(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7585315号
(P7585315)

(45)発行日　令和6年11月18日(2024.11.18)

(24)登録日　令和6年11月8日(2024.11.8)

(51)国際特許分類

Ｈ０４Ｌ　9/08　(2006.01)		Ｈ０４Ｌ	9/08	Ａ
Ｈ０４Ｌ　9/32　(2006.01)		Ｈ０４Ｌ	9/32	２００Ｚ

請求項の数　15　（全18頁）

(21)出願番号　特願2022-520338(P2022-520338)
(86)(22)出願日　令和2年10月6日(2020.10.6)
(65)公表番号　特表2023-500570(P2023-500570A)
(43)公表日　令和5年1月10日(2023.1.10)
(86)国際出願番号　PCT/EP2020/077977
(87)国際公開番号　WO2021/073953
(87)国際公開日　令和3年4月22日(2021.4.22)
審査請求日　令和5年8月17日(2023.8.17)
(31)優先権主張番号　19203273.8
(32)優先日　令和1年10月15日(2019.10.15)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)
(31)優先権主張番号　20151197.9
(32)優先日　令和2年1月10日(2020.1.10)
最終頁に続く

(73)特許権者　521393960
ブロックデーモン・アンパルツセルスケープ
Ｂｌｏｃｋｄａｅｍｏｎ ＡｐＳ
デンマーク８０００オーフス・セー、インゲ・レーマンス・ギャーゼ１０、６
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆
(74)代理人　100189544
弁理士　柏原 啓伸
(72)発明者　パグター，ヤコブ イレボー
デンマーク８２１０オーフス・ヴェー、フェンリスヴァイ７１
最終頁に続く

(54)【発明の名称】　コールドウォレットを用いたデジタルシグニチャ生成

(57)【特許請求の範囲】

【請求項１】

デジタルシグニチャを提供するための方法であって、

コールドウォレットの２つ以上のノード間で配布されるプライベートシグニチャキーを提供するステップであって、前記コールドウォレットの各ノードはそれによって前記プライベートシグニチャキーの１つ以上のシェアを所有し、前記コールドウォレットのどのノードも前記プライベートシグニチャキーの全てのシェアは所有しない、提供するステップと、

前記コールドウォレットの各ノードが、前記プライベートシグニチャキーのシェアに基づいてプレシグニチャを生成して、各プレシグニチャノードが前記コールドウォレットのノードのうちの１つのみから１つのプレシグニチャを受信する方法で、前記コールドウォレットの各ノードが、前記プレシグニチャを２つ以上のプレシグニチャノードのうちの１つに送信するステップと、

署名アプリケーションが、シグニチャを要求して、署名されるメッセージを前記プレシグニチャノードの各々に送信するステップと、

前記シグニチャの要求と前記署名されるメッセージとを受信することに応答して、前記プレシグニチャノードの各々が、そのプレシグニチャと前記署名されるメッセージとに基づいて、パーシャルシグニチャを生成するステップと、

前記プレシグニチャノードの各々が、そのパーシャルシグニチャを前記署名アプリケーションに送信するステップと、及び、

前記署名アプリケーションが、前記パーシャルシグニチャからデジタルシグニチャを計算するステップと
を含み、
前記コールドウォレットの各ノードが前記プレシグニチャを前記プレシグニチャノードの１つに送信するステップは、一方向通信チャネルを用いて実行される、
方法。
【請求項２】
前記パーシャルシグニチャを生成するステップの後、かつ、前記パーシャルシグニチャを送信するステップの前に、
前記プレシグニチャノードの各々が前記プレシグニチャを削除するステップを、更に含む、
請求項１に記載の方法。
【請求項３】
前記プライベートシグニチャキーを提供するステップは、前記コールドウォレットのノードがマルチパーティ計算プロトコルによって前記プライベートシグニチャキーを生成することによって実行される、
請求項１～２のうちのいずれか一に記載の方法。
【請求項４】
前記コールドウォレットの各ノードが、２つ以上のプレシグニチャを含むバッチの一部として前記プレシグニチャを生成する、
請求項１～３のうちのいずれか一に記載の方法。
【請求項５】
少なくとも、前記プライベートシグニチャキーを提供するステップと、前記プレシグニチャを生成して、前記プレシグニチャを前記プレシグニチャノードへ送信するステップとは、前記署名アプリケーションが前記シグニチャを要求するステップの前に、前処理のステップとして実行される、
請求項１～４のうちのいずれか一に記載の方法。
【請求項６】
前記コールドウォレットの各ノードが、前記プライベートシグニチャキーのシェアに基づいて前記プレシグニチャを生成して、前記プレシグニチャを前記２つ以上のプレシグニチャノードのうちの１つに送信するステップは、前記署名アプリケーションからの前記シグニチャの要求の受信に応答して前記プレシグニチャノードによって開始される、
請求項１～４のいずれか一に記載の方法。
【請求項７】
前記プレシグニチャノードの各々が前記パーシャルシグニチャを生成するステップは、
前記プレシグニチャノード間の内部通信無しで実行される、
請求項１～６のうちのいずれか一に記載の方法。
【請求項８】
前記署名アプリケーションからの前記シグニチャの要求を承認するステップを、更に含む、
請求項１～７のうちのいずれか一に記載の方法。
【請求項９】
前記コールドウォレットのノードが閾値条件ｔを満たし、前記プレシグニチャノードが閾値条件ｔ’を満たし、ここでｔ’≧ｔである、
請求項１～８のうちのいずれか一に記載の方法。
【請求項１０】
請求項１～９のうちのいずれか一に記載の方法であって、
前記コールドウォレットのノードの少なくともいくつかが、１つ以上の追加のプレシグニチャシェアを生成し、前記追加のプレシグニチャシェアを暗号化し、及び、前記暗号化された追加のプレシグニチャシェアを前記プレシグニチャとともに前記プレシグニチャノードの１つ以上に送信するステップと、並びに、

