
－前記第１のノードのマスター私有鍵の暗号化に基づいて前記第１のノードのマスター公開鍵を決定するように更に構成され、
前記第２の処理デバイスは、
－共通の暗号化システムにおいて指定される前記許容可能な範囲におけるランダムな整数に基づいて前記第２のノードのマスター私有鍵を作成し、
－前記第２のノードのマスター私有鍵の暗号化に基づいて前記第２のノードのマスター効果鍵を決定するように更に構成される、請求項２６～３６のいずれか１項に記載のシステム。
【請求項３８】
前記共通の暗号化システムは、共通の生成元（Ｇ）を備えた楕円曲線暗号化（ＥＣＣ）システムであり、
前記第１の処理デバイスは、
$$P_{1C} = V_{1C} \times G$$
の式による、前記第１のノードのマスター私有鍵（V_{1C}）と共通の生成元との楕円曲線点乗算に基づいて第１のノードのマスター公開鍵（P_{1C}）を決定するように更に構成され、
前記第２の処理デバイスは、
$$P_{1S} = V_{1S} \times G$$
の式による、前記第２のノードのマスター私有鍵（V_{1S}）と前記共通の生成元との楕円曲線点乗算に基づいて第２のノードのマスター公開鍵（P_{1S}）を決定するように更に構成されている
請求項３７に記載のシステム。
【請求項３９】
前記第１の処理デバイスは、
－メッセージのハッシュに基づいて前記決定性鍵（ＤＫ）を決定する
ように構成され、

－前記第１のノードの第２の私有鍵（V_{2C}）は、
$V_{2C}=V_{1C}+DK$
の式による、前記第１のノードのマスター私有鍵（V_{1C}）と前記決定性鍵（ＤＫ）とのスカラー加算に基づき、
－前記第２のノードの公開鍵（P_{2S}）は、
$P_{2S}=P_{1S}+DK\times G$
の式による、第２のノードのマスター公開鍵（P_{1S}）を、前記決定性鍵（ＤＫ）と前記共通の生成元（Ｇ）との楕円曲線点乗算に楕円曲線点加算したものに基づき、
前記第２の処理デバイスは、
－前記メッセージのハッシュに基づいて前記決定性鍵（ＤＫ）を決定する
ように構成され、
－前記第２のノードの第２の私有鍵（V_{2S}）は、
$V_{2S}=V_{1C}+DK$
の式による、前記第２のノードのマスター私有鍵（V_{1S}）と前記決定性鍵（ＤＫ）とのスカラー加算に基づき、
－前記第１のノードの公開鍵（P_{2C}）は、
$P_{2C}=P_{1C}+DK\times G$
の式による、前記第１のノードのマスター公開鍵（P_{1C}）を、前記決定性鍵（ＤＫ）と前記共通の生成元（Ｇ）との前記楕円曲線点乗算に楕円曲線点加算したものに基づいている
請求項２６～３８のいずれか１項に記載のシステム。
【請求項４０】
－前記第１の処理デバイスに関連付けられ、通信ネットワークを介して、メッセージ、前記第１のノードのマスター公開鍵、前記第２のノードのマスター公開鍵、第１の署名付きメッセージ、第２の署名付きメッセージ、及び共通の暗号化システムを用いることを示す通知のうちの１つ又は複数を送信及び／又は受信するための第１の通信モジュールと、
－前記第２の処理デバイスに関連付けられ、通信ネットワークを介して、前記メッセージ、前記第１のノードのマスター公開鍵、前記第２のノードのマスター公開鍵、前記第１の署名付きメッセージ、前記第２の署名付きメッセージ、及び共通の暗号化システムを用いることを示す通知のうちの１つ又は複数を送信及び／又は受信するための第２の通信モジュールと、
を更に備える、請求項２６～３９のいずれか１項に記載のシステム。
【請求項４１】
前記共通の暗号化システムは、共通の生成元を備えた楕円曲線暗号化（ＥＣＣ）システムである、請求項４０に記載のシステム。
【請求項４２】
前記決定性鍵は、以前の決定性鍵のハッシュを決定することに基づく、請求項２６～４１のいずれか１項に記載のシステム。
【請求項４３】
前記第１の非対称暗号対及び前記第２の非対称暗号対は、それぞれの以前の第１の非対称暗号対及び以前の第２の非対称暗号対の関数に基づいている、請求項２６～４２のいずれか１項に記載のシステム。
【請求項４４】
対称鍵アルゴリズムを用いた第１のノードと第２のノードとの間のセキュアな通信のためのシステムであって、
－前記第１の処理デバイス及び前記第２の処理デバイスとの共通秘密を決定するための
請求項２６～４３のいずれか１項に記載のシステム
を備え、前記第１の処理デバイスは、
－前記共通秘密に基づいて対称鍵を決定し、
－前記対称鍵を用いて、第１の通信メッセージを暗号化された第１の通信メッセージ

に暗号化し、
　－前記暗号化された第１の通信メッセージを送信する
ように更に構成され、
　前記第２の処理デバイスは、
　－前記共通秘密に基づいて同じ対称鍵を決定し、
　－前記暗号化された第１の通信メッセージを受信し、
　－前記対称鍵を用いて前記暗号化された第１の通信メッセージを前記第１の通信メッセージに復号する
ように更に構成されているシステム。
【請求項４５】
　対称鍵アルゴリズムを用いた第１のノードと第２のノードとの間のセキュアな通信のためのシステムであって、
　－前記第１の処理デバイス及び前記第２の処理デバイスとの共通秘密を決定するための請求項２６～４３のいずれか１項に記載のシステム
を備え、前記第２の処理デバイスは、
　－前記対称鍵を用いて、第２の通信メッセージを前記暗号化された第２の通信メッセージに暗号化し、
　－前記暗号化された第２の通信メッセージを送信する
ように更に構成され、
　前記第１の処理デバイスは、
　－前記暗号化された第２の通信メッセージを受信し、
　－前記対称鍵を用いて、前記暗号化された第２の通信メッセージを前記第２の通信メッセージに復号するように更に構成されているシステム。
【請求項４６】
　前記第１の通信メッセージ及び前記第２の通信メッセージは、前記第１のノードと前記第２のノードとの間のオンライントランザクションのための、前記第１のノードと前記第２のノードとの間のトランザクションメッセージである、請求項４４又は４５のいずれかに記載のシステム。
【請求項４７】
　処理デバイスに、請求項１～１９のいずれか１項に記載の方法を実施させるためのマシン可読命令を備えるコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本開示は、２つのノードのための共通秘密を決定することに関する。いくつかの用途では、共通秘密は、２つのノード間のセキュアな通信を可能にするための暗号学のために用いることができる。本発明は、限定しないが、デジタルウォレット、ブロックチェーン（例えば、ビットコイン）技術、及びパーソナルデバイスセキュリティと共に用いるのに適切である。
【背景技術】
【０００２】
　暗号学は、２つ以上のノード間のセキュアな通信のための技法を伴う。ノードは、モバイル通信デバイス、タブレットコンピュータ、ラップトップコンピュータ、デスクトップ、他の形態のコンピューティングデバイス及び通信デバイス、ネットワークにおけるサーバーデバイス、ネットワークにおけるクライアントデバイス、分散ネットワークにおける１つ又は複数のノード等を含むことができる。ノードは、自然人、会社の従業員等の人々のグループ、銀行システムのようなシステム等に関連付けることができる。
【０００３】
　いくつかの場合、２つ以上のノードがセキュアでない通信ネットワークによってリンクされる場合がある。例えば、２つのノードは、第三者がノード間の通信を盗聴することが

可能であり得る通信ネットワークによってリンクされる場合がある。従って、ノード間で送信されるメッセージを暗号化された形式で送信することができ、受信時に、意図される受信者が、対応する復号鍵（又は他の復号方法）を用いてメッセージを復号することができる。このため、そのような通信のセキュリティは、第三者が対応する暗号化鍵を決定することを防ぐことに依拠する。

【０００４】

暗号学の１つの方法は、対称鍵アルゴリズムを用いることを含む。鍵は、同じ対称鍵が、平文メッセージの暗号化及び暗号文の解読の双方に用いられるという意味で対称である。対称鍵アルゴリズムの使用の１つの検討事項は、盗聴者が対称鍵を取得することを防ぐセキュアな方法で双方のノードにどのように対称鍵を送信するかである。これは、例えば、対称鍵がセキュアでない通信ネットワークを介して決して送信されることがないように（認可された）ノードに対称鍵を物理的に送達することを含むことができる。しかし、物理的送達は、必ずしも常に選択肢ではない。従って、そのような暗号化システムにおける問題は、セキュアでないネットワークにわたるノード間の対称鍵（共通秘密に基づくことができる）の確立である。最近では、状況によって、鍵の送信がインターネット等の通信システムにわたって、通例、電子的に行われることが望ましい場合がある。このため、共有される秘密（例えば、対称鍵）を提供するこのステップは、潜在的に重篤な脆弱性である。対称鍵アルゴリズム（及びプロトコル）は、単純であり、広く用いられているため、２つのノードがセキュアでないネットワークにわたってセキュアに共通秘密鍵を決定する能力が必要とされている。

【０００５】

他の既存の暗号化方法は、非対称鍵を用いることを含む。これらは、公開鍵暗号学において用いることができ、ここでは、非対称鍵は、私有鍵（ｐｒｉｖａｔｅ　ｋｅｙ）及び対応する公開鍵を含む。公開鍵は、公開で入手可能にすることができるのに対し、私有鍵は、名前が意味するように、プライベートのままにされる。これらの非対称鍵は、数ある中でも公開鍵暗号化及びデジタル署名のために用いることができる。ディフィー・ヘルマン鍵交換及び３パスプロトコル等を含む既存のプロトコルは、セキュアでないネットワークにわたる秘密のセキュアな共有を可能にする。しかし、これらの方法は、新たな秘密が連続して作成され共有される等のいくつかの事例において計算コストが高い。

【０００６】

代替的な非対称鍵階層（ビットコイン開発者のガイドに記載されているもの等）は、ランダムシード及びインデックス構造に依拠し、この結果、鍵管理が不十分となる。対照的に、本発明の実施形態は、非対称鍵を作成するのみでなく、実証可能な方法で特定のデータと関連付けられた決定性で階層的な共有秘密も作成するための有意義な「メッセージ」（Ｍ）の使用を含むことができる。

【０００７】

本明細書に含まれている文書、動作、マテリアル、デバイス、論文等の任意の論考は、これらのもののうちの任意のもの若しくは全てが従来技術の基礎の一部を形成するか、又は本出願の各請求項の優先日前に存在していたような本開示の関連分野における一般的に知られた知識であることを認めるものとして解釈されない。

【０００８】

本明細書全体を通じて、「含む（ｃｏｍｐｒｉｓｅ）」という語、又は「含む（ｃｏｍｐｒｉｓｅｓ」若しくは「含む（ｃｏｍｐｒｉｓｉｎｇ）」等の変化形は、述べた要素、完全体若しくはステップ、又は要素、完全体若しくはステップのグループを含むことを意味するが、任意の他の要素、完全体若しくはステップ、又は要素、完全体若しくはステップのグループを排除することを意味するものではないことは理解されよう。

【発明の概要】

【課題を解決するための手段】

【０００９】

本発明の１つの態様によれば、第１のノード（Ｃ）において、第１のノード（Ｃ）及び

第２のノード（Ｓ）に共通の共通秘密（ＣＳ）を決定するコンピュータ実施方法であって、第１のノード（Ｃ）は、第１のノードのマスター私有鍵（$Ｖ_{1\ C}$）及び第１のノードのマスター公開鍵（$Ｐ_{1\ C}$）を有する第１の非対称暗号対に関連付けられ、第２のノード（Ｓ）は、第２のノードのマスター私有鍵（$Ｖ_{1\ S}$）及び第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）を有する第２の非対称暗号対に関連付けられ、このコンピュータ実施方法は、

－　少なくとも第１のノードのマスター私有鍵（$Ｖ_{1\ C}$）及び決定性鍵（ＤＫ）に基づいて第１のノードの第２の私有鍵（$Ｖ_{2\ C}$）を決定することと、

－　少なくとも第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）及び決定性鍵（ＤＫ）に基づいて第２のノードの第２の公開鍵（$Ｐ_{2\ S}$）を決定することと、

－　第１のノードの第２の私有鍵（$Ｖ_{2\ C}$）及び第２のノードの第２の公開鍵（$Ｐ_{2\ S}$）に基づいて共通秘密（ＣＳ）を決定することと、

を含み、

第２のノード（Ｓ）は、第１のノードの第２の公開鍵（$Ｐ_{2\ C}$）及び第２のノードの第２の私有鍵（$Ｖ_{2\ S}$）に基づいて同じ共通秘密（Ｓ）を有し、第１のノードの第２の公開鍵（$Ｐ_{2\ C}$）は、少なくとも、第１のノードのマスター公開鍵（$Ｐ_{1\ C}$）及び決定性鍵（ＤＫ）に基づき、第２のノードの第２の私有鍵（$Ｖ_{2\ S}$）は、少なくとも、第２のノードのマスター私有鍵（$Ｖ_{1\ S}$）及び決定性鍵（ＤＫ）に基づく方法が提供される。

【００１０】

これにより、第２の公開鍵が、各ノードにおいて独立して導出されることが可能になり、それによってセキュリティが増大するという利点が得られ、一方、マシンがサブ鍵の作成を自動化することも可能になる。公開鍵間の関係は、第三者によって決定することができないので、追跡することができない合致したトランザクション入力を有するという利点も得られる。従って、これにより、高レベルの匿名性を達成することが可能になり、従ってセキュリティが改善される。