前記暗号化された追加のプレシグニチャシェアを受信した前記プレシグニチャノードの各々が、前記暗号化された追加のプレシグニチャシェアを前記パーシャルシグニチャとともに前記署名アプリケーションに送信するステップと
を、更に含み、
前記署名アプリケーションが前記デジタルシグニチャを計算するステップは、
前記署名アプリケーションが、受信した前記暗号化された追加のプレシグニチャシェアを復号化するステップと、
前記署名アプリケーションが、復号化された前記追加のプレシグニチャシェアに基づいて追加のプレシグニチャを生成し、及び、前記追加のプレシグニチャと、前記署名されるメッセージとに基づいて、追加のパーシャルシグニチャを生成するステップと、並びに、
前記署名アプリケーションが、前記プレシグニチャノードから受信した前記パーシャルシグニチャと、前記生成された追加のパーシャルシグニチャとから、前記デジタルシグニチャを計算するステップと、
を含む、
方法。
【請求項１１】
前記１つ以上の追加のプレシグニチャシェアを生成するステップは、
前記コールドウォレットのノードの各々が１つの追加のプレシグニチャシェアを生成して前記追加のプレシグニチャシェアを暗号化することによって、実行される、
請求項１０に記載の方法。
【請求項１２】
前記１つ以上の追加のプレシグニチャシェアを生成するステップは、
前記コールドウォレットのノードのうちの少なくとも２つがマルチパーティ計算プロトコルを適用することによって実行される、
請求項１０に記載の方法。
【請求項１３】
前記追加のプレシグニチャシェアは、前記コールドウォレットの夫々のノードと前記署名アプリケーションとの間でシェアされる対称暗号化キーによって暗号化及び復号化される、請求項１０～１２のいずれか一に記載の方法。
【請求項１４】
デジタルシグニチャを提供するシステムにおいて、
プライベートシグニチャキーがノード間で分散されている、２つ以上のノードを含むコールドウォレットであって、前記コールドウォレットの各ノードはこれにより前記プライベートシグニチャキーの１つ以上のシェアを所有し、前記コールドウォレットのどのノードも前記プライベートシグニチャキーの全てのシェアは所有せず、前記コールドウォレットのノードは、前記プライベートシグニチャキーのシェアに基づいてプレシグニチャを生成し、一方向通信チャネルを用いて該プレシグニチャをプレシグニチャノードに送信するように構成されている、コールドウォレットと、
二つ以上のプレシグニチャノードを含むプレシグニチャウォレットであって、前記プレシグニチャノードは、前記プレシグニチャノードの各々が前記コールドウォレットのノードの一つのみから１つのプレシグニチャを受信する方法で、前記コールドウォレットのノードからプレシグニチャを受信するように構成され、前記プレシグニチャノードは、そのプレシグニチャと署名されるメッセージとに基づいてパーシャルシグニチャを生成し、そのパーシャルシグニチャを署名アプリケーションに送信するように構成されている、プレシグニチャウォレットと、及び、
署名の要求及び署名されるメッセージを前記プレシグニチャノードに送信し、前記プレシグニチャノードから前記パーシャルシグニチャを受信し、前記パーシャルシグニチャからデジタルシグニチャを計算するように構成されている署名アプリケーションと
を含む、システム。
【請求項１５】

前記コールドウォレットへのデータ伝送が防止される、
請求項１４に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
発明の属する技術分野
本発明は、プライベートシグニチャキーを保持するコールドウォレットを用いて、デジタルシグニチャを生成する方法及びシステムに関するものである。
【背景技術】
【０００２】
発明の背景
デジタルシグニチャは、文書に署名する人または取引を実行する人が実際にそうする権限を有することを保証する方法で、文書の署名、取引の実行などのために広く使用されている。これは、例えば、暗号通貨に関連する取引を行う場合に関連している。悪意のある者がプライベートシグニチャキーにアクセスした場合、悪意のある者はプライベートシグニチャキーの正当な所有者の名前で署名及び取引を行うことができ、かかる取引は不可逆的なものとなる可能性がある。このような悪意のあるアクセスは、修復不可能な損害を与える可能性があるため、プライベートシグニチャキーは安全な状態で保管されることが不可欠である。
【０００３】
デジタルシグニチャを行う場合、通常、署名者の身元を証明するプライベートシグニチャキーが必要である。このようなプライベートシグニチャキーは、例えば、ユーザの個人所有のＰＣや、ポータブルメモリストレージやドングルなどの専用ハードウェアにローカルに保存することができる。代替案として、署名鍵の保存にハードウェアセキュリティモジュール（ＨＳＭ）を適用することもできる。この場合、署名はＰＣまたは専用ハードウェアからしか生成できないという欠点がある。さらに、システムのセキュリティは、プライベートシグニチャキーが格納されているハードウェアの盗難や不正アクセスを防止することに関してユーザがどれだけ注意するかなど、ユーザの行動によって制限される。
【０００４】
もう一つの可能性は、プライベートシグニチャキーを信頼できる鍵管理サービスに保管することである。これにより、ユーザは必ずしも特定のハードウェアにアクセスすることなく、プライベートシグニチャキーにアクセスすることができる。さらに、システムのセキュリティは信頼できる鍵管理サービスによって一元的に処理されるため、個々のユーザの行動にはあまり影響されない。しかし、システムのセキュリティは、正当な利用者が容易にアクセスできるようにする一方で、悪意のある者が署名鍵にアクセスするのを防ぐというバランスをとる必要がある。
【０００５】
高い安全性を確保するために、いわゆる「コールドウォレット」が適用されることがある。コールドウォレットとは、インターネットなどの通信ネットワークに接続されていない、プライベートシグニチャキーを保管・管理するためのシステムである。これは「エアギャップ」システムと呼ばれることもある。通信ネットワークからのアクセスは鍵管理システムに対する主要な攻撃ベクトルの１つと考えられているため、コールドウォレットは非常に高いセキュリティレベルを示している。しかし、通信ネットワークからのアクセスがないため、正当な利用者が自分のプライベートシグニチャキーにアクセスすることは困難である。さらに、コールドウォレットは単一障害点であり、悪意のある者がコールドウォレットを保持するハードウェアを危険にさらすことに成功した場合、その者はプライベートシグニチャキーに完全にアクセスすることができるのである。これは、プライベートシグニチャキーが異なる場所でシェアされ保管されている場合でも同様で、署名を生成するためにプライベートシグニチャキーを組み立てる必要があるからである。最後に、署名を実行するために、いくつかのデータがエアギャップ・システムに入る必要があり、それ

によってマルウェアがエアギャップ・システムに入り、プライベートシグニチャキーを危険にさらすというリスクが生じる。

【０００６】

https://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdfにて利用できるSteven Goldfederらによる"Securing Bitcoin wallets via threshold signatures"（２０１４年６月３日）（非特許文献１）は、ＢｉｔｃｏｉｎのＥＣＤＳＡ署名と互換性があり、ウォレットのシェア制御、安全な簿記、安全な権限委譲、個人ウォレットの２要素セキュリティなど複雑かつ有用なセキュリティポリシーを施行するのに使用可能な閾値署名スキームを開示している。有効な署名を構築する能力はｎ人のプレイヤーに分散され、各プレイヤーは秘密分散方式などによってプライベートシグニチャキーのシェアを受ける。署名にはｔ人以上の参加が必要であり、その人数はある固定値ｔ≦ｎである。鍵のシェアは、コールドウォレットに格納されてもよい。ＥＣＤＳＡ閾値署名プロトコルは、プライベートシグニチャキーを再構築することなく、並列制御で署名付きトランザクションを提供するために使用される。署名は鍵シェアから直接取得され、鍵シェアを持つプレイヤー間の通信を必要とするステップを経る。

【先行技術文献】

【非特許文献】

【０００７】

【文献】"Securing Bitcoin wallets via threshold signatures" https://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf

【発明の概要】

【０００８】

本発明の実施形態の目的は、正当なユーザが容易にアクセスできるようにしながら、高いレベルのセキュリティを得ることができる、デジタルシグニチャを提供するための方法を提供することである。

【０００９】

本発明の実施形態のさらなる目的は、デジタルシグニチャを提供するためのシステムを提供することであり、このシステムでは、正当なユーザが容易にアクセスできるようにしながら、高レベルのセキュリティを提供する。

【００１０】

第１の態様によれば、本発明は、デジタルシグニチャを提供するための方法を提供し、該方法は、以下のステップを含む。

コールドウォレットの２つ以上のノードに分配されるプライベートシグニチャキーを提供し、コールドウォレットの各ノードがプライベートシグニチャキーの１つ以上のシェアを所有し、コールドウォレットのどのノードもプライベートシグニチャキーのすべてのシェアは所有しない、提供するステップと、