【００１１】

決定性鍵（ＤＫ）は、メッセージ（Ｍ）に基づいているこの方法は、メッセージ（Ｍ）及び第１のノードの第２の私有鍵（$Ｖ_{2\ C}$）に基づいて第１の署名付きメッセージ（ＳＭ１）を生成することと、通信ネットワークを介して、第１の署名付きメッセージ（ＳＭ１）を第２のノード（Ｓ）に送信することとを更に含んでおり、第１の署名付きメッセージ（ＳＭ１）は、第１のノード（Ｃ）を認証するために、第１のノードの第２の公開鍵（$Ｐ_{2\ C}$）を用いて有効性を確認することができる。

【００１２】

本方法は、また、通信ネットワークを介して、第２のノード（Ｓ）から第２の署名付きメッセージ（ＳＭ２）を受信することと、第２のノードの第２の公開鍵（$Ｐ_{2\ S}$）を用いて第２の署名付きメッセージ（ＳＭ２）の有効性を確認することと、第２の署名付きメッセージ（ＳＭ２）の有効性を確認した結果に基づいて、第２のノード（Ｓ）を認証することとを更に含むことができ、第２の署名付きメッセージ（ＳＭ２）は、メッセージ（Ｍ）又は第２のメッセージ（Ｍ２）、及び第２のノードの第２の私有鍵（$Ｖ_{2\ S}$）に基づいて生成されたものである。

【００１３】

本方法は、メッセージ（Ｍ）を生成することと、通信ネットワークを介して、メッセージ（Ｍ）を第２のノード（Ｓ）に送信することとを更に含むことができる。それに代えて本方法は、通信ネットワークを介して、第２のノード（Ｓ）からメッセージ（Ｍ）を受信することを含んでもよい。更に別の代替形態では、本方法は、通信ネットワークを介して、別のノードからメッセージ（Ｍ）を受信することを含んでいてもよい。更に別の代替形態では、本方法は、データストア、及び／又は第１のノード（Ｃ）に関連付けられた入力インタフェースからメッセージ（Ｍ）を受信することを含んでもよい。

【００１４】

第１のノードのマスター公開鍵（$Ｐ_{1\ C}$）及び第２のノードのマスター公開鍵（$Ｐ_{1\ S}$）は、それぞれの第１のノードのマスター私有鍵（$Ｖ_{1\ C}$）及び第２のノードのマスター

私有鍵（V_{1S}）と発生器（G）との楕円曲線点乗算に基づくことができる。

【００１５】

本方法は、通信ネットワークを介して、第２のノードのマスター公開鍵（P_{1S}）を受信するステップと、第１のノード（Ｃ）に関連付けられたデータストアに、第２のノードのマスター公開鍵（P_{1S}）を記憶するステップとを更に含むことができる。

【００１６】

本方法は、第１のノード（Ｃ）において、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を作成するステップと、通信ネットワークを介して、第１のノードのマスター公開鍵（P_{1C}）を第２のノード（Ｓ）及び／又は他のノードに送信するステップと、第１のノード（Ｃ）に関連付けられた第１のデータストアに、第１のノードのマスター私有鍵（V_{1C}）を記憶するステップとを更に含むことができる。

【００１７】

本方法は、また、通信ネットワークを介して、第２のノードに、共通秘密（ＣＳ）を決定する方法のために共通発生器（Ｇ）と共に共通楕円曲線暗号（ＥＣＣ）システムを用いることを示す通知を送信することを含むことができる。第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を作成するステップは、共通ＥＣＣシステムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて第１のノードのマスター私有鍵（V_{1C}）を作成することと、以下の式

$$P_{1C}=V_{1C}\times G$$

による、第１のノードのマスター私有鍵（V_{1C}）と共通発生器（Ｇ）との楕円曲線点乗算に基づいて第１のノードのマスター公開鍵（P_{1C}）を決定することとを含むことができる。

【００１８】

本方法は、メッセージ（Ｍ）のハッシュの決定に基づいて決定性鍵（ＤＫ）を決定することを更に含むことができ、第１のノードの第２の私有鍵（V_{2C}）を決定するステップは、以下の式

$$V_{2C}=V_{1C}+DK$$

による、第１のノードのマスター私有鍵（V_{1C}）及び決定性鍵（ＤＫ）のスカラー加算に基づいている。

【００１９】

第２のノードの第２の公開鍵（P_{2S}）を決定するステップは、以下の式、

$$P_{2S}=P_{1S}+DK\times G$$

による、第２のノードのマスター公開鍵（P_{1S}）を、決定性鍵（ＤＫ）と共通発生器（Ｇ）との楕円曲線点乗算に楕円曲線点加算したものに基づくことができる。

【００２０】

決定性鍵（ＤＫ）は、以前の決定性鍵のハッシュを決定することに基づくことができる。

【００２１】

第１の非対称暗号対及び第２の非対称暗号対は、それぞれの以前の第１の非対称暗号対及び以前の第２の非対称暗号対の関数に基づくことができる。

【００２２】

本発明の他の態様によれば、対称鍵アルゴリズムを用いた第１のノードと第２のノードとの間のセキュアな通信の方法であって、

－　上記の方法に従って決定された共通秘密に基づいて対称鍵を決定することと、

－　対称鍵を用いて、第１の通信メッセージを暗号化された第１の通信メッセージに暗号化することと、

－　通信ネットワークを介して、暗号化された第１の通信メッセージを第１のノード（Ｃ）から第２のノード（Ｓ）に送信することと、

を含む、方法が提供される。

【００２３】
本方法は、通信ネットワークを介して、第２のノード（Ｓ）から暗号化された第２の通信メッセージを受信することと、対称鍵を用いて、暗号化された第２の通信メッセージを第２の通信メッセージに復号することとを更に含むことができる。
【００２４】
本発明の更に他の態様によれば、第１のノードと第２のノードとの間のオンライントランザクションを行う方法であって、上記の方法に従って決定された共通秘密に基づいて対称鍵を決定することと、対称鍵を用いて、第１のトランザクションメッセージを暗号化された第１のトランザクションメッセージに暗号化することと、通信ネットワークを介して、暗号化された第１のトランザクションメッセージを第１のノード（Ｃ）から第２のノード（Ｓ）に送信することと、通信ネットワークを介して、第２のノード（Ｓ）から暗号化された第２のトランザクションメッセージを受信することと、対称鍵を用いて、暗号化された第２のトランザクションメッセージを第２のトランザクションメッセージに復号することとを含む方法が提供される。
【００２５】
本発明の更に異なる態様によれば、第１のノード（Ｃ）において、第２のノード（Ｓ）と共通の共通秘密（ＣＳ）を決定するためのデバイスであって、第１のノード（Ｃ）は、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を有する第１の非対称暗号対に関連付けられ、第２のノード（Ｓ）は、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を有する第２の非対称暗号対に関連付けられ、このデバイスは、共通秘密を決定するために上記で定義された方法を行うための第１の処理デバイスを備えているデバイスが提供される。
【００２６】
本発明の更なる態様によれば、第１のノードと第２のノードとの間のセキュアな通信又はセキュアなオンライントランザクションを行うためのデバイスであって、上記セキュアな通信又はセキュアなオンライントランザクションの方法を行うための第１の処理デバイスを備えているデバイスが提供される。
【００２７】
このデバイスは、第１のノードのマスター私有鍵（V_{1C}）のうちの１つ又は複数を記憶するための第１のデータストアを更に備えることができる。第１のデータストアは、第１のノードのマスター公開鍵（P_{1C}）、第２のノードのマスター公開鍵（P_{1S}）、及びメッセージ（Ｍ）のうちの１つ又は複数を更に記憶することができる。
【００２８】
このデバイスは、通信ネットワークを介して、メッセージ（Ｍ）、第１のノードのマスター公開鍵（P_{1C}）、第２のノードのマスター公開鍵（P_{1S}）、第１の署名付きメッセージ（ＳＭ１）、第２の署名付きメッセージ（ＳＭ２）、共通楕円曲線暗号（ＥＣＣ）システムを共通発生器（Ｇ）と共に用いることを示す通知のうちの１つ又は複数を送信及び／又は受信するための通信モジュールを更に備えることができる。
【００２９】
本発明の更なる態様によれば、第１のノード（Ｃ）と第２のノード（Ｓ）との間の共通秘密を決定するためのシステムであって、
－　第１のノード（Ｃ）は、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を有する第１の非対称暗号対に関連付けられ、
－　第２のノード（Ｓ）は、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を有する第２の非対称暗号対に関連付けられ、
このシステムは、
－　第１のノード（Ｃ）に関連付けられた第１の処理デバイスであって、
　－　少なくとも第１のノードのマスター私有鍵（V_{1C}）及び決定性鍵（ＤＫ）に基づいて第１のノードの第２の私有鍵（V_{2C}）を決定し、
　－　少なくとも第２のノードのマスター公開鍵（P_{1S}）及び決定性鍵（ＤＫ）に基

づいて第２のノードの第２の公開鍵（P_{2S}）を決定し、
－　第１のノードの第２の私有鍵（V_{2C}）及び第２のノードの第２の公開鍵（P_{2S}）に基づいて共通秘密（ＣＳ）を決定する
ように構成される、第１の処理デバイスと、
－　第２のノード（Ｓ）に関連付けられた第２の処理デバイスであって、
－　少なくとも、第１のノードのマスター公開鍵（P_{1C}）及び決定性鍵（ＤＫ）に基づいて第１のノードの第２の公開鍵（P_{2C}）を決定し、
－　少なくとも、第２のノードのマスター私有鍵（V_{1S}）及び決定性鍵（ＤＫ）に基づいて第２のノードの第２の私有鍵（V_{2S}）を決定し、
－　第１のノードの第２の公開鍵（P_{2C}）及び第２のノードの第２の私有鍵（V_{2S}）に基づいて共通秘密を決定する
ように構成される、第２の処理デバイスと、
を備え、
前記の第１の処理デバイス及び第２の処理デバイスは、同じ共通秘密（ＣＳ）を決定するシステムが提供される。

【００３０】

本システムにおいて、決定性鍵（ＤＫ）は、メッセージ（Ｍ）に基づき、第１の処理デバイスは、メッセージ（Ｍ）及び第１のノードの第２の私有鍵（V_{2C}）に基づいて第１の署名付きメッセージ（ＳＭ１）を作成し、通信ネットワークを介して、第１の署名付きメッセージ（ＳＭ１）を第２のノード（Ｓ）に送信するように更に構成されている。第２処理デバイスは、第１の署名付きメッセージ（ＳＭ１）を受信し、第１のノードの第２の公開鍵（P_{2C}）を用いて第１の署名付きメッセージ（ＳＭ１）の有効性を確認し、有効性を確認された第１の署名付きメッセージ（ＳＭ１）の結果に基づいて第１のノード（Ｃ）を認証するように更に構成することができる。

【００３１】

このシステムにおいて、第２の処理デバイスは、メッセージ（Ｍ）又は第２のメッセージ（Ｍ２）、及び第２のノードの第２の私有鍵（V_{2S}）に基づいて第２の署名付きメッセージ（ＳＭ２）を作成し、この第２の署名付きメッセージ（ＳＭ２）を第１のノード（Ｃ）に送信するように更に構成することができ、第１の処理デバイスは、第２の署名付きメッセージ（ＳＭ２）を受信し、第２のノードの第２の公開鍵（P_{2S}）を用いて第２の署名付きメッセージ（ＳＭ２）の有効性を確認し、有効性を確認された第２の署名付きメッセージ（ＳＭ２）の結果に基づいて第２のノード（Ｓ）を認証するように更に構成されている。

【００３２】

本システムにおいて、第１の処理デバイスは、メッセージ（Ｍ）を作成し、メッセージ（Ｍ）を送信するように更に構成することができ、第２の処理デバイスは、このメッセージ（Ｍ）を受信するように構成される。１つの代替形態では、メッセージは、別のノードによって作成され、第１の処理デバイスは、メッセージ（Ｍ）を受信するように構成され、第２の処理デバイスは、メッセージ（Ｍ）を受信するように構成されている。

【００３３】

更に他の代替形態では、本システムは、システムデータストア及び／又は入力インタフェースを備え、第１の処理デバイス及び第２の処理デバイスは、システムデータストア及び／又は入力インタフェースから、メッセージ（Ｍ）又は第２のメッセージ（Ｍ２）を受信する。

【００３４】

第１の処理デバイスは、システムデータストア及び／又は入力デバイスから第２のノードのマスター公開鍵（P_{1S}）を受信することができ、第２の処理デバイスは、システムデータストア及び／又は入力デバイスから第１のノードのマスター公開鍵（P_{1C}）を受信することができる。

【００３５】

第１のノードのマスター公開鍵（P_{1C}）、第２のノードのマスター公開鍵（P_{1S}）は、それぞれの第１のノードのマスター私有鍵（V_{1C}）及び第２のノードのマスター私有鍵（V_{1S}）と発生器（Ｇ）との楕円曲線点乗算に基づくことができる。

【００３６】

本システムは、第１のノードのマスター私有鍵（V_{1C}）を記憶するための、第１のノード（Ｃ）に関連付けられた第１のデータストアと、第２のノードのマスター私有鍵（V_{1S}）を記憶するための、第２のノード（Ｓ）に関連付けられた第２のデータストアとを更に備えることができる。

【００３７】

本システムにおいて、第１の処理デバイスは、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を作成し、第１のノードのマスター公開鍵（P_{1C}）を送信し、第１のノードのマスター私有鍵（V_{1C}）を第１のデータストアに記憶するように構成することができ、第２の処理デバイスは、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を作成し、第２のノードのマスター公開鍵（P_{1S}）を送信し、第２のノードのマスター私有鍵（V_{1S}）を第２のデータストアに記憶するように構成されている。

【００３８】

本システムにおいて、第１のデータストアは、第２のノードのマスター公開鍵（P_{1S}）を受信して記憶することができ、第２のデータストアは、第１のノードのマスター公開鍵（P_{1C}）を受信して記憶することができる。

【００３９】

本システムにおいて、第１の処理デバイスは、共通楕円曲線暗号（ＥＣＣ）システムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて第１のノードのマスター私有鍵（V_{1C}）を作成し、以下の式

$$P_{1C}=V_{1C}\times G$$

による、第１のノードのマスター私有鍵（V_{1C}）と共通発生器（Ｇ）との楕円曲線点乗算に基づいて第１のノードのマスター公開鍵（P_{1C}）を決定するように更に構成することができる。

【００４０】

第２の処理デバイスは、共通ＥＣＣシステムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて第２のノードのマスター私有鍵（V_{1S}）を作成し、以下の式

$$P_{1S}=V_{1S}\times G$$

による、第２のノードのマスター私有鍵（V_{1S}）と共通発生器（Ｇ）との楕円曲線点乗算に基づいて第２のノードのマスター公開鍵（P_{1S}）を決定するように更に構成することができる。

【００４１】

本システムにおいて、第１の処理デバイスは、メッセージ（Ｍ）のハッシュに基づいて決定性鍵（ＤＫ）を決定するように構成することができ、第１のノードの第２の私有鍵（V_{2C}）は、以下の式

$$V_{2C}=V_{1C}+DK$$

による、第１のノードのマスター私有鍵（V_{1C}）と決定性鍵（ＤＫ）とのスカラー加算に基づいており、第２のノードの公開鍵（P_{2S}）は、以下の式

$$P_{2S}=P_{1S}+DK\times G$$

による、第２のノードのマスター公開鍵（P_{1S}）を、決定性鍵（ＤＫ）と共通発生器（Ｇ）との楕円曲線点乗算に楕円曲線点加算したものに基づいている。第２の処理デバイスは、メッセージ（Ｍ）のハッシュに基づいて決定性鍵（ＤＫ）を決定するように更に構成することができ、第２のノードの第２の私有鍵（V_{2S}）は、以下の式

$$V_{2S}=V_{1C}+DK$$

による、第２のノードのマスター私有鍵（V_{1S}）と決定性鍵（ＤＫ）とのスカラー加算

に基づいており、第１のノードの第２の公開鍵（P_{2C}）は、以下の式

$$P_{2C} = P_{1C} + DK \times G$$

による、第１のノードのマスター公開鍵（P_{1C}）を、決定性鍵（ＤＫ）と共通発生器（Ｇ）との楕円曲線点乗算に楕円曲線点加算したものに基づいている。

【００４２】

本システムは、第１の処理デバイスに関連付けられ、通信ネットワークを介して、メッセージ（Ｍ）、第１のノードのマスター公開鍵（P_{1C}）、第２のノードのマスター公開鍵（P_{1S}）、第１の署名付きメッセージ（ＳＭ１）、第２の署名付きメッセージ（ＳＭ２）、及び共通楕円曲線暗号（ＥＣＣ）システムを共通発生器（Ｇ）と共に用いることを示す通知のうちの１つ又は複数を送信及び／又は受信するための第１の通信モジュールと、第２の処理デバイスに関連付けられ、通信ネットワークを介して、メッセージ（Ｍ）、第１のノードのマスター公開鍵（P_{1C}）、第２のノードのマスター公開鍵（P_{1S}）、第１の署名付きメッセージ（ＳＭ１）、第２の署名付きメッセージ（ＳＭ２）、及び共通楕円曲線暗号（ＥＣＣ）システムを共通発生器（Ｇ）と共に用いることを示す通知のうちの１つ又は複数を送信及び／又は受信するための第２の通信モジュールとを更に備えることができる。

【００４３】

本システムにおいて、決定性鍵（ＤＫ）は、以前の決定性鍵のハッシュを決定することに基づくことができる。

【００４４】

本システムにおいて、第１の非対称暗号対及び第２の非対称暗号対は、それぞれの以前の第１の非対称暗号対及び以前の第２の非対称暗号対の関数に基づくことができる。

【００４５】

本発明の更なる態様によれば、対称鍵アルゴリズムを用いた第１のノードと第２のノードとの間のセキュアな通信のためのものであって、第１の処理デバイス及び第２の処理デバイスとの共通秘密を決定するためのシステムを備え、第１の処理デバイスは、共通秘密に基づいて対称鍵を決定し、この対称鍵を用いて、第１の通信メッセージを暗号化された第１の通信メッセージに暗号化し、暗号化された第１の通信メッセージを送信するように更に構成される、システムが提供される。第２の処理デバイスは、共通秘密に基づいて同じ対称鍵を決定し、暗号化された第１の通信メッセージを受信し、対称鍵を用いて暗号化された第１の通信メッセージを第１の通信メッセージに復号するように更に構成されている。

【００４６】

セキュアな通信のためのこのシステムにおいて、第２の処理デバイスは、対称鍵を用いて、第２の通信メッセージを暗号化された第２の通信メッセージに暗号化し、暗号化された第２の通信メッセージを送信するように更に構成することができる。第１の処理デバイスは、暗号化された第２の通信メッセージを受信し、対称鍵を用いて、暗号化された第２の通信メッセージを第２の通信メッセージに復号するように更に構成することができる。

【００４７】

上記のシステムにおいて、第１と第２の通信メッセージは、第１のノードと第２のノードとの間のオンライントランザクションのための、第１のノードと第２のノードとの間のトランザクションメッセージとすることができる。

【００４８】

本発明の更なる態様によれば、処理デバイスに、上記の方法のうちのいずれか１つを実施させるためのマシン可読命令を備えるコンピュータプログラムが提供される。

【００４９】

本開示の例が以下を参照して説明される。

【図面の簡単な説明】

【００５０】

【図１】第１のノード及び第２のノードのための共通秘密を決定する例示的なシステムの

概略図である。
【図２】共通秘密を決定するためのコンピュータ実施方法のフローチャートである。
【図３】第１のノード及び第２のノードを登録するコンピュータ実施方法のフローチャートである。
【図４】共通秘密を決定するためのコンピュータ実施方法の別のフローチャートである。
【図５】第１と第２のノードの間のセキュアな通信のコンピュータ実施方法のフローチャートである。
【図６】電子リソースレンタルのための例示的なシステムの概略図である。
【図７】パスワード交換に本方法を適用する例示的なシステムの概略図である。
【図８】第１と第２のノードを認証するためのコンピュータ実施方法のフローチャートである。
【図９】異なる目的の異なる鍵のツリー構造の例である。
【図１０】マスター鍵生成方法を用いたツリー構造の例である。
【図１１】例示的な処理デバイスの概略図を示す。
【発明を実施するための形態】
【００５１】
概説
第１のノード（Ｃ）において、第２のノード（Ｓ）における同じ共通秘密である共通秘密（ＣＳ）を決定するための方法、デバイス及びシステムを以下に説明する。図１は、通信ネットワーク５を介して第２のノード７と通信する第１のノード３を含むシステム１を示す。第１のノード３は、関連付けられた第１の処理デバイス２３を有し、第２のノード７は、関連付けられた第２の処理デバイス２７を有する。第１のノード３及び第２のノード７は、コンピュータ、タブレットコンピュータ、モバイル通信デバイス、コンピュータサーバー等の電子デバイスを含むことができる。１つの例において、第１のノード３はクライアントデバイスとすることができ、第２のノード７はサーバーとすることができる。
【００５２】
第１のノード３は、第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を有する第１の非対称暗号対に関連付けられる。第２のノード（７）は、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を有する第２の非対称暗号対に関連付けられる。それぞれの第１のノード３及び第２のノード７のための第１及び第２の非対称暗号対は、登録中に作成することができる。第１のノード３及び第２のノード７によって行われる登録メソッド１００、２００は、以下で図３を参照して更に詳細に説明する。ノードごとの公開鍵は、例えば通信ネットワーク５を介して、公開で共有することができる。
【００５３】
第１のノード３及び第２のノード７の双方において共通秘密（ＣＳ）を決定するために、ノード３、７は、通信ネットワーク５を介して私有鍵を通信することなく、それぞれのメソッド３００、４００のステップを行う。
【００５４】
第１のノード３によって行われるメソッド３００は、少なくとも、第１のノードのマスター私有鍵（V_{1C}）及び決定性鍵（ＤＫ）に基づいて、第１のノードの第２の私有鍵（V_{2C}）を決定すること（３３０）を含む。この決定性鍵は、第１のノードと第２のノードとの間で共有されるメッセージ（Ｍ）に基づくことができ、これは、以下で更に詳細に説明するように、通信ネットワーク５を介してメッセージを共有することを含むことができる。このメソッド３００は、少なくとも、第２のノードのマスター公開鍵（P_{1S}）及び決定性鍵（ＤＫ）に基づいて、第２のノードの第２の公開鍵（P_{2S}）を決定すること（３７０）も含む。このメソッド３００は、第１のノードの第２の私有鍵（V_{2C}）及び第２のノードの第２の公開鍵（P_{2S}）に基づいて、共通秘密（ＣＳ）を決定すること（３８０）を含む。

【００５５】
重要なことであるが、同じ共通秘密（ＣＳ）を、メソッド４００によって第２のノード７において決定することもできる。メソッド４００は、第１のノードのマスター公開鍵（P_{1C}）及び決定性鍵（ＤＫ）に基づいて、第１のノードの第２の公開鍵（P_{2C}）を決定すること（４３０）を含む。このメソッド４００は、第２のノードのマスター私有鍵（V_{1S}）及び決定性鍵（ＤＫ）に基づいて、第２のノードの第２の私有鍵（V_{2S}）を決定すること（４７０）を更に含む。メソッド４００は、第２のノードの第２の私有鍵（V_{2S}）及び第１のノードの第２の公開鍵（P_{2C}）に基づいて、共通秘密（ＣＳ）を決定すること（４８０）を含む。

【００５６】
通信ネットワーク５は、ローカルエリアネットワーク、広域ネットワーク、セルラーネットワーク、無線通信ネットワーク、インターネット等を含むことができる。電気配線、光ファイバー等の通信媒体を介して、又は無線でデータを送信することができるこれらのネットワークは、盗聴者１１等による盗聴を受けやすい場合がある。メソッド３００、４００は、第１のノード３及び第２のノード７が共に、通信ネットワーク５を介して共通秘密を送信することなく共通秘密を独立して決定することを可能にすることができる。このため、１つの利点は、潜在的にセキュアでない通信ネットワーク５を介して私有鍵を送信する必要なく、各ノードによってセキュアに共通秘密（ＣＳ）を決定することができることである。そして、共通秘密は、通信ネットワーク５を介して、第１のノード３と第２のノード７との間の暗号化された通信のための秘密鍵（又は秘密鍵の基礎）として用いることができる。

【００５７】
メソッド３００、４００は、追加のステップを含む。メソッド３００は、第１のノード３において、メッセージ（Ｍ）及び第１のノードの第２の私有鍵（V_{2C}）に基づいて、署名付きメッセージ（ＳＭ１）を作成することを含むことができる。メソッド３００は、通信ネットワークを介して、第２のノード７に第１の署名付きメッセージ（ＳＭ１）を送信すること（３６０）を更に含む。そして、第２のノード７は、第１の署名付きメッセージ（ＳＭ１）を受信するステップ４４０を行うことができる。メソッド４００は、第１のノードの第２の公開鍵（P_{2C}）を用いて第１の署名付きメッセージ（ＳＭ１）の有効性を確認し（４５０）、第１の署名付きメッセージ（ＳＭ１）の有効性確認結果に基づいて第１のノード３を認証するステップ（４６０）も含む。有利には、これによって、第２のノード７が、（第１の署名付きメッセージが作成された）第１のノードとされているノードが第１のノード３であることを認証することが可能になる。これは、第１のノード３のみが第１のノードのマスター私有鍵（V_{1C}）へのアクセスを有し、従って、第１のノード３のみが第１の署名付きメッセージ（ＳＭ１）を作成するための第１のノードの第２の私有鍵（V_{2C}）を決定することができるという仮定に基づく。同様に、第２の署名付きメッセージ（ＳＭ２）を第２のノード７において作成し、第１のノード３に送信することができ、それによって、ピアツーピアのシナリオ等において第１のノード３が第２のノード７を認証することができることが理解されよう。

【００５８】
第１と第２のノードの間でのメッセージ（Ｍ）を共有することは、多岐にわたる方法で達成することができる。１つの例において、メッセージは、第１のノード３において作成することができ、このメッセージは次に、通信ネットワーク５を介して、第２のノード７に送信される。それに代えて、メッセージは、第２のノード７において作成され、次に、通信ネットワーク５を介して第２のノード７に送信されてもよい。更に別の例では、メッセージは、第３のノード９において生成され、このメッセージが第１のノード３及び第２のノード７の双方に送信されてもよい。更に他の代替形態では、ユーザは、ユーザインタフェース１５を通じて、第１のノード３及び第２のノード７によって受信されるメッセージを入力してもよい。更に別の例では、メッセージ（Ｍ）は、データストア１９から取り出され、第１のノード３及び第２のノード７に送信されてもよい。いくつかの例では、メ

ッセージ（Ｍ）は公開であってもよく、従って、セキュアでないネットワーク５を介して送信されてもよい。

【００５９】

更に他の例では、１つ又は複数のメッセージ（Ｍ）を、データストア１３、１７、１９に記憶することができる。データストアにおいて、メッセージは、第１のノード３と第２のノード７との間のセッション、トランザクション等と関連付けることができる。このため、メッセージ（Ｍ）を取り出し、それぞれの第１のノード３及び第２のノード７において、そのセッション又はトランザクションに関連付けられた共通秘密（ＣＳ）を再現するのに用いることができる。有利には、共通秘密（ＣＳ）の再現を可能にするレコードは、レコード自体がプライベートに記憶されるか又はセキュアに送信される必要なく保持することができる。これは、第１のノード３及び第２のノード７において多数のトランザクションが行われ、全てのメッセージ（Ｍ）をノード自体に記憶することが実際的でない場合に有利である。