コールドウォレットの各ノードが、プライベートシグニチャキーのシェアに基づいてプレシグニチャを生成し、プレシグニチャを２つ以上のプレシグニチャノードのうちの１つに送信し、各プレシグニチャノードは、コールドウォレットのノードのうちの１つからプレシグニチャを受信するような方法で、プレシグニチャを送信するステップと、

署名アプリケーションが、シグニチャを要求し、署名されるメッセージをプレシグニチャノードの各々に送信するステップと、

シグニチャの要求と署名されるメッセージを受信したことに応答して、各プレシグニチャノードは、そのプレシグニチャと署名されるメッセージに基づいて、パーシャルシグニチャを生成するステップと、

各プレシグニチャノードが、そのパーシャルシグニチャを署名アプリケーションに送信するステップと、

前記署名アプリケーションが、前記パーシャルシグニチャからデジタルシグニチャを計算するステップと

である。

【００１１】
このように、本発明の第１の態様による方法は、デジタルシグニチャを提供するための方法である。上述したように、このようなデジタルシグニチャは、文書に署名するため、または、例えばブロックチェーン技術に基づく暗号通貨取引などの取引を実行するために使用され得る。
【００１２】
最初に、プライベートシグニチャキーが提供される。プライベートシグニチャキーは、システムのセットアップ時に一度だけ提供されてもよく、プライベートシグニチャキーは、その後、複数の署名に適用されてもよく、すなわち、プライベートシグニチャキーを提供するステップを繰り返さずに、以下に説明するステップの一部または全部が繰り返されてもよい。
【００１３】
プライベートシグニチャキーは、コールドウォレットの２つ以上のノードの間で配布される。したがって、コールドウォレットのノードの各々は、プライベートシグニチャキーの少なくとも１つのシェアを所有しており、コールドウォレットのノードのいずれも、プライベートシグニチャキーのシェアのすべてを所有しておらず、それによって、ノードのいずれも単一障害点を構成しない。さらに、コールドウォレットのノードは通信ネットワークに接続されていないため、エアギャップ・システムを形成し、それに応じてプライベートシグニチャキーは非常に安全な条件下で保存される。ノードが特定の状況下で、例えばプライベートシグニチャキーを生成するために、限られた期間だけ互いに通信することを許可されることは否定しません。しかし、どのノードもコールドウォレットの外から通信を受けることはできない。
【００１４】
プライベートシグニチャキーのシェアは、マルチシグニチャセットアップの複数のプライベートキーとして機能してもよく、この場合、有効なシグニチャを提供するため、または取引を有効に承認するために、複数の別々のプライベートキーに基づく複数の有効なシグニチャが要求される。これにより、本発明による方法は、マルチシグニチャワークフローをエミュレートするために適用され得る。例えば、コールドウォレットのノードは別々のサーバーに配置されてもよく、そのサーバーは互いに物理的に離れていてもよい。
【００１５】
プライベートシグニチャキーが、ルート鍵と、ルート鍵から決定論的に導出された複数の階層鍵の形式であることは否定されない。これは、例えば、コールドウォレットが、他の暗号通貨のビットコインに関連して適用されることがある、いわゆるＨＤウォレットの形態である場合である可能性がある。この場合、複数の階層的な鍵は、例えば、ルート鍵が生成され、したがってノードが互いに通信する必要がある場合に導出されてもよく、各ノードは、ルート鍵の１つ以上のシェアと複数の導出された鍵シェアとを保持してもよい。鍵シェアはそれぞれインデックス番号を与えられてもよい。階層的なキーシェアは、例えば、ルート鍵からハッシュ（例えばＨＭＡＣ）を計算することによって導出されてもよい。このシナリオでは、ルート鍵はコールドウォレットに保持される。しかし、派生した鍵の層のいくつかは、コールドウォレットから出ることを許可され、それによって、ルート鍵のセキュリティを損なうことなく、よりアクセスしやすくすることができる。
【００１６】
次に、コールドウォレットの各ノードは、プライベートシグニチャキーのシェア（複数可）に基づいてプレシグニチャを生成する。各プレシグニチャはプライベートシグニチャキーのシェアの一部のみに基づいて生成されるので、どのプレシグニチャもプライベートシグニチャキー全体を表すことはない。したがって、プレシグニチャはプレシグニチャシェアとみなすことができ、コールドウォレットの各ノードはプレシグニチャシェアを保有することになる。プライベートシグニチャキーがルート鍵及び複数の決定論的派生階層鍵からなる種類のものである場合、コールドウォレットの各ノードは、派生鍵シェアのうちの1つに基づいてプレシグニチャを生成してもよい。

【００１７】
プレシグニチャの生成は、コールドウォレットのノード間で内部通信を行ってもよいし、行わなくてもよい。プレシグニチャの生成がコールドウォレットのノード間の内部通信を必要とする場合、プレシグニチャは、有利には、指定された時間、例えば、コールドウォレットのノード間の通信も必要とするプライベートシグニチャキーを提供するステップの直後に生成されてもよい。それによって、コールドウォレットのノード間の通信は最小限に抑えられ、明確に定義された時間間隔に制限され、それによって、プライベートシグニチャキーのシェアが漏れるリスクを最小限に抑えることができる。
【００１８】
本発明の方法がマルチシグニチャワークフローのエミュレーションに適用される場合、プライベートシグニチャキーのシェアを保有するノードのすべてがコールドウォレットの一部を形成する必要はなく、ノードの少なくともいくつかが、閉鎖またはエアギャップ環境の外で通信することが許可され得るという意味において、コールドウォレットの一部を形成する必要はない。
【００１９】
さらに、コールドウォレットの各ノードは、生成されたプレシグニチャを２つ以上のプレシグニチャノードのうちの１つに送信し、各プレシグニチャノードは、コールドウォレットのノードのうちの１つのみからプレシグニチャを受信するような態様で、プレシグニチャを送信する。したがって、コールドウォレットのノードとプレシグニチャノードとの間には１対１の関係があり、プレシグニチャノードのいずれも、組み合わせるとプライベートシグニチャキー全体を代表するプレシグニチャを所持していない。その結果、どのプレシグニチャノードも単一障害点とはならない。さらに、プレシグニチャは、プライベートシグニチャキーの全部または一部を明らかにすることなく、コールドウォレットからエクスポートされる。プレシグニチャを生成し送信するステップは、署名されるメッセージを知らなくても実行可能であり、したがって、コールドウォレットにメッセージを送信する必要はないことに留意されたい。
【００２０】
次に、署名アプリケーションは、シグニチャを要求し、署名されるメッセージをプレシグニチャノードの各々に送信する。これに応答して、各プレシグニチャノードは、そのプレシグニチャと署名対象のメッセージとに基づいて、パーシャルシグニチャを生成する。パーシャルシグニチャは、それぞれのプレシグニチャノードによって、それぞれのノードが所有しているプレシグニチャに基づいて生成されるので、どのパーシャルシグニチャもプライベートシグニチャキー全体を代表するものではなく、したがって、どのパーシャルシグニチャもメッセージの完全な署名を形成することはできない。しかし、パーシャルシグニチャの組み合わせから完全な署名を形成することができる。
【００２１】
したがって、プレシグニチャノードの各々は、そのパーシャルシグニチャを署名アプリケーションに送信する。これにより、署名アプリケーションは、すべてのパーシャルシグニチャを所有することになり、完全な署名を形成することができる。したがって、署名アプリケーションは、最終的にパーシャルシグニチャからデジタルシグニチャを計算する。コールドウォレットにデータが入らないように、またコールドウォレットからプライベートシグニチャキーのシェアが出ないように、プレシグニチャがコールドウォレット内で生成されることは、プライベートシグニチャキーに関するあらゆる情報の漏洩リスクを劇的に低減するため、利点である。
【００２２】
さらに、プレシグニチャは、ユーザにとってアクセスしやすいコールドウォレットの外側にあるプレシグニチャノードに送信されるので、正規ユーザにとって非常に使い勝手の良いシステムである。
【００２３】
このように、本発明の第１の態様に係る方法においては、コールドウォレットは、全プ