【００６０】

登録メソッド１００、２００

登録メソッド１００、２００の例を図３を参照して説明する。ここで、メソッド１００は、第１のノード３によって行われ、メソッド２００は、第２のノード７によって行われる。これは、それぞれの第１のノード３及び第２のノード７について第１及び第２の非対称暗号対を確立することを含む。

【００６１】

非対称暗号対は、公開鍵暗号化において用いられるような、関連付けられた私有鍵及び公開鍵を含む。この例において、非対称暗号対は、楕円曲線暗号（ＥＣＣ）及び楕円曲線演算の特性を用いて作製される。

【００６２】

ＥＣＣのための規格は、ＳＥＣＧ（Ｓｔａｎｄａｒｄｓ ｆｏｒ Ｅｆｆｉｃｉｅｎｔ Ｃｒｙｐｔｏｇｒａｐｈｙ Ｇｒｏｕｐ）（ｗｗｗ．ｓｃｅｇ．ｏｒｇ）によって記載されているような既知の規格を含むことができる。楕円曲線暗号については、米国特許第５，６００，７２５号、米国特許第５，７６１，３０５号、米国特許第５，８８９，８６５号、米国特許第５，８９６，４５５号、米国特許第５，９３３，５０４号、米国特許第６，１２２，７３６号、米国特許第６，１４１，４２０号、米国特許第６，６１８，４８３号、米国特許第６，７０４，８７０号、米国特許第６，７８５，８１３号、米国特許第６，０７８，６６７号、米国特許第６，７９２，５３０号にも記載されている。

【００６３】

メソッド１００、２００において、これは、第１及び第２のノードが共通ＥＣＣシステム、及び共通発生器（Ｇ）を用いることについて確定すること（１１０、２１０）を含む。１つの例において、共通ＥＣＣシステムは、ビットコインによって用いられるＥＣＣシステムであるｓｅｃｐ２５６Ｋｌに基づくことができる。共通発生器（Ｇ）は、選択されるか、ランダムに作成されるか、又は割り当てられる。

【００６４】

ここで、第１のノード３を述べると、メソッド１００は、共通ＥＣＣシステム及び共通発生器（Ｇ）について確定すること（１１０）を含む。これは、第２のノード７又は第３のノード９から、共通ＥＣＣシステム及び共通発生器を受信することを含むことができる。それに代えて、ユーザインタフェース１５は、第１のノード３に関連付けられてもよく、これによってユーザは、共通ＥＣＣシステム及び／又は共通発生器（Ｇ）を選択的に提供することができる。更に別の代替形態では、共通ＥＣＣシステム及び／又は共通発生器（Ｇ）の一方又は双方が、第１のノード３によってランダムに選択されてもよい。第１のノード３は、通信ネットワーク５を介して、共通発生器（Ｇ）と共に共通ＥＣＣシステムを用いることを示す通知を第２のノード７に送信することができる。そして、第２のノード７は、確認応答を示す通知を送信することによって、共通ＥＣＣシステム及び共通発生器（Ｇ）を用いることについて確定すること（２１０）ができる。

【００６５】
メソッド１００は、第１のノード３が第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を含む第１の非対称暗号対を作成すること（１２０）も含む。これは、少なくとも部分的に、共通ＥＣＣシステムにおいて指定される許容可能な範囲におけるランダムな整数に基づいて第１のノードのマスター私有鍵（V_{1C}）を作成することを含む。これは、以下の式

$$P_{1C}=V_{1C}\times G \quad （式１）$$

による、第１のノードのマスター私有鍵（V_{1C}）と共通発生器（Ｇ）との楕円曲線点乗算に基づいて第１のノードのマスター公開鍵（P_{1C}）を決定することも含む。
【００６６】
このようにして、第１の非対称暗号対は以下を含む。
V_{1C}：第１のノードによって秘密にされている第１のノードのマスター私有鍵。
P_{1C}：公開で知られている第１のノードのマスター公開鍵。
【００６７】
第１のノード３は、第１のノード３に関連付けられた第１のデータストア１３に第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）を記憶することができる。セキュリティのために、第１のノードのマスター私有鍵（V_{1C}）は、第１のデータストア１３のセキュアな部分に記憶され、鍵がプライベートなままであることを確実にすることができる。
【００６８】
メソッド１００は、第１のノードのマスター公開鍵（P_{1C}）を、通信ネットワーク５を介して第２のノード７に送信すること（１３０）を更に含む。第２のノード７は、第１のノードのマスター公開鍵（P_{1C}）を受信する際（２２０）、第１のノードのマスター公開鍵（P_{1C}）を、第２のノード７に関連付けられた第２のデータストア１７に記憶すること（２３０）ができる。
【００６９】
第１のノード３と同様に、第２のノード７のメソッド２００は、第２のノードのマスター私有鍵（V_{1S}）及び第２のノードのマスター公開鍵（P_{1S}）を含む第２の非対称暗号対を作成すること（２４０）を含む。第２のノードのマスター私有鍵（V_{1S}）は、許容可能な範囲内のランダムな整数でもある。そして、第２のノードのマスター公開鍵（P_{1S}）は、以下の式によって決定される。

$$P_{1S}=V_{1S}\times G \quad （式２）$$

【００７０】
このようにして、第２の非対称暗号対は、以下を含む。
V_{1S}：第２のノードによって秘密にされている第２のノードのマスター私有鍵。
P_{1S}：公開で知られている第２のノードのマスター公開鍵。
【００７１】
第２のノード７は、第２のデータストア１７に第２の非対称暗号対を記憶することができる。メソッド２００は、第２のノードのマスター公開鍵（P_{1S}）を第１のノード３に送信すること（２５０）を更に含む。そして、第１のノード３は、第２のノードのマスター公開鍵（P_{1S}）を受信し（１４０）、記憶すること（１５０）ができる。
【００７２】
いくつかの代替形態において、それぞれの公開マスター鍵が受信され、第３のノード９（信頼された第三者等）に関連付けられた第３のデータストア１９に記憶されてもよいことが理解されよう。これは、認証局等の、公開ディレクトリとしての役割を果たす第三者を含むことができる。このため、いくつかの例では、第１のノードのマスター公開鍵（P_{1C}）は、共通秘密（ＣＳ）を決定することが必要とされているときにのみ第２のノード７によって要求及び受信される場合がある（逆もまた同様である）。
【００７３】
登録ステップは、初期セットアップとして一度のみ行われればよい。その後、マスター

鍵を、セキュアな方式で再利用し、中でも、決定性鍵（ＤＫ）に依拠した共通秘密を作成することができる。

【００７４】

第１のノード３によるセッション開始及び共通秘密の決定

ここで、図４を参照して、共通秘密（ＣＳ）を決定する例を説明する。共通秘密（ＣＳ）は、第１のノード３と第２のノード７との間の特定のセッション、時間、トランザクション、又は他の目的のために用いられる場合があり、同じ共通秘密（ＣＳ）を用いることは、望ましくないか、又はセキュアでない場合がある。このため、異なるセッション、時間、トランザクション等の間で共通秘密（ＣＳ）を変更することができる。

【００７５】

メッセージ（Ｍ）の作成３１０

この例において、第１のノード３によって行われるメソッド３００は、メッセージ（Ｍ）を作成すること（３１０）を含む。メッセージ（Ｍ）は、ランダムであるか、疑似ランダムであるか、又はユーザにより定義される場合がある。１つの例では、メッセージ（Ｍ）は、Ｕｎｉｘ(ユニックス)時間及びノンス（及び任意の値）に基づいている。例えば、メッセージ（Ｍ）は、以下のように提供することができる。

メッセージ（Ｍ）＝ＵｎｉｘＴｉｍｅ＋ノンス　（式３）

【００７６】

いくつかの例では、メッセージ（Ｍ）は、任意である。しかし、メッセージ（Ｍ）は、いくつかの用途において有用であり得る選択的値（Ｕｎｉｘ時間等）を有してもよいことが理解されよう。

【００７７】

メソッド３００は、通信ネットワーク３を介して第２のノード７にメッセージ（Ｍ）を送信すること（３１５）を含む。メッセージ（Ｍ）は、私有鍵に関する情報を含んでいないので、セキュアでないネットワークを介して送信することができる。

【００７８】

決定性鍵の決定３２０

メソッド３００は、メッセージ（Ｍ）に基づいて決定性鍵（ＤＫ）を決定するステップ（３２０）を更に含む。この例において、これは、メッセージの暗号学的ハッシュを決定することを含む。暗号学的ハッシュアルゴリズムの例は、２５６ビット決定性鍵（ＤＫ）を生成するためのＳＨＡ－２５６を含む。すなわち、以下となる。

ＤＫ＝ＳＨＡ－２５６（Ｍ）　（式４）

【００７９】

他のハッシュアルゴリズムが用いられてもよいことが理解されよう。これは、セキュアハッシュアルゴリズム（ＳＨＡ）ファミリーにおける他のハッシュアルゴリズムを含むことができる。いくつかの特定の例は、ＳＨＡ３－２２４、ＳＨＡ３－２５６、ＳＨＡ３－３８４、ＳＨＡ３－５１２、ＳＨＡＫＥ１２８、ＳＨＡＫＥ２５６を含む、ＳＨＡ－３サブセットにおけるインスタンスを含む。他のハッシュアルゴリズムは、ＲＡＣＥ完全性プリミティブ評価メッセージダイジェスト（ＲＩＰＥＭＤ）ファミリーにおけるハッシュアルゴリズムを含むことができる。特定の例は、ＲＩＰＥＭＤ－１６０を含むことができる。他のハッシュ関数は、Ｚｅｍｏｒ－Ｔｉｌｌｉｃｈハッシュ関数及びナップサックベースのハッシュ関数に基づくファミリーを含むことができる。

【００８０】

第１のノードの第２の私有鍵の決定３３０

次に、メソッド３００は、第２のノードのマスター私有鍵（V_{1C}）及び決定性鍵（ＤＫ）に基づいて第１のノードの第２の私有鍵（V_{2C}）を決定するステップ（３３０）を含む。これは、以下の式

$V_{2C}=V_{1C}+DK$　（式５）

による、第１のノードのマスター私有鍵（V_{1C}）と決定性鍵（ＤＫ）とのスカラー加算に基づくことができる。

【００８１】
このようにして、第１のノードの第２の私有鍵（V_{2C}）は、ランダムな値ではなく、代わりに、第１のノードのマスター私有鍵から決定論的に導出される。暗号対における対応する公開鍵、すなわち、第１のノードの第２の公開鍵（P_{2C}）は、以下の関係を有する。

$$P_{2C}=V_{2C}\times G \quad （式６）$$

【００８２】
式５からのV_{2C}を式６に代入することにより、以下が得られる。

$$P_{2C}=(V_{1C}+DK)\times G \quad （式７）$$

【００８３】
ここで、「＋」演算子は、スカラー加算に関し、「×」演算子は、楕円曲線点乗算に関する。楕円曲線暗号代数が分配的であることに留意すると、式７は以下のように表すことができる。

$$P_{2C}=V_{1C}\times G+DK\times G \quad （式８）$$

【００８４】
最後に、式１を式７に代入し、以下を得ることができる。

$$P_{2C}=P_{1C}+DK\times G \quad （式９．１）$$

$$P_{2C}=P_{1C}+SHA-256(M)\times G \quad （式９．２）$$

【００８５】
式８～式９．２において、「＋」演算子は、楕円曲線点加算に関するものである。このため、対応する第１のノードの第２の公開鍵（P_{2C}）は、第１のノードのマスター公開鍵（P_{1C}）及びメッセージ（Ｍ）の知識を与えられると導出可能とすることができる。メソッド４００に関して以下で更に詳細に論じられるように、第２のノード７は、そのような知識を有して、第１のノードの第２の公開鍵（P_{2C}）を独立して決定することができる。

【００８６】
メッセージ及び第１のノードの第２の私有鍵に基づく第１の署名付きメッセージ（ＳＭ１）の生成３５０

メソッド３００は、メッセージ（Ｍ）及び決定された第１のノードの第２の私有鍵（V_{2C}）に基づいて、第１の署名付きメッセージ（ＳＭ１）を作成すること（３５０）を更に含む。署名付きメッセージを作成することは、デジタル署名アルゴリズムを適用して、メッセージ（Ｍ）にデジタル署名することを含む。１つの例において、これは、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）において第１のノードの第２の私有鍵（V_{2C}）をメッセージに適用して、第１の署名付きメッセージ（ＳＭ１）を得ることを含む。

【００８７】
ＥＣＤＳＡの例は、ｓｅｃｐ２５６ｋｌ、ｓｅｃｐ２５６ｒｌ、ｓｅｃｐ３８４ｒｌ、ｓｅ３ｃｐ５２１ｒｌを有するＥＣＣシステムに基づくものを含む。

【００８８】
第１の署名付きメッセージ（ＳＭ１）は、第２のノード７において、対応する第１のノードの第２の公開鍵（P_{2C}）を用いて検証することができる。第１の署名付きメッセージ（ＳＭ１）の検証は、第２のノード７によって、第１のノード３を認証するのに用いることができる。これについては、メソッド４００において以下で述べる。

【００８９】
第２のノードの第２の公開鍵の決定３７０’

次に、第１のノード３は、第２のノードの第２の公開鍵（P_{2S}）を決定すること（３７０）ができる。上記したように、第２のノードの第２の公開鍵（P_{2S}）は、少なくとも、第２のノードのマスター公開鍵（P_{1S}）及び決定性鍵（ＤＫ）に基づくことができる。この例において、公開鍵は、発生器（Ｇ）との楕円曲線点乗算により私有鍵として決定される（３７０’）ので、第２のノードの第２の公開鍵（P_{2S}）は、式６と同様の方式で、以下のように表すことができる。

$P_{2S}=V_{2S}\times G$　（式１０．１）
$P_{2S}=P_{1S}+DK\times G$　（式１０．２）

【００９０】

式１０．２の数学的証明は、第１のノードの第２の公開鍵（P_{2C}）について式９．１を導出するために上記で説明されたのと同じである。第１のノード３は、第２のノード７と独立して第２のノードの第２の公開鍵を決定すること（３７０）ができることが理解されよう。

【００９１】

第１のノード３における共通秘密の決定３８０

次に、第１のノード３は、決定された第１のノードの第２の私有鍵（V_{2C}）及び決定された第２のノードの第２の公開鍵（P_{2S}）に基づいて共通秘密（ＣＳ）を決定する（３８０）。この共通秘密（ＣＳ）は、第１のノード３によって、以下の式により決定することができる。

$S=V_{2C}\times P_{2S}$　（式１１）

【００９２】

第２のノード７において行われるメソッド４００

第２のノード７において行われる対応するメソッド４００を説明すると、これらのステップのうちのいくつかは、第１のノード３によって行われた上記したステップと類似していることが理解されよう。

【００９３】

メソッド４００は、通信ネットワーク５を介して、第１のノード３からメッセージ（Ｍ）を受信すること（４１０）を含む。これは、ステップ３１５において第１のノード３によって送信されたメッセージ（Ｍ）を含んでいる。次に、第２のノード７は、メッセージ（Ｍ）に基づいて決定性鍵（ＤＫ）を決定する（４２０）。第２のノード７によって決定性鍵（ＤＫ）を決定するステップ４２０は、上記した第１のノードによって行われるステップ３２０と類似している。この例では、第２のノード７は、この決定するステップ４２０を、第１のノード３と独立して行う。

【００９４】

次のステップは、第１のノードのマスター公開鍵（P_{1C}）及び決定性鍵（ＤＫ）に基づいて第１のノードの第２の公開鍵（P_{2C}）を決定すること（４３０）を含んでいる。この例において、公開鍵は、発生器（Ｇ）との楕円曲線点乗算により私有鍵として決定される（４３０’）ので、第１のノードの第２の公開鍵（P_{2C}）は、式９と同様の方式で、以下のように表すことができる。

$P_{2C}=V_{2C}\times G$　（式１２．１）
$P_{2C}=P_{1C}+DK\times G$　（式１２．２）

【００９５】

式１２．１及び式１２．２の数学的証明は、式１０．１及び式１０．２について上記で説明されたのと同じである。

【００９６】

第２のノード７による第１のノード３の認証

メソッド４００は、第２のノード７によって、推定の第１のノード３が第１のノード３であることを認証することによって行われるステップを含むことができる。上記したように、これは、第１のノード３から第１の署名付きメッセージ（ＳＭ１）を受信すること（４４０）を含む。次に、第２のノード７は、ステップ４３０において決定された第１のノードの第２の公開鍵（P_{2C}）を用いて、第１の署名付きメッセージ（ＳＭ１）における署名の有効性を確認する（４５０）。

【００９７】

上記したように、デジタル署名の検証は、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）に従って行うことができる。重要なことであるが、第１のノードの第２の私有鍵（V_{2C}）で署名された第１の署名付きメッセージ（ＳＭ１）は、対応する第１のノードの

第２の公開鍵（P_{2C}）によってのみ正しく検証されるべきである。なぜなら、V_{2C}及びP_{2C}は暗号対を形成するためである。これらの鍵は、第１のノード３の登録時に生成された第１のノードのマスター私有鍵（V_{1C}）及び第１のノードのマスター公開鍵（P_{1C}）に対し決定性であるので、第１の署名付きメッセージ（ＳＭ１）を検証することは、第１の署名付きメッセージ（ＳＭ１）を送信する推定の第１のノードが登録中に同じ第１のノード３であることを認証する基礎として用いることができる。このため、第２のノード７は、第１の署名付きメッセージの有効性を確認した結果（４５０）に基づいて、第１のノード３を認証するステップ（４６０）を更に行うことができる。

【００９８】

上記の認証は、２つのノードのうちの一方が信頼されるノードであり、ノードのうちの一方のみが認証される必要があるシナリオに適している。例えば、第１のノード３は、クライアントである場合があり、第２のノード７は、クライアントによって信頼されているサーバーである場合がある。このため、サーバー（第２のノード７）は、サーバーシステムへのクライアントアクセスを許可するために、クライアント（第１のノード３）の信用証明書を認証する必要がある場合がある。サーバーがクライアントに対しサーバーの信用証明書を認証することが必要ない場合がある。しかし、いくつかのシナリオでは、以下の別の例において説明されるピアツーピアシナリオ等において、双方のノードが互いに対し認証されることが望ましい場合がある。

【００９９】

第２のノード７による共通秘密の決定

メソッド４００は、第２のノード７が、第２のノードのマスター私有鍵（V_{1S}）及び決定性鍵（ＤＫ）に基づいて第２のノードの第２の私有鍵（V_{2S}）を決定すること（４７０）を更に含むことができる。第１のノード３によって行われるステップ３３０と同様に、第２のノードの第２の私有鍵（V_{2S}）は、以下の式

$$V_{2S}=V_{1S}+DK \quad （式１３．１）$$

$$V_{2S}=V_{1S}+SHA-256(M) \quad （式１３．２）$$

による第２のノードのマスター私有鍵（V_{1S}）と決定性鍵（ＤＫ）とのスカラー加算に基づくことができる。

【０１００】

次に、第２のノード７は、第１のノード３と独立して、以下の式に基づいて、第２のノードの第２の私有鍵（V_{2S}）及び第１のノードの第２の公開鍵（P_{2C}）に基づいて共通秘密（ＣＳ）を決定すること（４８０）ができる。

$$S=V_{2S}\times P_{2C} \quad （式１４）$$

【０１０１】

第１のノード３及び第２のノード７によって決定される共通秘密（ＣＳ）の証明

第１のノード３によって決定される共通秘密（ＣＳ）は、第２のノード７において決定される共通秘密（ＣＳ）と同じである。ここで、式１１及び式１４が同じ共通秘密（ＣＳ）をもたらすことの数学的証明を説明する。

【０１０２】

第１のノード３によって決定される共通秘密（ＣＳ）を参照すると、式１０．１は以下のように式１１に代入することができる。

$$S=V_{2C}\times P_{2S} \quad （式１１）$$

$$S=V_{2C}\times(V_{2S}\times G)$$

$$S=(V_{2C}\times V_{2S})\times G \quad （式１５）$$

【０１０３】

第２のノード７によって決定される共通秘密（ＣＳ）を参照すると、式１２．１は、以下のように式１４に代入することができる。

$$S=V_{2S}\times P_{2C} \quad （式１４）$$

$$S=V_{2S}\times(V_{2C}\times G)$$

$$S=(V_{2S}\times V_{2C})\times G \quad （式１６）$$

【０１０４】
ＥＣＣ代数は交換可能であるため、式１５及び式１６は等価である。従って、以下の式が成り立つ。
$$S=(V_{2C}\times V_{2S})\times G=(V_{2S}\times V_{2C})\times G \quad (式17)$$
【０１０５】
共通秘密（ＣＳ）及び秘密鍵
共通秘密（ＣＳ）は、第１のノード３と第２のノード７との間のソース通信のための対称鍵アルゴリズムにおける秘密鍵として、又は秘密鍵の基礎として用いることができる。
【０１０６】
共通秘密（ＣＳ）は、楕円曲線点（ｘｓ、ｙｓ）の形態をとすることができる。これは、ノード３、７によって合意された標準的な公開で既知の演算を用いて標準的な鍵フォーマットに変換される。例えば、ｘｓ値は、AES_{256}暗号化のための鍵として用いることができる２５６ビットの整数とすることができる。これは、この長さの鍵を必要とする任意の用途について、ＲＩＰＥＭＤ１６０を用いて１６０ビットの整数に変換することもできる。
【０１０７】
共通秘密（ＣＳ）は、要望に応じて決定することができる。重要なことであるが、第１のノード３は、共通秘密（ＣＳ）を記憶する必要がない。なぜなら、これはメッセージ（Ｍ）に基づいて再決定することができるためである。いくつかの例では、用いられるメッセージ（Ｍ）は、マスター私有鍵に必要とされるのと同じレベルのセキュリティを有することなく、データストア１３、１７、１９（又は他のデータストア）に記憶することができる。いくつかの例では、メッセージ（Ｍ）は、公開で入手可能である場合がある。
【０１０８】
しかし、用途によっては、共通秘密（ＣＳ）が第１のノードのマスター私有鍵（V_{1C}）としてセキュアに保持されている限り、共通秘密（ＣＳ）は、第１のノードに関連付けられた第１のデータストア（Ｘ）に記憶することができる。
【０１０９】
更に、此処に開示されるシステムは、単一のマスター鍵暗号対に基づいて、複数のセキュアな秘密鍵に対応することができる複数の共通秘密の決定を可能にすることができる。この利点は、以下の例によって説明することができる。
【０１１０】
各々が複数のそれぞれの共通秘密（ＣＳ）に関連付けられた複数のセッションが存在する状況では、それぞれの共通秘密（ＣＳ）を未来のために再決定することができるように、これらの複数のセッションに関連付けられたレコードを有することが望ましい場合がある。既知のシステムでは、これは、複数の秘密鍵が、維持が高価であるか又は不都合である場合があるセキュアなデータストアに記憶されることを必要としていた場合がある。対照的に、本システムは、それぞれの第１のノード及び第２のノードにおいてマスター私有鍵をセキュアに保持するのに対し、他の決定性鍵又はメッセージ（Ｍ）は、セキュアに記憶されていてもよく、セキュアでなく記憶されていてもよい。決定性鍵（ＤＫ）又はメッセージ（Ｍ）がセキュアでなく記憶されているにもかかわらず、共通秘密を決定するのに必要とされるマスター私有鍵は依然としてセキュアであるため、複数の共通秘密は（ＣＳ）はセキュアに保持される。
【０１１１】
本方法は、例えばログインパスワードをセキュアに送信するために、一時的通信リンクのための「セッション鍵」を作成するのに用いることもできる。
【０１１２】
例示的な用途
本明細書に開示の方法、デバイス及びシステムは、限定ではないが、以下に説明するものを含む複数の用途を有する。
【０１１３】

メッセージ暗号化

本明細書の開示は、セキュアな通信、特に、潜在的にセキュアでない通信ネットワーク５を介して第１のノード３と第２のノード７との間で通信メッセージを送信及び受信することを容易にするのに用いることができる。これは、対称鍵の基礎として共通秘密（ＣＳ）を用いることによって達成することができる。共通秘密（ＣＳ）を決定し、通信メッセージの暗号化及び復号のために対称鍵を用いるこの方法は、既知の公開鍵暗号化方法と比較して、計算効率を良くすることができる。

【０１１４】

第１のノード３と第２のノード７との間のセキュアな通信のメソッド５００、６００を、図５を参照して説明すると、第１のノード３は、上記の方法において決定された共通秘密（ＣＳ）に基づいて対称鍵を決定する（５１０）。これは、共通秘密（ＣＳ）を標準的な鍵フォーマットに変換することを含んでいる。同様に、第２のノード７も、共通秘密（ＣＳ）に基づいて対称鍵を決定すること（６１０）ができる。

【０１１５】

第１のノード３から、通信ネットワークを介して第２のノードにセキュアに第１の通信メッセージを送信するために、第１の通信メッセージを暗号化する必要がある。このため、第１のノードによって第１の通信メッセージを暗号化して第１の暗号化通信メッセージを形成するために対称鍵が用いられる（５２０）。この暗号化された第１の通信メッセージは、次に、通信ネットワーク５を介して、第２のノード７に送信される（５３０）。そして、第２のノード７は、暗号化された第１の通信メッセージを受信し（６２０）、暗号化された第１の通信メッセージを、対称鍵を用いて第１の通信メッセージに復号する（６３０）。

【０１１６】

同様に、第２のノード７は、対称鍵を用いて、第２の通信メッセージを暗号化された第２の通信メッセージに暗号化すること（６４０）ができる。この第２の暗号化通信メッセージは、次に、第１のノード３に送信される（６５０）。次に、第１のノード３は、暗号化された第２の通信メッセージを受信し（５４０）、これを第２の通信メッセージに復号する（５５０）。

【０１１７】

暗号通貨ウォレット

他の例では、このメソッドは、暗号通貨トランザクションのための秘密鍵等の共通秘密（ＣＳ）の作成及び管理のために用いることができる。ビットコイントランザクションにおいて用いられているもの等の暗号通貨鍵は、通常、バリュー（value）と交換することができる資金及び資産に関連付けられている。

【０１１８】

電子リソースレンタル

電子リソースレンタルを容易にするための方法及びシステムを用いる例を図６を参照して説明すると、これは、第１のノード３がクライアント７０３に関連付けられ、第２のノード７が電子リソース、例えばスーパーコンピュータ施設７０７に関連付けられるシステム７０１を示す。従って、クライアント５０４は、大量の機密データを処理するために遠隔に位置するスーパーコンピュータ施設７０７を用いることを望むことができる。

【０１１９】

スーパーコンピュータ施設７０７は、時間単位及び／又はＣＰＵサイクル単位でスーパーコンピュータＣＰＵ時間を貸し出すことができる。クライアント７０３は、自身の公開鍵を預けることによって、例えば、通信ネットワーク５を介して、第１のノードのマスター公開鍵（P_{1C}）を第２のノード７に送信すること（１３０）によって、スーパーコンピュータ施設に登録することができる。