ロセスの間、エアギャップされたままである。それにより、コールドウォレットにマルウェアが導入されるリスク、及びプライベートシグニチャキーが漏洩するリスクは、最小限に抑えられる。しかしながら、プレシグニチャはプレシグニチャノードによって保持されるので、これらは実際の署名プロセス中にプライベートシグニチャキーよりも著しくアクセス可能であり、それによって正当なユーザが署名に容易にアクセスできるようになる。したがって、本発明の第１の態様による方法は、プライベートシグニチャキーのシェアがコールドウォレットのノードによって保持されることに起因して、高いレベルのセキュリティを提供する一方で、プレシグニチャがプレシグニチャノードによって保持されることに起因して、正当なユーザにとって容易なアクセスを可能にする。

【００２４】

本方法は、パーシャルシグニチャを生成するステップの後、パーシャルシグニチャを送信するステップの前に、プレシグニチャノードの各々がプレシグニチャを削除するステップをさらに備えてもよい。本実施形態によれば、プレシグニチャは、パーシャルシグニチャを生成するために適用されるとすぐに、プレシグニチャノードから削除される。それにより、所定のプレシグニチャが２つ以上のパーシャルシグニチャの生成のために適用されることが防止される。これは、１つのプレシグニチャに由来する複数のパーシャルシグニチャがプライベートシグニチャキーの機密性を損なう可能性があるため、利点である。パーシャルシグニチャが署名アプリケーションに送信される前にプレシグニチャを削除することにより、署名アプリケーションにアクセスした悪意のある者が、同じプレシグニチャに基づく第２のパーシャルシグニチャを要求することをさらに防止することができる。これは、楕円曲線デジタルシグニチャアルゴリズム（ＥＣＤＳＡ）が適用される場合に特に関連する。

【００２５】

コールドウォレットの各ノードがプレシグニチャをプレシグニチャノードの１つに送信するステップは、一方向通信チャネルを使用して実行されてもよい。本実施形態によれば、コールドウォレットから情報のみを出すことができ、コールドウォレットにデータを入れないことが効率的に確保される。したがって、プライベートシグニチャキーと署名されるメッセージとが同じ位置に配置されることはない。これにより、マルウェアがメッセージとともにコールドウォレットに入り込み、それによってプライベートシグニチャキーが危険にさらされる危険性をかなり低減することができる。

【００２６】

一方向通信チャネルは、例えば、プレシグニチャノードによってスキャンすることができる二次元コードなどの視覚的出力の形態であり得る。代替的または追加的に、一方向通信チャネルは、一方向通信のみを可能にするネットワーク機器および／または接続を含むことができる。

【００２７】

プライベートシグニチャキーを提供するステップは、コールドウォレットのノードがマルチパーティ計算プロトコルによってプライベートシグニチャキーを生成することによって実行されてもよい。マルチパーティ計算プロトコルは、例えば、暗号化プロトコルであってもよい。本実施形態によれば、コールドウォレットのノードは、プライベートシグニチャキー全体が決して集合しないような方法で、かつ、プライベートシグニチャキーのシェアのいずれもコールドウォレットから出ないような方法で、プライベートシグニチャキーの生成に協力する。

【００２８】

コールドウォレットの各ノードは、２つ以上のプレシグニチャからなるバッチの一部として、プレシグニチャを生成してもよい。この実施形態によれば、複数のプレシグニチャが、例えば、プライベートシグニチャキーの生成時に最初に生成され、プレシグニチャは、署名が要求されたときに、１つずつ使用される。例えば、プレシグニチャの生成は、コールドウォレットのノードの少なくとも一部の間で通信を必要とする場合がある。これは、例えば、上述のプライベートシグニチャキーの生成と同様に、マルチパーティ計算プロ

トコルの適用を含み得る。プライベートシグニチャキーの危殆化のリスクを最小化するために、コールドウォレットのノード間の通信を短時間で頻繁でない時間間隔に制限することが望ましい場合がある。多数のプレシグニチャがバッチとして生成される場合、コールドウォレットのノードは、次にプレシグニチャが必要となったときに互いに通信する必要がない。それにより、システムのセキュリティが向上する。

【００２９】

プレシグニチャは、さらに、プレシグニチャのバッチとしてそれぞれのプレシグニチャノードに送信されてもよい。代替案として、プレシグニチャのバッチは、コールドウォレットのそれぞれのノードで保存され、プレシグニチャは、署名が要求されるたびに、それぞれのプレシグニチャノードに一度に１つずつ送信されてもよい。

【００３０】

少なくとも、プライベートシグニチャキーを提供するステップ、プレシグニチャを生成するステップ、及びプレシグニチャをプレシグニチャノードに送信するステップは、署名アプリケーションがシグニチャを要求するステップの前に、前処理ステップとして実行されてもよい。

【００３１】

プライベートシグニチャキーの提供、プレシグニチャの生成、およびプレシグニチャノードへのプレシグニチャの送信のステップは、署名されるメッセージの知識がなくても実行可能である。したがって、これらのステップは、有利には、シグニチャが要求される前に、前処理ステップとして実行され、場合によってはシステムの負荷が低い時間に実行されることがある。これにより、実際にシグニチャが要求されたときのシステムの待ち時間を短縮することができる。さらに、シグニチャが要求され生成される時点では、コールドウォレットのノードとプレシグニチャのノードとの間の通信が必要ないため、署名プロセス中に通信障害が発生するリスクが低減され、システムの信頼性が向上している。最後に、これは、実際の署名プロセスの間、コールドウォレットがエアギャップされたままであることを保証し、それによって、システムに対する悪意のある攻撃が成功するリスクをかなり減少させる。

【００３２】

代替案として、コールドウォレットの各ノードが、プライベートシグニチャキーのシェアに基づいてプレシグニチャを生成し、プレシグニチャを２つ以上のプレシグニチャノードのうちの１つに送信するステップは、署名アプリケーションからの署名要求の受信に応答してプレシグニチャノードによって開始され得る。この実施形態によれば、プレシグニチャは、実際に署名が要求されるまで生成されない。その代わり、署名アプリケーションが署名を要求し、署名するメッセージをプレシグニチャノードに送信することによって、プロセスが開始される。これに応答して、プレシグニチャノードはコールドウォレットの各ノードからプレシグニチャを要求し、コールドウォレットはプレシグニチャを生成してプレシグニチャノードに送信する。