【０１２０】

スーパーコンピュータ施設７０７は、次に、ＡＥＳ暗号化を用いてセキュアな接続を確立する等のバックグラウンドプロセスを行い、上記したメソッド３００のステップを容易

にするためのソフトウェアをクライアント７０３に提供することができる。

【０１２１】

メソッド３００を行うとき、第１のノード３は、ノンスとリンクされたＵｎｉｘ時間を含むメッセージ（Ｍ）に部分的に基づく第１の署名付きメッセージ（ＳＭ１）を送信すること（３６０）ができる。

【０１２２】

第２のノード７は、第１の署名付きメッセージ（ＳＭ１）を受信する（４４０）。第２のノード７は、メッセージ（Ｍ）におけるＵｎｉｘ時間がＵｎｉｘ時間のために許容される値の範囲内にあるか否かを判断するステップを更に行う。例えば、Ｕｎｉｘ時間のために許容される値は、クライアント７０３とスーパーコンピュータ施設７０７との間で確定された条項及び条件に従って設定することができる。例えば、（メッセージの）Ｕｎｉｘ時間は、スーパーコンピュータ施設が第１の署名付きメッセージ（ＳＭ１）を受信する（４４０）設定された期間（例えば、３００秒）以内であることが必要とされる場合がある。メッセージ（Ｍ）におけるＵｎｉｘ時間が許容される時間外である場合、機密データの交換は受容されない。

【０１２３】

上記のステップは、ステップ３８０、４８０において決定された共通秘密（ＣＳ）に基づく結果として得られるセッション鍵を、後の時点において決して再現することができないで、確立されているセッションに特有であることを確実にすることができる。次に、プロトコルを用いて、セッションの持続時間にわたってＡＥＳ暗号化／復号鍵等の対称セッション鍵を確立することができる。セッション鍵は、セッションの持続時間にわたって第１のノード３と第２のノード７との間の全ての通信に用いられる。これによって、クライアントは、コード及び／又は大量のデータを暗号化し、これらを処理のためにスーパーコンピュータ施設７０７に送信し、スーパーコンピュータ施設７０７から返された暗号化結果を受信することが可能になる。

【０１２４】

パスワード交換、補完又は代替

このシステム及び方法は、パスワード交換、補完又はこれらに代替するものとして用いることもできる。図７を参照すると、ユーザ及び複数の追加ノード７’、７’’、７’’’に関連付けられた第１のノード３を含むシステムが提供される。複数の追加のノードは、各々、同じプロトコルに参加するそれぞれの機関に関連付けることができる。例えば、機関は、銀行、サービスプロバイダ、政府サービス、保険会社、電気通信プロバイダ、小売店等を含むことができる。

【０１２５】

ユーザ８０３は、サービスにアクセスするためにこれらの機関にセキュアな方式で通信することを望んでいる。既知のシステムにおいて、これは、ユーザが、それぞれの機関ごとにログインするための複数のパスワードを有することを必要とする。複数の機関に対してログインのために同じパスワードを用いることは、セキュリティの理由から望ましくない。

【０１２６】

この例において、ユーザ及び複数の機関は、同じプロトコルの使用について確定する。これは、ＥＣＣシステム（ｓｅｃｐ２５６ｋｌ、ｓｅｃｐ２５６ｒｌ、ｓｅｃｐ３８４ｒｌ、ｓｅｃｐ５２１ｒｌに基づくもの等）及び発生器（Ｇ）について確定することも含むことができる。次に、ユーザは、第１のノードのマスター公開鍵（P_{1C}）を複数の機関及び関連付けられた追加ノード７’、７’’、７’’’に登録し、これを共有することができる。追加ノード７’、７’’、７’’’は、各々、上記したような第２のノード７に類似した方法のステップを行うことができる。

【０１２７】

ユーザ８０３は、参加する機関のウェブサイトのうちの１つにログインすることを望むたびにパスワードを用いる必要はない。代わりに、プロトコルが、機関ごとのパスワード

の必要性に置き換えられる。第１のノード３において必要とされるのは、常に入手可能な機関の公開鍵、及び機関におけるユーザの登録（第１のノードのマスター公開鍵（P_{1C}）を機関に登録することを含む）のみである。ユーザによる機関への登録は、ウェブベースのサービスを用いるための慣例であるため、これは、ユーザ８０３にとって負担とならない。登録が完了すると、パスワードの代わりに共通秘密（ＣＳ）を決定し、使用し、再利用すること（３１０）ができる。例えば、全てのセッションの開始時に、第１のノード３は、セッションに関与する追加ノード７’、７’’、７’’’に送信されるメッセージ（Ｍ）を作成することができる。メッセージ（Ｍ）は、対応する決定性鍵を決定する（３２０、４２０）のに用いられ、この決定性鍵は、次に、上記の方法において説明されたように、第１のノード３及び追加ノード７’、７’’、７’’’の双方によって用いられ、共通秘密（ＣＳ）が決定される。それに代えて、メッセージ（Ｍ）は、追加ノード７’、７’’、７’’’から作成又は受信することができる。更に他の代替形態では、メッセージ（Ｍ）は、第１のノード３及び／又は追加ノード７’、７’’、７’’’によってアクセス可能なデータストア１３、１７、１９に記憶された所定のメッセージとすることができる。

【０１２８】

この技法は、機関から大きなセキュリティの負担を取り除く。特に、共通秘密は、非秘密情報から再計算することができるので、機関は、もはやパスワードファイル（パスワードの秘密レコード又はパスワードハッシュ）を保持する必要がない。むしろ、機関は、自身の独自のマスター私有鍵をセキュアに保持するのみでよい。更に、ユーザは、自身の第１のノードのマスター私有鍵（V_{1C}）をセキュアに保持することができる限り、多くのパスワード（機関ごとに１つ）を覚えておくか又はセキュアに記憶する必要がない。

【０１２９】

変形形態

ここで、以下の例を参照して、いくつかの変形形態を説明する。

【０１３０】

ピアツーピア認証

ピアツーピアのシナリオにおいて、第１のノード３及び第２のノード７は、互いの信用証明書を認証する必要がある。この例を図８を参照して説明すると、この例において、有効性を確認された第１の署名付きメッセージ（ＳＭ１）に基づいて第１のノード３を認証するためのメソッド３００、４００のステップは、上記したものと類似している。

【０１３１】

しかし、第２のノード７によって行われるメソッド４００は、メッセージ（Ｍ）及び第２のノードの私有鍵（V_{2S}）に基づいて第２の署名付きメッセージ（ＳＭ２）を作成すること（４６２）を更に含む。いくつかの代替形態では、第２の署名付きメッセージ（ＳＭ２）は、第２のメッセージ（Ｍ２）及び第２のノードの私有鍵（V_{2S}）に基づくことができ、ここで、第２のメッセージ（Ｍ２）は第１のノード３と共有される。メソッド４００は、第２の署名付きメッセージ（ＳＭ２）を、通信ネットワーク５を介して第１のノード３に送信すること（４６４）を更に含む。

【０１３２】

第１のノード３において、メソッド３００は、第２のノード７から第２の署名付きメッセージ（ＳＭ２）を受信することを含む。このメソッドは、ステップ３７０において決定された第２のノードの第２の公開鍵（P_{2S}）を用いて第２の署名付きメッセージ（ＳＭ２）における署名の有効性を確認すること（３７４）を含む。メソッド３００は、次に、第２の署名付きメッセージ（ＳＭ２）の有効性を確認した結果に基づいて第２のノード７を認証すること（３７６）を含んでいる。この結果、第１のノード３及び第２のノード７は互いを認証する。

【０１３３】

決定性鍵の階層

１つの例において、一連の連続した決定性鍵を決定し、各連続した鍵を、先行する決定

性鍵に基づいて決定する。

【０１３４】

例えば、ノード間の事前の合意によって、ステップ３１０～３７０及び４１０～４７０を繰り返して連続した単一の目的の鍵を作成する代わりに、以前に用いられた決定性鍵（ＤＫ）を、双方の関係者によって繰り返し再ハッシングして、決定性鍵の階層を確立することができる。実際に、決定性鍵は、メッセージ（Ｍ）のハッシュに基づいて、次世代の決定性鍵（ＤＫ’）のための次世代メッセージ（Ｍ’）とすることができる。これを行うことにより、更なるプロトコル確立送信、特に、共通秘密の世代ごとの複数のメッセージの送信を必要とすることなく、共有される秘密の連続作成が可能になる。次世代共通秘密（ＣＳ’）は以下のように計算することができる。

【０１３５】

まず、第１のノード３及び第２のノード７の双方が独立して次世代の決定性鍵（ＤＫ’）を決定する。これは、ステップ３２０及び４２０に類似しているが、以下の式により適合される。

Ｍ’＝ＳＨＡ－２５６（Ｍ）　（式１８）

ＤＫ’＝ＳＨＡ－２５６（Ｍ’）　（式１９．１）

ＤＫ’＝ＳＨＡ－２５６（ＳＨＡ－２５６（Ｍ））　（式１９．２）

【０１３６】

次に、第１のノード３は、上記したステップ３７０及び３３０に類似した次世代の第２のノードの第２の公開鍵（P_{1S}’）及び第１のノードの第２の私有鍵（V_{2C}’）を決定することができるが、以下の式により適合される。

P_{2S}’＝P_{1S}＋ＤＫ’×Ｇ　（式２０．１）

V_{2C}’＝V_{1C}＋ＤＫ’　（式２０．２）

【０１３７】

次に、第２のノード７は、上記したステップ４３０及び４７０に類似した次世代の第１のノードの第２の公開鍵（P_{1C}’）及び第２のノードの第２の私有鍵（V_{2S}’）を決定することができるが、以下の式により適合される。

P_{2C}’＝P_{1C}＋ＤＫ’×Ｇ　（式２１．１）

V_{2S}’＝V_{1S}＋ＤＫ’　（式２１．２）

【０１３８】

次に、第１のノード３及び第２のノード７は、各々、次世代の共通秘密（ＣＳ’）を決定する。

【０１３９】

特に、第１のノード３は、以下の式を用いて次世代共通秘密（ＣＳ’）を決定する。

ＣＳ’＝V_{2C}’×P_{2S}’　（式２２）

【０１４０】

第２のノード７は、以下の式を用いて次世代共通秘密（ＣＳ’）を決定する。

ＣＳ’＝V_{2S}’×P_{2C}’　（式２３）

【０１４１】

更なる世代（ＣＳ’’、ＣＳ’’’等）は、チェーン階層を生成するのと同様にして計算することができる。この技法は、第１のノード３及び第２のノード７の双方が、元のメッセージ（Ｍ）又は最初に計算された決定性鍵（ＤＫ）、並びにいずれのノードに自身が関係するかを追跡することを必要とする。これは公開で既知の情報であるため、この情報の保有に関するセキュリティ問題は存在しない。従って、この情報は、「ハッシュテーブル」（ハッシュ値を公開鍵にリンクする）において保持され、（例えば、Ｔｏｒｒｅｎｔを用いて）ネットワーク５を通して自由に配信され得る。更に、階層における任意の個々の共通秘密（ＣＳ）が損なわれた場合、私有鍵V_{1C}、V_{1S}がセキュアなままであるならば、これは階層におけるいかなる他の共通秘密のセキュリティにも影響を及ぼさない。

【０１４２】

鍵のツリー構造

上記したようなチェーン（線形）階層と同様に、ツリー構造の形式の階層を生成することができる。

【０１４３】

ツリー構造を用いて、認証鍵、暗号化鍵、署名鍵、支払い鍵等の異なる目的の多岐にわたる鍵を決定し、これによって、これらの鍵は、全て、単一のセキュアに維持されたマスター鍵にリンクされる。これは、多岐にわたる異なる鍵を有するツリー構造９０１を示す図９に最も良く示されている。これらの各々を用いて、別の関係者と共有される秘密を生成することができる。

【０１４４】

ツリー分岐は、幾つかの方法で達成することができ、それらのうちの３つを以下で説明する。

【０１４５】

（ｉ）マスター鍵生成

チェーン階層において、各新たな「リンク」（公開鍵／私有鍵対）は、複数の再ハッシングされたメッセージを元のマスター鍵に加算することによって生成される。例えば、以下の式が成り立つ（明確にするため、第１のノード３の私有鍵のみを示す）。

$V_{2C}=V_{1C}+SHA-256(M)$　（式２４）

$V_{2C}'=V_{1C}+SHA-256(SHA-256(M))$　（式２５）

$V_{2C}''=V_{1C}+SHA-256(SHA-256(SHA-256(M)))$　（式２６）

…等

【０１４６】

分岐を生成するために、任意の鍵をサブマスター鍵として用いることができる。例えば、正規のマスター鍵について行われたようにV_{2C}'にハッシュを加算することによって、V_{2C}'をサブマスター鍵（V_{3C}）として用いることができる。

$V_{3C}=V_{2C}'+SHA-256(M)$　（式２７）

【０１４７】

サブマスター鍵（V_{3C}）自体が、例えば以下の次世代鍵を有することができる。

$V_{3C}'=V_{2C}'+SHA-256(SHA-256(M))$　（式２８）

【０１４８】

このようにして、図１０に示すようなマスター鍵生成方法を用いたツリー構造９０３が提供される。

【０１４９】

（ｉｉ）論理的関連付け

この方法において、ツリー内の全てのノード（公開鍵／私有鍵対）が、チェーンとして（又は任意の他の形で）作成され、ツリー内のノード間の論理的関係が、テーブルによって維持されるが、このテーブルでは、ツリー内の各ノードは、単に、ポインターを用いてツリー内の自身の親ノードと関連付けられる。このため、ポインターを用いて、セッションのための共通秘密鍵（ＣＳ）を決定するために、関連する公開鍵／私有鍵対を決定することができる。