【００３３】

なお、各プレシグニチャノードがパーシャルシグニチャを生成するステップは、プレシグニチャノード間で内部通信を行わずに実行してもよい。本実施形態によれば、プレシグニチャノードがコールドウォレットのノードからそれぞれのプレシグニチャを受信すると、各プレシグニチャノードは、他のプレシグニチャノードと通信を行わずに、そのパーシャルシグニチャを生成することができる。これにより、実際の署名が生成されるときに必要な通信が最小限に抑えられ、それによって待ち時間が減少し、システムの安全性と信頼性が向上する。この実施形態は、上述したように、方法ステップの一部が前処理ステップとして実行される実施形態と組み合わせて特に関連性がある。

【００３４】

本方法は、署名アプリケーションからの署名の要求を承認するステップをさらに含んでもよい。この実施形態によれば、署名の要求が認可されたユーザから発信されていることが確認できる場合にのみ、署名プロセスが開始される。承認は、例えば、パスワードの入

力又は他の任意の適切な識別方法を含んでもよい。

【００３５】

コールドウォレットのノードは、閾値条件tを満たしてよく、プレシグニチャノードは、閾値条件t'を満たしてよく、ここで、t'はt以上である。

【００３６】

マルチパーティデジタルシグニチャを行うシステムは、しばしば（t,n）を満たすように設計されており、ここでnはノードの数であり、tは閾値である。閾値tは、署名プロセスを完了させる一方で、悪意のあるパーティや非参加パーティをどれだけ許容できるかを指定する。一般に、有効な署名は任意のt+1個の正直なノードによって生成されることができる。

【００３７】

例えば、t＝n／2、n＝3の場合、任意の２つのノードによって有効な署名が生成され、最大1つの悪意のあるノードまたは不参加のノードが許容される。

【００３８】

本実施形態によれば、コールドウォレットのノードは、閾値条件tを満たすので、コールドウォレットの任意のt＋1個のノードは、プライベートシグニチャキーを計算することができる。さらに、プレシグニチャのノードは、閾値条件、t'を満たす。したがって、有効な署名は、プレシグニチャノードのうち任意のt'+1から発信されるプレシグニチャから計算することができる。t'≧tなので、必要な参加ノードおよび誠実なプレシグニチャノードの数は、コールドウォレットの必要な誠実な参加ノードの数と少なくとも同じ大きさである。一実施形態によれば、t'＝2tである。したがって、コールドウォレットと比較してより高いアクセス性によって引き起こされるプレシグニチャノードのより低いセキュリティレベルは、より厳しい閾値条件を課すことによって補償される。

【００３９】

本方法は、更に、

コールドウォレットのノードの少なくともいくつかが、１つ以上の追加のプレシグニチャシェアを生成し、追加のプレシグニチャシェアを暗号化し、暗号化された追加のプレシグニチャシェアをプレシグニチャとともにプレシグニチャノードの１つ以上に送信するステップと、及び、

暗号化された追加のプレシグニチャシェアを受信した各プレシグニチャノードが、暗号化された追加のプレシグニチャシェアをパーシャルシグニチャとともに署名アプリケーションに送信するステップと

を含んでもよく、

および、署名アプリケーションがデジタルシグニチャを計算するステップは、

署名アプリケーションが、受信した暗号化された追加のプレシグニチャシェアを復号化するステップと、

署名アプリケーションが、復号化された追加のプレシグニチャシェアに基づいて追加のプレシグニチャを生成し、追加のプレシグニチャおよび署名されるメッセージに基づいて追加のパーシャルシグニチャを生成するステップと、及び、

署名アプリケーションが、プレシグニチャノードから受信したパーシャルシグニチャと、生成された追加パーシャルシグニチャとからデジタルシグニチャを計算するステップとを含んでもよい。

【００４０】

本実施形態によれば、署名アプリケーションは、プレシグニチャノードとともに、署名プロセスにおける追加のパーティとして機能する。したがって、n個のプレシグニチャノードから発信されるn個のパーシャルシグニチャの代わりに、n＋1個のパーシャルシグニチャが存在し、（n＋1）番目のパーシャルシグニチャは、n個のプレシグニチャノードによって提供される１つ以上の追加のプレシグニチャシェアを使用して、署名アプリケーションによって生成される。

【００４１】

署名プロセスにこのような追加のパーティを導入することにより、コールドウォレットの外で行われるプロセスの部分のセキュリティが改善される。例えば、コールドウォレット内で行われる署名プロセスの部分は、（t，n）閾値条件を満たすことができ、一方、コールドウォレットの外側で行われる署名プロセスの部分、例えば、プレシグニチャノード及び署名アプリケーションで行われる署名プロセスの部分は、（t＋1，n＋1）閾値条件を満たすことができる。

【００４２】

さらに、署名アプリケーションが署名プロセスの最終部分にのみ関与することは、署名アプリケーションとシステムの他のパーティとの間の必要な相互作用の数を最小化し、それによって署名プロセス中の待ち時間を最小化するため、利点である。

【００４３】

この実施形態によれば、署名プロセスは、以下の方法で実行されてもよい。コールドウォレットのノードがプレシグニチャを生成するとき、そのノード間でも１つまたは複数の追加のプレシグニチャシェアを生成し、それらの組み合わせで追加のプレシグニチャを形成する。追加のプレシグニチャシェアは暗号化され、暗号化された追加のプレシグニチャシェアはプレシグニチャとともにそれぞれのプレシグニチャノードに送信される。追加のプレシグニチャシェアは、コールドウォレットのそれぞれのノードによって、コールドウォレットの他のノードから独立して生成されてもよく、またはコールドウォレットのノードの２つ以上が追加のプレシグニチャシェアの生成に協力してもよい。これについては、以下でさらに詳細に説明する。

【００４４】

署名の要求を受信することに応答して、各プレシグニチャノードは、パーシャルシグニチャを生成し、上述したように、署名アプリケーションにパーシャルシグニチャを送信する。コールドウォレットのノードの１つから暗号化された追加のプレシグニチャシェアを受信したプレシグニチャノードは、受信した暗号化されたプレシグニチャシェアを、そのプレシグニチャとともに、署名アプリケーションにさらに送信する。このように、署名アプリケーションは、プレシグニチャノードからパーシャルシグニチャと１つ以上の暗号化された追加のプレシグニチャシェアを受信する。

【００４５】

署名アプリケーションは、受信した暗号化された追加のプレシグニチャのシェアを復号化し、復号化されたシェアから追加のプレシグニチャを生成する。署名アプリケーションは、プレシグニチャノードがパーシャルシグニチャを生成した方法と同様の方法で、追加のプレシグニチャと署名されるメッセージに基づいて、追加のパーシャルシグニチャを生成する。最後に、署名アプリケーションは、プレシグニチャノードから受信したパーシャルシグニチャと追加のパーシャルシグニチャからデジタルシグニチャを計算する。このように、署名アプリケーションは、プレシグニチャノードと同様に動作する追加のパーティとして、署名プロセスに参加する。

【００４６】

１つ以上の追加のプレシグニチャシェアを生成するステップは、コールドウォレットの各ノードが追加のプレシグニチャシェアを生成し、追加のプレシグニチャシェアを暗号化することによって実行されてもよい。

【００４７】

この実施形態によれば、プレシグニチャシェアは、コールドウォレットの他のノードから独立して、コールドウォレットのそれぞれのノードによって生成される。それによって、コールドウォレットのノードのいずれも、コールドウォレットの他のノードによって生成された追加のプレシグニチャシェアに関するいかなる知識も得ることはない。同様に、プレシグニチャノードのいずれも、他のプレシグニチャノードによって受信される暗号化された追加のプレシグニチャシェアに関するいかなる知識も得ることはない。