【０１５０】

（ｉｉｉ）メッセージ多重度

チェーン又はツリーにおける任意のポイントに新たなメッセージを導入することによって、新たな公開鍵／私有鍵対を作成することができる。メッセージ自体は、任意とすることができるか、又は何らかの意味若しくは機能を有することができる（例えば、メッセージは、「実際の」銀行口座番号等に関連している場合がある等）。新たな公開鍵／私有鍵対を形成するために、そのような新たなメッセージがセキュアに保たれることが望ましい場合がある。

【０１５１】

処理デバイス

上述したように、第１のノード３及び第２のノード７は、コンピュータ、タブレットコンピュータ、モバイル通信デバイス、コンピュータサーバー等の電子デバイスとすることができる。電子デバイスは、処理デバイス２３、２７と、データストア１３、１７と、ユーザインタフェース１５とを含むことができる。

【０１５２】

図１１は、処理デバイス２３、２７の例を示す。処理デバイス２３、２７は、第１のノード３、第２のノード７又は他のノード９で用いることができる。処理デバイス２３、２７は、プロセッサ１５１０と、メモリ１５２０と、バス１５３０を介して互いに通信するインタフェースデバイス１５４０とを含む。メモリ１５２０は、上記したメソッド１００、２００、３００、４００を実施するための命令及びデータを記憶し、プロセッサ１５１０は、メモリ１５２０からの命令を実行してメソッド１００、２００、３００、４００を実施する。インタフェースデバイス１５４０は、通信ネットワーク５、及び幾つかの例では、ユーザインタフェース１５及びデータストア１３、１７、１９等の周辺機器との通信を容易にする通信モジュールを含むことができる。処理デバイス１５０１は、独立したネットワーク要素であってもよいが、別個のネットワーク要素の一部であってもよいことに留意されたい。更に、処理デバイス１５０１によって行われる幾つかの機能は、複数のネットワーク要素間で分散させることができる。例えば、第１のノード３は、第１のノード３に関連付けられたセキュアなローカルエリアネットワークにおいてメソッド１００、３００を行うための複数の処理デバイス２３を有することができる。

【０１５３】

本明細書は、ユーザ、発行者、業者、プロバイダ又は他のエンティティが特定のアクション（署名、発行、決定、計算、送信、受信、生成等を含む）を行うことを説明しているが、この表現は、提示を明確にするために用いられている。これらのアクションは、これらのエンティティによって操作されるコンピューティングデバイスによって行われることが理解されるべきである。

【０１５４】

署名は、暗号関数を実行することを含む。暗号関数は、平文のための入力と、私有鍵等の鍵のための入力とを有する。プロセッサは、関数を実行して、署名として用いることができる数字又は文字列を計算することができる。次に、署名は、署名付きテキストを提供するために平文とともに提供される。メッセージテキスト又は鍵が単一ビット変化する場合、署名は完全に変化する。署名の計算は、ほとんど計算能力を必要としないのに対し、所与の署名を有するメッセージの再現は、実際的に不可能である。このようにして、平文は、私有鍵が利用可能である場合にのみ変更され、有効な署名が付される。更に、他のエンティティは、公開で入手可能な公開鍵を用いて署名を容易に検証することができる。

【０１５５】

ほとんどの環境において、暗号化及び復号は、暗号関数を実行して、暗号化メッセージ又は平文メッセージがそれぞれ表す出力文字列を計算するプロセッサを備える。

【０１５６】

鍵、トークン、メタデータ、トランザクション、オファー、契約、署名、スクリプト、メタデータ、招待等は、「文字列」若しくは「整数」タイプ若しくは他のタイプ又はテキストファイルのプログラムコードにおける変数等の、データメモリに記憶される数字、テキスト又は文字列として表されるデータを指す。

【０１５７】

ピアツーピア台帳の例は、ビットコインＢｌｏｃｋｃｈａｉｎである。資金又は支払い料金をビットコイン貨幣で転送することは、ビットコインＢｌｏｃｋｃｈａｉｎにおいて、資金又は料金がトランザクションから出力されるトランザクションを生成することを含む。ビットコイントランザクションの例は、入力トランザクションハッシュ、トランザクション量、１つ又は複数の宛先、単数又は複数の受取人の公開鍵、及び入力トランザクションを入力メッセージとして使用することにより生成される署名、並びに署名を計算するための支払人の私有鍵を含む。トランザクションは、入力トランザクションハッシュがビ

ットコインＢｌｏｃｋｃｈａｉｎのコピーにおいて存在すること、及び公開鍵を用いて署名が正しいことをチェックすることによって検証することができる。同じ入力トランザクションハッシュが、他の箇所で既に用いられていないことを確実にするために、トランザクションは、計算ノード（「マイナー」）のネットワークにブロードキャストされる。マイナーは、入力トランザクションハッシュがまだ接続されておらず、かつ署名が有効である場合にのみ、Ｂｌｏｃｋｃｈａｉｎにおけるトランザクションを受け入れ、記録する。入力トランザクションハッシュが既に異なるトランザクションにリンクされている場合、マイナーはトランザクションを拒否する。

【０１５８】

トークンに暗号通貨を割り当てることは、トランザクションのメタデータフィールドに表される割り当てられた暗号通貨及びトークンを用いてトランザクションを生成することを含む。

【０１５９】

２つの項目が関連しているとき、これは、これらの項目間に論理的接続が存在していることを意味する。データベースにおいて、例えば、２つの項目を互いに関連付けるために、２つの項目のための識別子を同じレコードに記憶することができる。トランザクションにおいて、２つの項目を互いに関連付けるために、２つの項目のための識別子をトランザクション文字列に含めることができる。

【０１６０】

ビットコインプロトコルの使用、スクリプトの回復、及び／又はトークンのロック解除は、私有鍵を用いてスクリプト及び／又はトランザクションの署名文字列を計算することを含む。スクリプトは、異なる私有鍵又は他の条件から導出された２つ以上の署名を必要とする場合がある。次いで、このトランザクションの出力は、マイナーに与えられる。

【０１６１】

別のエンティティを認可することは、私有鍵を用いてトランザクションの署名文字列を計算し、署名文字列をエンティティに提供して、エンティティが署名を用いてトランザクションを検証することを可能にすることを含むことができる。

【０１６２】

別のエンティティとのアカウントを有するユーザは、電子メールアドレス、名称、及び潜在的には公開鍵等の、ユーザに関する情報を記憶するエンティティを含む場合がある。例えば、エンティティは、ＳＱＬ、ＯｒｉｅｎｔＤＢ、ＭｏｎｇｏＤＢ等のデータベースを維持することができる。幾つかの例では、エンティティは、ユーザの私有鍵のうちの１つ又は複数を記憶することもできる。

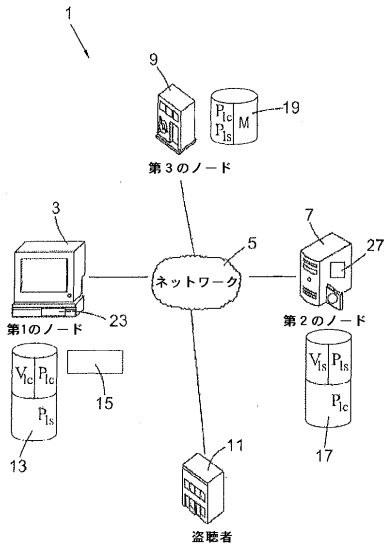
【０１６３】

当業者であれば、本発明は、従来技術を上回る多数の技術的利益及び利点を提供することを理解するであろう。例えば、（例えばビットコイン開発者の手引に記載されているような）ＢＩＰ３２プロトコルは、ランダムシードを用いてサブ鍵を作成する。これによって、インデックスのデータベースを維持する必要が生じる。しかし、本発明によれば、有意義なメッセージＭを用いてサブ鍵を（従ってサブ共有秘密も）生成する。有利には、これにより、インデックスのデータベースの必要性が回避され、このため、これを実行するのに必要な計算リソースの観点からより効率的な、より単純なセキュリティ技法が提供される。更に、これは、有意義な情報とサブ鍵との関連付けを可能にする。例えば、再利用可能なサブ鍵を用いて、特定の銀行アカウント又はクライアントコード等を表すことができる。それに代えて、特定のインボイス又はムービー（又は他のデータ）ファイル等のハッシングに基づいて、使い捨てのサブ鍵が作成されてもよい。

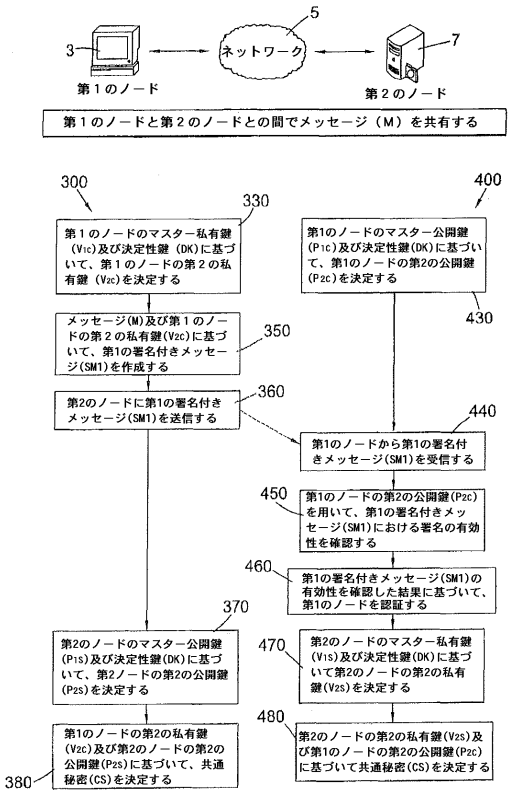
【０１６４】

当業者であれば、添付の特許請求の範囲において定義されるような本明細書の開示の広い一般的な範囲から逸脱することなく、上記した実施形態に対し多数の変形及び／又は変更を行うことができることが理解されよう。従って、本実施形態は、全ての観点において限定的ではなく例示的であることを考慮すべきである。

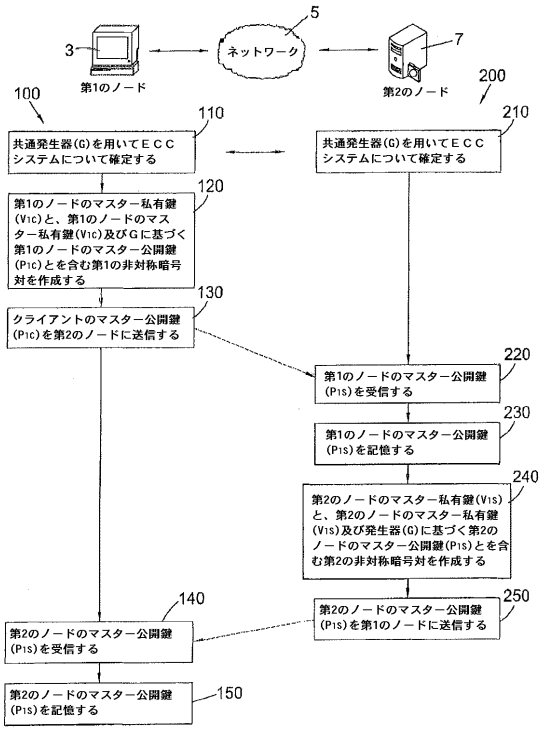
【図１】


1
9
19
第３のノード
3
5
7
27
ネットワーク
第１のノード
23
第２のノード
15
13
17
11
盗聴者

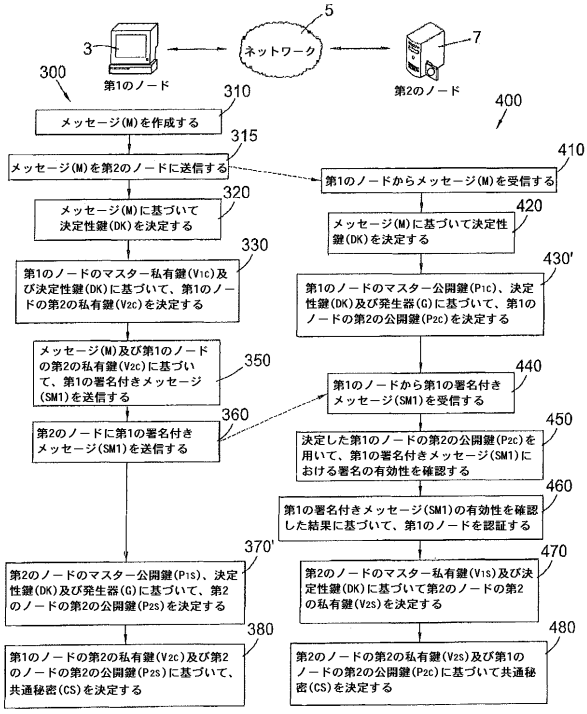
【図２】


3
5
7
ネットワーク
第１のノード
第２のノード
第１のノードと第２のノードとの間でメッセージ（M）を共有する
300
400
330
第１のノードのマスター私有鍵(V1C)及び決定性鍵(DK)に基づいて、第１のノードの第２の私有鍵(V2C)を決定する
第1のノードのマスター公開鍵(P1C)及び決定性鍵(DK)に基づいて、第1のノードの第2の公開鍵(P2C)を決定する
430
メッセージ(M)及び第１のノードの第２の私有鍵(V2C)に基づいて、第1の署名付きメッセージ(SM1)を作成する
350
第2のノードに第1の署名付きメッセージ(SM1)を送信する
360
440
第1のノードから第1の署名付きメッセージ(SM1)を受信する
450
第1のノードの第2の公開鍵(P2C)を用いて、第1の署名付きメッセージ(SM1)における署名の有効性を確認する
460
第1の署名付きメッセージ(SM1)の有効性を確認した結果に基づいて、第1のノードを認証する
370
470
第2のノードのマスター公開鍵(P1S)及び決定性鍵(DK)に基づいて、第2ノードの第2の公開鍵(P2S)を決定する
第2のノードのマスター私有鍵(V1S)及び決定性鍵(DK)に基づいて第2のノードの第2の私有鍵(V2S)を決定する
480
第1のノードの第2の私有鍵(V2C)及び第2のノードの第2の公開鍵(P2S)に基づいて、共通秘密(CS)を決定する
第2のノードの第2の私有鍵(V2S)及び第1のノードの第2の公開鍵(P2C)に基づいて共通秘密(CS)を決定する
380