【００４８】

本実施形態によれば、署名プロセスは、例えば、以下の方法で実行され得る。コールド

ウォレットがn個のノードからなり、コールドウォレットの各ノードが、例えば標準的なSchnorrシグニチャスキームにおいて、プライベートシグニチャキー、［x］のシェア、x_i、及び、ランダムなシェア値のシェア、［k］のシェア、k_iを保持すると仮定する。そして、公開検証鍵は、$y=g^x$であり、gは環状群の生成子である。メッセージmの署名は、(r,s)であり、ここで $r=H(m||R)$及び$s=k+rx$であり、Rはg^k及びHは適用される署名アルゴリズムで指定される関数である。コールドウォレットの各ノードは、$y=g^x$、$R=g^k$、及び暗号化キー、例えば対称暗号化キー、d_iを保持しているとさらに仮定することができる。

【００４９】

そして、コールドウォレットの各ノードは、乱数a_i及びb_iを選び、$k'_i=k_i-a_i$及び$x'_i=x_i-b_i$を計算することができる。さらに、コールドウォレットの各ノードは、$D_i=E_{di}(a_i||b||R||y)$を計算し得、ここでEは、暗号化キーを使用する認証された暗号化を表す。コールドウォレットの所定のノードから対応するプレシグニチャノードに送信されるメッセージは、$M_i=(k'_i, x'_i, R, D_i)$であり、k'_i，x'_i及びRはプレシグニチャを形成し、D_iは暗号化された追加のプレシグニチャシェアを形成している。

【００５０】

署名アプリケーションは、署名を要求し、署名すべきメッセージmを各プレシグニチャノードに送信する。これに応答して、各プレシグニチャノードは、コールドウォレットのノードから受信したメッセージM_iと、署名対象のメッセージmとに基づいて、$partial_i=k'_i+H(m||R)\cdot x_i$として、パーシャルシグニチャを生成する。各プレシグニチャのノードは、メッセージ$N_i=(partial_i,D_i)$を署名アプリケーションに送信する。

【００５１】

署名アプリケーションは、暗号化されたプレシグニチャシェアD_iの各々を復号化することができる復号化キーを保持する。対称暗号が適用されている場合、復号化キーは暗号化キーd_iと同一である。したがって、メッセージN_iを受信すると、署名アプリケーションは、暗号化された追加のプレシグニチャシェアD_iを復号し、$k'_{n+1}=a_1+a_2+...+a_n$と$x'_{n+1}=b_1+b_2+...+b_n$を計算して追加のプレシグニチャを発生させる。署名アプリケーションはさらに、$partial_{n+1}=k'_{n+1}+H(m||R)\cdot x_{n+1}$として、すなわちプレシグニチャノードがそれぞれのパーシャルシグニチャを生成したのと同じ方法で、追加のパーシャルシグニチャを生成する。

【００５２】

最後に、署名アプリケーションはデジタルシグニチャ(r,s)を計算するが、ここで、$r=H(m||R)$であり、sはパーシャルシグニチャの合計、すなわち、$s=partial_1+partial_2+\cdots+partial_{n+1}$である。さらに、署名アプリケーションは、受け取ったRの値がすべて同一であることを チェックし得る。そうでない場合、署名は不正であり、例えば悪意のある、または不正なパーティによるものである。結果として、署名アプリケーションは、受信したRの値が同一でない場合、署名プロセスを中断することを選択することができる。

【００５３】

代替案として、１つ以上の追加のプレシグニチャシェアを生成するステップは、上述の実施形態と同様の方法で実行されてもよいが、コールドウォレットのノードの一部のみが参加している状態で実行されてもよい。この場合、（ｎ＋１）番目のプレシグニチャを生成するために、ｎ未満の追加のプレシグニチャシェアが必要とされる。

【００５４】

別の代替案として、１つ以上の追加のプレシグニチャシェアを生成するステップは、マルチパーティ計算プロトコルを適用するコールドウォレットのノードのうちの少なくとも２つによって実行されてもよい。

【００５５】

この実施形態によれば、１つ以上の追加のプレシグニチャシェアは、コールドウォレットのノードの２つ以上によって協力して生成される。コールドウォレットのノードの全てがこのプロセスに参加してもよく、コールドウォレットのノードの一部のみが参加してもよい。

【００５６】
例えば、コールドウォレットのノードは、マルチパーティ計算プロトコルによって、２つ以上の追加のプレシグニチャシェアを生成し、これらをコールドウォレットの２つ以上のノードの間で分配してもよい。これは、例えば、上述したマルチパーティ計算プロトコルによる分散型プライベートシグニチャキーの生成と同様であってもよい。追加のプレシグニチャシェアの暗号化は、例えば、分散されたシェアが暗号化されたシェアとみなされるという意味で、マルチパーティ計算プロトコルの統合された部分であってよい。
【００５７】
代替案として、マルチパーティ計算プロトコルは、追加のプレシグニチャ全体の暗号化バージョンを構成する、単一の暗号化された追加のプレシグニチャシェアの生成をもたらし得る。この暗号化された追加のプレシグニチャシェアは、その後、コールドウォレットのノードの１つまたは複数によってプレシグニチャノードの１つまたは複数に送信され得る。この場合、署名アプリケーションが追加のプレシグニチャシェアを復号化すると、追加のプレシグニチャシェアも生成されたことになる。
【００５８】
上記のように、追加のプレシグニチャシェアは、コールドウォレットのそれぞれのノードと署名アプリケーションとの間でシェアされる対称暗号化キーによって暗号化および復号化されてもよい。この場合、コールドウォレットの各ノードは、署名アプリケーションと対称暗号鍵をシェアし、この鍵は、追加のプレシグニチャシェアを暗号化するためだけでなく、追加のプレシグニチャシェアを復号化するために適用される。代替案として、別の暗号化スキーム、例えば、公開鍵基盤（ＰＫＩ）スキームなどの非対称暗号化鍵を適用してもよい。
【００５９】
第２の態様によれば、本発明は、デジタルシグニチャを提供するためのシステムを提供し、このシステムは、以下を備える。
ノード間で分散されたプライベートシグニチャキーを有する２つ以上のノードを含むコールドウォレットであって、コールドウォレットの各ノードはそれによってプライベートシグニチャキーの１つ以上のシェアを所有し、コールドウォレットのどのノードもプライベートシグニチャキーの全てのシェアは所有せず、コールドウォレットのノードは、プライベートシグニチャキーのシェアに基づいてプレシグニチャを生成し、プレシグニチャノードにプレシグニチャを転送するよう構成された、コールドウォレットと、
２つ以上のプレシグニチャノードを含むプレシグニチャウォレットであって、各プレシグニチャノードがコールドウォレットのノードのうちの１つのみからプレシグニチャを受信し、そのプレシグニチャと署名されるメッセージとに基づいてパーシャルシグニチャを生成し、そのパーシャルシグニチャを署名アプリケーションに送信する、というようにして、コールドウォレットのノードからプレシグニチャを受信するように構成されたプレシグニチャノード、及び、
署名の要求および署名されるメッセージをプレシグニチャノードに送信し、プレシグニチャノードからパーシャルシグニチャを受信し、パーシャルシグニチャからデジタルシグニチャを計算するように構成される署名アプリケーションと
である。
【００６０】
本発明の第２の態様によるシステムは、本発明の第１の態様による方法を実行するために使用されてもよく、したがって、上に述べた備考は、ここでも同様に適用可能である。
【００６１】
したがって、本発明の第２の態様によるシステムは、コールドウォレットと、プレシグニチャウォレットと、署名アプリケーションとから構成される。
【００６２】
コールドウォレットは、本発明の第１の態様を参照して上述した方法でそれらの間で分散されたプライベートシグニチャキーを有する２つ以上のノードから構成される。コール