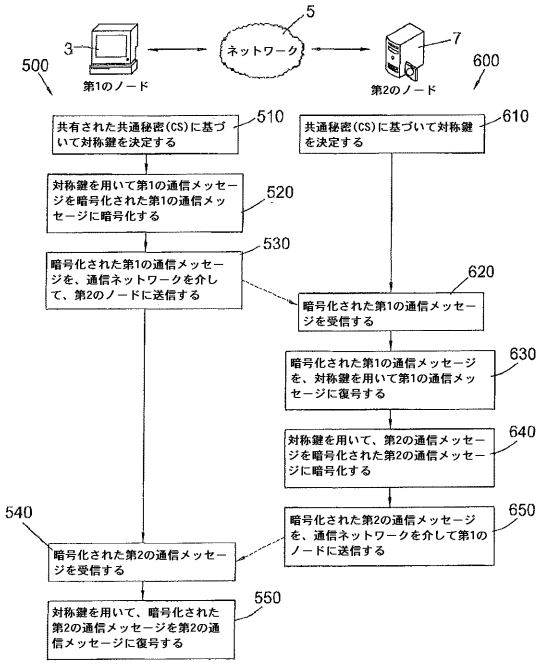
【図３】


3
5
7
ネットワーク
第1のノード
第2のノード
100
200
110
共通発生器(G)を用いてＥＣＣシステムについて確定する
210
共通発生器(G)を用いてＥＣＣシステムについて確定する
120
第1のノードのマスター私有鍵(V1C)と、第1のノードのマスター私有鍵(V1C)及びGに基づく第1のノードのマスター公開鍵(P1C)とを含む第1の非対称暗号対を作成する
130
クライアントのマスター公開鍵(P1C)を第2のノードに送信する
220
第1のノードのマスター公開鍵(P1S)を受信する
230
第1のノードのマスター公開鍵(P1S)を記憶する
240
第2のノードのマスター私有鍵(V1S)と、第2のノードのマスター私有鍵(V1S)及び発生器(G)に基づく第2のノードのマスター公開鍵(P1S)とを含む第2の非対称暗号対を作成する
140
250
第2のノードのマスター公開鍵(P1S)を受信する
第2のノードのマスター公開鍵(P1S)を第1のノードに送信する
第2のノードのマスター公開鍵(P1S)を記憶する
150

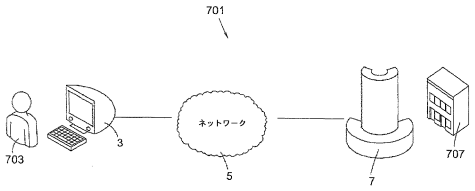
【図４】


3
5
7
ネットワーク
第1のノード
第2のノード
300
400
310
メッセージ(M)を作成する
315
メッセージ(M)を第2のノードに送信する
410
第1のノードからメッセージ(M)を受信する
320
メッセージ(M)に基づいて決定性鍵(DK)を決定する
420
メッセージ(M)に基づいて決定性鍵(DK)を決定する
330
第1のノードのマスター私有鍵(V1C)及び決定性鍵(DK)に基づいて、第1のノードの第2の私有鍵(V2C)を決定する
430'
第1のノードのマスター公開鍵(P1C)、決定性鍵(DK)及び発生器(G)に基づいて、第1のノードの第2の公開鍵(P2C)を決定する
メッセージ(M)及び第1のノードの第2の私有鍵(V2C)に基づいて、第1の署名付きメッセージ(SM1)を送信する
350
440
第1のノードから第1の署名付きメッセージ(SM1)を受信する
第2のノードに第1の署名付きメッセージ(SM1)を送信する
360
450
決定した第1のノードの第2の公開鍵(P2C)を用いて、第1の署名付きメッセージ(SM1)における署名の有効性を確認する
460
第1の署名付きメッセージ(SM1)の有効性を確認した結果に基づいて、第1のノードを認証する
370'
470
第2のノードのマスター公開鍵(P1S)、決定性鍵(DK)及び発生器(G)に基づいて、第2のノードの第2の公開鍵(P2S)を決定する
第2のノードのマスター私有鍵(V1S)及び決定性鍵(DK)に基づいて第2のノードの第2の私有鍵(V2S)を決定する
380
480
第1のノードの第2の私有鍵(V2C)及び第2のノードの第2の公開鍵(P2S)に基づいて、共通秘密(CS)を決定する
第2のノードの第2の私有鍵(V2S)及び第1のノードの第2の公開鍵(P2C)に基づいて共通秘密(CS)を決定する

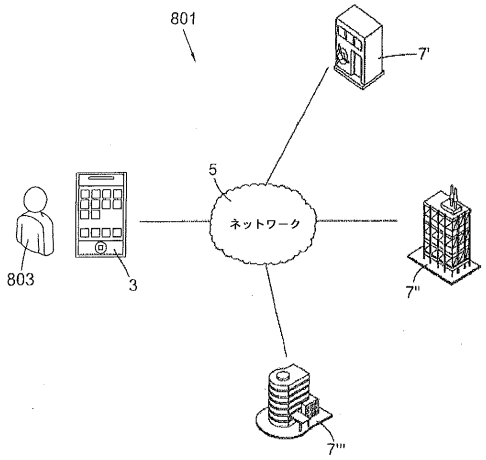
【図５】


5
3
ネットワーク
7
500
第1のノード
第2のノード
600
共有された共通秘密(CS)に基づいて対称鍵を決定する
510
共通秘密(CS)に基づいて対称鍵を決定する
610
対称鍵を用いて第1の通信メッセージを暗号化された第1の通信メッセージに暗号化する
520
暗号化された第1の通信メッセージを、通信ネットワークを介して、第2のノードに送信する
530
620
暗号化された第1の通信メッセージを受信する
暗号化された第1の通信メッセージを、対称鍵を用いて第1の通信メッセージに復号する
630
対称鍵を用いて、第2の通信メッセージを暗号化された第2の通信メッセージに暗号化する
640
暗号化された第2の通信メッセージを、通信ネットワークを介して第1のノードに送信する
650
540
暗号化された第2の通信メッセージを受信する
対称鍵を用いて、暗号化された第2の通信メッセージを第2の通信メッセージに復号する
550

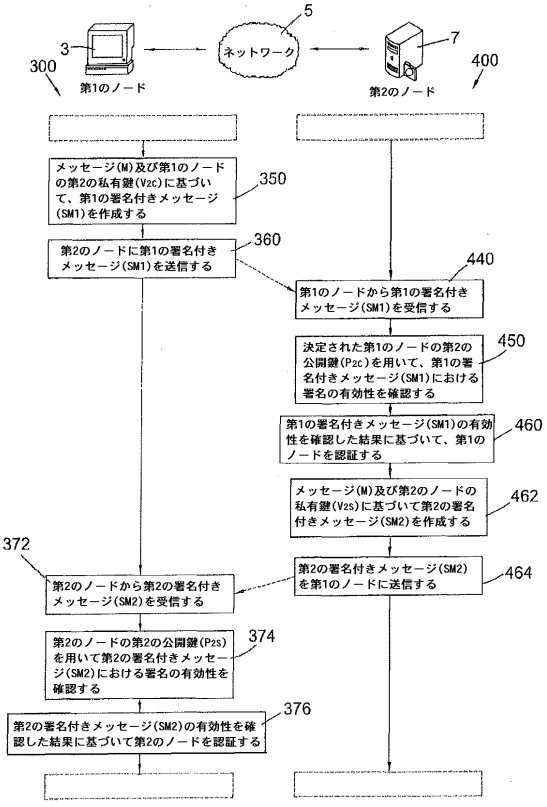
【図６】


701
703
3
ネットワーク
5
7
707

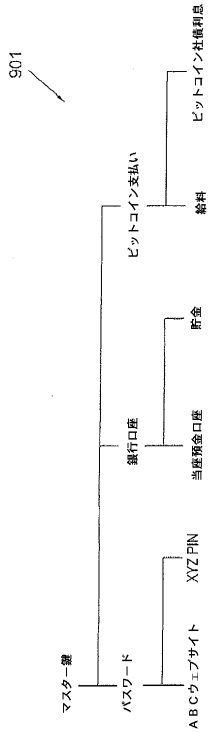
【図７】


801
7'
5
ネットワーク
803
3
7''
7'''

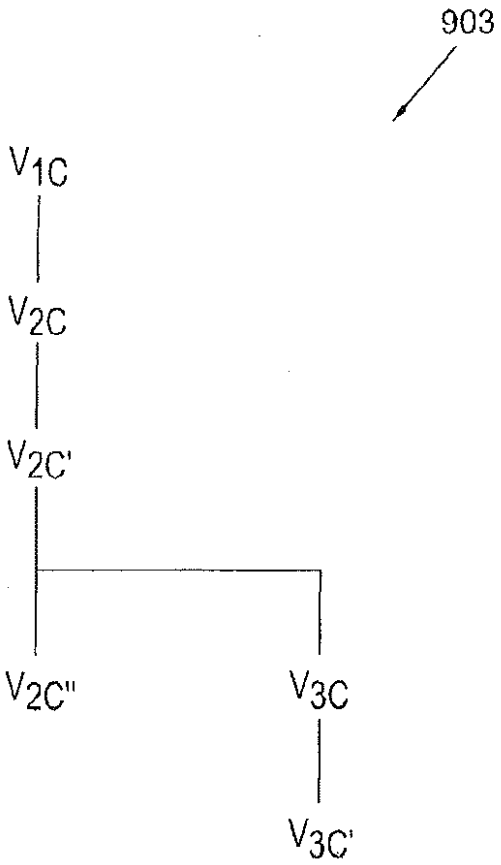
【図８】


5
3
ネットワーク
7
300
400
第1のノード
第2のノード
メッセージ(M)及び第1のノードの第2の私有鍵(V2c)に基づいて、第1の署名付きメッセージ(SM1)を作成する
350
第2のノードに第1の署名付きメッセージ(SM1)を送信する
360
440
第1のノードから第1の署名付きメッセージ(SM1)を受信する
決定された第1のノードの第2の公開鍵(P2c)を用いて、第1の署名付きメッセージ(SM1)における署名の有効性を確認する
450
第1の署名付きメッセージ(SM1)の有効性を確認した結果に基づいて、第1のノードを認証する
460
メッセージ(M)及び第2のノードの私有鍵(V2s)に基づいて第2の署名付きメッセージ(SM2)を作成する
462
372
第2のノードから第2の署名付きメッセージ(SM2)を受信する
第2の署名付きメッセージ(SM2)を第1のノードに送信する
464
第2のノードの第2の公開鍵(P2s)を用いて第2の署名付きメッセージ(SM2)における署名の有効性を確認する
374
第2の署名付きメッセージ(SM2)の有効性を確認した結果に基づいて第2のノードを認証する
376

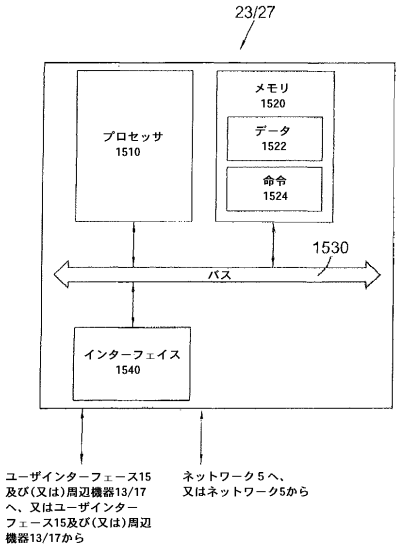
【図９】


901
ビットコイン社債利息
ビットコイン支払い
給料
貯金
銀行口座
当座預金口座
XYZ PIN
マスター鍵
パスワード
ABCウェブサイト

【図１０】


903
V1C
V2C
V2C'
V2C''
V3C
V3C'

【図１１】


23/27
プロセッサ
1510
メモリ
1520
データ
1522
命令
1524
1530
バス
インターフェイス
1540
ユーザインターフェース15及び(又は)周辺機器13/17へ、又はユーザインターフェース15及び(又は)周辺機器13/17から
ネットワーク5へ、又はネットワーク5から

フロントページの続き

(74)代理人 100070150
弁理士 伊東 忠彦
(74)代理人 100091214
弁理士 大貫 進介
(72)発明者 クレイグ ステヴァン ライト
英国、 ＣＦ１０ ２ＨＨ カーディフ、 チャーチル ウェイ、 チャーチル ハウス ７階、 アークハートーダイクス アンド ロード エルエルピー内
(72)発明者 ステファン サヴァナー
英国、 ＣＦ１０ ２ＨＨ カーディフ、 チャーチル ウェイ、 チャーチル ハウス ７階、 アークハートーダイクス アンド ロード エルエルピー内

審査官 中里 裕正

(56)参考文献 特表２０００－５０２５５３（ＪＰ，Ａ）
特表２００９－５２６４１１（ＪＰ，Ａ）
HAO, F., On Robust Key Agreement Based on Public Key Authenticaiton, Cryptology ePrint Archive, [online], ２０１０年 ３月, Report 2010/136, [2019年1月8日検索], ＵＲＬ, https://eprit.iacr.org/2010/136
McCORRY, P. et al, Authenticated Key Exchange over Bitcoin, Cryptology ePrint Archive, [online], ２０１５年 ９月, Report 2015/308, [2019年1月9日検索], ＵＲＬ, https://eprit.iacr.org/2015/308

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