ドウォレットのノードは、さらに、プレシグニチャを生成し、これを、本発明の第１の態様を参照して上述した方法でプレシグニチャノードに送信するように構成される。コールドウォレットはエアギャップされており、すなわち、コールドウォレットのノードは、プライベートシグニチャキーが生成されるとき、ノードが互いに通信することのみが許可され、プレシグニチャが出力されるとき、この場合、ノードは情報を送信することはできるが、情報を受信することはできない以外はオフラインになる。

【００６３】

プレシグニチャウォレットは、２つ以上のプレシグニチャノードからなり、各ノードは、本発明の第１の態様を参照して上述した方法でプレシグニチャを受信するように構成される。プレシグニチャノードは、さらに、パーシャルシグニチャを生成し、これらを、本発明の第１の態様を参照して上述した方法で、署名アプリケーションに送信するように構成される。

【００６４】

署名アプリケーションは、本発明の第１の態様を参照して上述した方法で、署名の要求および署名されるメッセージをプレシグニチャノードに送信し、プレシグニチャノードからパーシャルシグニチャを受信し、デジタルシグニチャを計算するように構成されている。

【００６５】

コールドウォレットへのデータ送信は、防止されてもよい。この場合、データは、プレシグニチャノードに送信されるプレシグニチャの形で、コールドウォレットを離れることのみが許可される。しかし、署名されるメッセージはコールドウォレットに入ることはなく、プライベートシグニチャキーのシェアはコールドウォレットを離れることはない。これにより、プライベートシグニチャキーと署名されるメッセージが同じ位置に配置されることがないことが効率的に保証される。

【図面の簡単な説明】

【００６６】

次に、添付の図面を参照して、本発明をさらに詳細に説明する。

【００６７】

【図１】図１は、本発明の一実施形態によるシステムの斜視図である。

【図２】図２は、本発明の一実施形態による方法を示すフローチャートである。

【発明を実施するための形態】

【００６８】

図面の詳細な説明

【００６９】

図１は、本発明の一実施形態に係るシステム１の斜視図である。システム１は、コールドウォレット２と、プレシグニチャウォレット３と、署名アプリケーション４とから構成される。

【００７０】

コールドウォレット２は、多数のノード５から構成される。例示の目的のために、３つのノード５が示されている。しかしながら、コールドウォレット２が２つのノード５からなること、又はコールドウォレット２が４つ以上のノード５からなることを否定するものではないことに留意されたい。コールドウォレット２は、コールドウォレット２のノード５が本質的にオフラインであり、それによって悪意のあるパーティによってアクセスを得ることが困難であるという意味で、エアギャップされている。

【００７１】

プレシグニチャウォレット３は、多数のプレシグニチャノード６から構成される。例示の目的で、３つのプレシグニチャノード６が示されているが、プレシグニチャウォレット３が２つのプレシグニチャノード６から構成され得ること、又はプレシグニチャウォレット３が４つ以上のプレシグニチャノード６から構成され得ることは否定されない。しかしながら、コールドウォレット２のノード５の数とプレシグニチャノード６の数は同一であることが好ましい。プレシグニチャウォレット３は、プレシグニチャウォレット３との間

の限定された通信が許可されるという意味で、「ぬるま湯」と考えることができる。それにより、プレシグニチャウォレット３のセキュリティレベルは、コールドウォレット２のセキュリティレベルよりも低くなる。しかしながら、プレシグニチャウォレット３は、許可されたユーザにとってアクセスしやすく、したがって、コールドウォレット２よりもユーザフレンドリである。

【００７２】

図１のシステム１は、以下のように動作してもよい。初めに、コールドウォレット２のノード５によって、マルチパーティ暗号プロトコルを使用して、プライベートシグニチャキーが生成される。それにより、プライベートシグニチャキーは、各ノード５がプライベートシグニチャキーの１つ以上のシェアを所有し、どのノード５もプライベートシグニチャキーのシェアの全てを所有しないように、コールドウォレット２のノード５間で分配される。従って、プライベートシグニチャキーが１つの位置に集められることはなく、いずれのノード５もプライベートシグニチャキーに関する単一障害点を構成することはない。図１に示す実施形態では、プライベートシグニチャキーのシェアは３つであり、ノード５の各々は、そのうちの１つのシェアを所持している。コールドウォレット２のノード５は、プライベートシグニチャキーを生成している間は、互いに通信することができるが、それ以外は互いに隔離されている。それにより、プライベートシグニチャキーが後の時点で組み立てられることが防止される。コールドウォレット２のノード５は、コールドウォレット２の外部のいかなるエンティティからも、いつでもデータを受信することが防止される。

【００７３】

プライベートシグニチャキーのシェアは、マルチシグニチャセットの複数のプライベートキーの別々のプライベートキーとして機能してもよく、それによって、システム１は、上述したように、マルチシグニチャワークフローをエミュレートすることができる。

【００７４】

次に、コールドウォレット２のノード５の各々は、プライベートシグニチャキーのシェアに基づいて、プレシグニチャを生成する。コールドウォレット２の所定のノード５によって生成されたプレシグニチャは、それによって、そのノード５によって保持されるプライベートシグニチャキーのシェアについて代表されるが、コールドウォレット２の他の２つのノード５によって保持されるプライベートシグニチャキーのシェアについては、代表されない。プレシグニチャは、プレシグニチャのバッチの一部として生成されてもよいし、一度に１つずつ生成されてもよい。コールドウォレット２のノード５は、プレシグニチャの生成中に互いに通信することを許可されてもよい。

【００７５】

コールドウォレット２の各ノード５は、さらに、対応するプレシグニチャノード６にプレシグニチャを送信する。このように、各プレシグニチャノード６は、コールドウォレット２のノード５のうちの１つ、及び１つのみからプレシグニチャを受信する。したがって、プレシグニチャノード６のいずれも、プライベートシグニチャキー全体を代表するプレシグニチャを受信せず、それによって、プレシグニチャノード６のいずれも、それ自体で有効な署名を計算することができなくなる。しかし、プレシグニチャノード６が組み合わせると、有効な署名を計算することができるプレシグニチャを保有していることになる。コールドウォレット２のノード５からプレシグニチャノード６へのプレシグニチャの送信は、一方通行の通信路を用いて行われる。例えば、コールドウォレット２のノード５は、例えばカメラ又は適切なスキャナによって、関連するプレシグニチャノード６によって読み取ることができる二次元バーコードなどの視覚的又は機械可読コードを生成してもよい。それによって、コールドウォレット２にデータが入らないことが効率的に保証される。

【００７６】

これまで説明したステップは、署名されるメッセージに関する知識を必要とせず、したがって、これらは前処理ステップとして実行され得る。これにより、実際に署名が生成される時点で必要となるステップ数、特に通信ステップ数を削減することができる。これに

より、システム１のレイテンシが減少し、通信障害またはタイムアウトによる署名プロセスの失敗のリスクが減少する。

【００７７】

署名が必要な場合、認可されたユーザは署名アプリケーション４に連絡し、署名されるメッセージを提供する。次に、署名アプリケーション４は、署名を要求することによってプレシグニチャノード６に連絡し、署名すべきメッセージをプレシグニチャノード６の各々に送信する。これに応答して、プレシグニチャノード６の各々は、そのプレシグニチャに基づき、署名アプリケーション４から受信したメッセージに基づいて、パーシャルシグニチャを生成する。したがって、パーシャルシグニチャのいずれも有効な署名全体を構成しないが、３つのパーシャルシグニチャを組み合わせることで、メッセージの有効な署名を計算するのに十分な情報を含む。さらに、パーシャルシグニチャは、署名されるメッセージに基づき、また、プライベートシグニチャキーに基づき、プレシグニチャがプライベートシグニチャキーのそれぞれのシェアに基づき生成される形態で、生成される。ただし、パーシャルシグニチャは、署名すべきメッセージがコールドウォレット２に入ることを必要とせず、また、プライベートシグニチャキーのシェアのいずれかがコールドウォレット２から出ることを必要とせず、生成される。さらに、パーシャルシグニチャは、プレシグニチャノード６が互いに通信することを要求することなく生成されてもよい。上述したように、これにより、システム１のレイテンシを低減し、システム１が侵害されるリスクを最小化することができる。システム１がマルチシグニチャワークフローのエミュレーションに適用される場合、これはさらに、シグニチャプロセスを標準的なマルチシグニチャワークフローに非常によく似た方法で実行することを可能にし、すなわち、ユーザが従うのに慣れているワークフローを変更する必要がないことを意味している。例えば、全てのパーティがオンラインであることや、パーシャルシグニチャを同時に生成することは要求されない。

【００７８】

プレシグニチャノード６は、さらに、生成されたパーシャルシグニチャを署名アプリケーション４に送信し、署名アプリケーション４は、次に、パーシャルシグニチャからメッセージのデジタルシグニチャを計算する。以上のように、図１に示すシステム１では、コールドウォレット２とプレシグニチャウォレット３とが分離されているため、正当なユーザが容易にアクセスできる一方で、高いセキュリティが実現される。

【００７９】

図２は、本発明の一実施形態による方法を示すフローチャートである。処理は、ステップ７で開始される。ステップ８で、プライベートシグニチャキーが、コールドウォレットの２つ以上のノードによって、例えば上述した方法で、マルチパーティ暗号計算プロトコルを使用して生成される。従って、プライベートシグニチャキーは、コールドウォレットのノード間で配布される。

【００８０】

ステップ９において、コールドウォレットの各ノードは、プライベートシグニチャキーのシェアに基づいてプレシグニチャを生成し、上記の方法で、プレシグニチャをプレシグニチャノードに送信する。

【００８１】

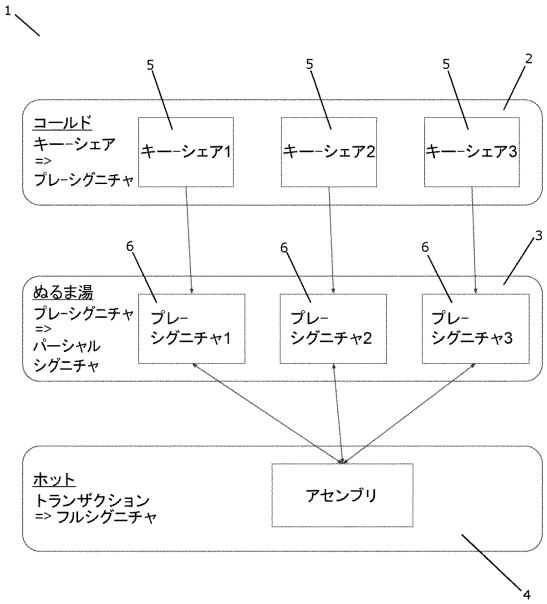
ステップ１０では、署名アプリケーションから署名が要求されたかどうかが調査される。そうでない場合はそれ以上何もせず、一定の時間間隔で繰り返し署名の要求があったかどうかが調べられる。署名が要求され、署名アプリケーションによって署名すべきメッセージがプレシグニチャノードに送信されると、処理はステップ１１に進められ、各プレシグニチャノードは、そのプレシグニチャと、署名されるメッセージとに基づいて、パーシャルシグニチャを生成する。パーシャルシグニチャが生成されると、将来の別の署名に再利用されないようにするため、それぞれのプレシグニチャノードによってプレシグニチャが削除される。

【００８２】

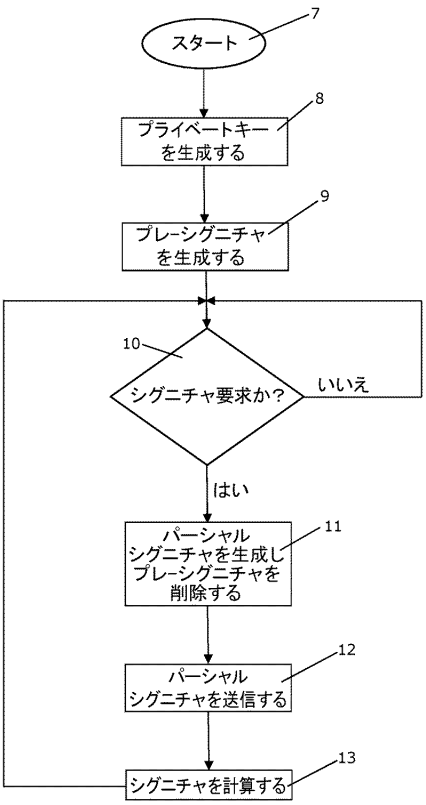
ステップ１２で、プレシグニチャノードのそれぞれは、署名を要求した署名アプリケーションにそのパーシャルシグニチャを送信する。最後に、署名アプリケーションは、ステップ１３で、受信したパーシャルシグニチャからシグニチャを計算する。

【図面】

【図１】



【図２】



フロントページの続き

(33)優先権主張国・地域又は機関
欧州特許庁(EP)
(72)発明者 ヤコブセン，トマス ペレ
デンマーク８３２０モースレト、オブストルプヴァイ１２コー
審査官 田中 啓介
(56)参考文献 国際公開第２０１９／１９３４５２（WO，Ａ１）
国際公開第２０１９／０４３４６６（WO，Ａ１）
国際公開第２０１９／１５９１７２（WO，Ａ１）
米国特許出願公開第２０１９／０２８０８６４（ＵＳ，Ａ１）
Steven Goldfeder et al.，Securing Bitcoin wallets via threshold signatures，Computer Science，2014年06月03日，https://jkroll.com/papers/bitcoin_threshold_signatures.pdf
Rosario Gennaro et al.，Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security，Applied Cryptography and Network Security 2016，2016年06月09日，https://link.springer.com/chapter/10.1007/978-3-319-39555-5_9
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ１２／１４、２１／００－２１／８８
Ｇ０６Ｑ１０／００－９９／００
Ｇ０９Ｃ１／００－５／００
Ｈ０４Ｋ１／００－３／００
Ｈ０４Ｌ９／００－９／４０