(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2022-545809
(P2022-545809A)
(43)公表日　令和4年10月31日(2022.10.31)

(51)国際特許分類　F I
H04L 9/08 (2006.01)　H04L 9/08 C
H04L 9/08 F

審査請求　未請求　予備審査請求　未請求　（全25頁）

(21)出願番号　特願2022-512404(P2022-512404)
(86)(22)出願日　令和2年8月24日(2020.8.24)
(85)翻訳文提出日　令和4年2月22日(2022.2.22)
(86)国際出願番号　PCT/AU2020/050888
(87)国際公開番号　WO2021/035295
(87)国際公開日　令和3年3月4日(2021.3.4)
(31)優先権主張番号　2019903083
(32)優先日　令和1年8月23日(2019.8.23)
(33)優先権主張国・地域又は機関
オーストラリア(AU)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　590003283
コモンウェルス サイエンティフィック アンド インダストリアル リサーチ オーガナイゼーション
オーストラリア２６０１オーストラリアン・キャピタル・テリトリー、アクトン、クルーニーズ・ロス・ストリート
(74)代理人　100108855
弁理士　蔵田 昌俊
(74)代理人　100179062
弁理士　井上 正
(74)代理人　100199565
弁理士　飯野 茂
(74)代理人　100212705
弁理士　矢頭 尚之
最終頁に続く

(54)【発明の名称】　暗号鍵生成のためのセキュアな環境

(57)【要約】
暗号鍵ペアを生成及び格納するためのデバイス（１０２）が開示される。デバイスは、非持続性メモリユニット（１１６）及びプロセッサ（１１４）を備える。プロセッサ（１１４）は、それぞれの複数のユーザから複数のシードを受信し、シードを組み合わせて複合シードを定義するように構成される。プロセッサ（１１４）はさらに、複合シード及び決定論的鍵生成方法を使用して、公開鍵及び秘密鍵（１０４）を含む鍵ペアを生成し、非持続性メモリユニット（１１６）に秘密鍵（１０４）を記録するように構成される。
【選択図】図１

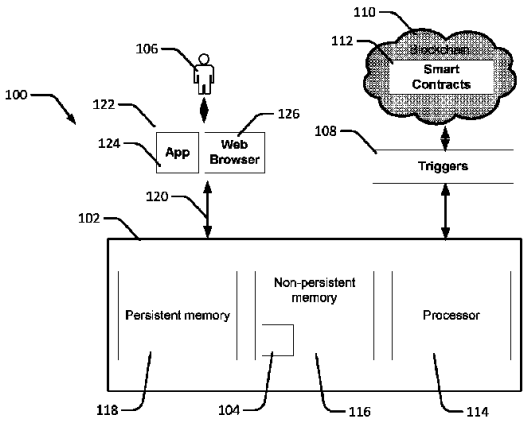


Fig. 1

【特許請求の範囲】
【請求項１】
暗号鍵ペアを生成及び格納するためのデバイスであって、
非持続性メモリユニットと、
プロセッサであって、
それぞれの複数のユーザから複数のシードを受信し、
前記シードを組み合わせて複合シードを定義し、
前記複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵を含む前記鍵ペアを生成し、
前記非持続性メモリユニットに前記秘密鍵を記録する、
ように構成された、前記プロセッサと、
を備える、前記デバイス。
【請求項２】
前記プロセッサが、
前記複数のシードの特定のシードが前記複合シードを定義するために使用されるという暗号証明を生成し、
前記それぞれのユーザに前記証明を提供する、
ようにさらに構成されている、請求項１に記載のデバイス。
【請求項３】
前記シードが、前記複数のシードをアルファベット順に並べ、それらを連結することによって組み合わせられる、請求項１または請求項２に記載のデバイス。
【請求項４】
前記複数のシードのそれぞれが、受信される前に、前記デバイスの公開鍵を使用して、前記それぞれのユーザによって暗号化される、先行請求項のいずれか１項に記載のデバイス。
【請求項５】
前記プロセッサが、前記秘密鍵を前記非持続性メモリユニットに記録する前に暗号化するようにさらに構成されている、先行請求項のいずれか１項に記載のデバイス。
【請求項６】
前記プロセッサが、
前記複数のシードの各サブセットであって、少なくとも所定の数のシードを含む前記各サブセット、をグループ化して、シードグルーピングを定義し、
前記シードグルーピングを使用して前記複合シードを暗号化することにより、シードグルーピングごとに複合シード暗号を生成し、
各複合シード暗号を持続性メモリユニットに記録する、
ようにさらに構成されている、先行請求項のいずれか１項に記載のデバイス。
【請求項７】
前記プロセッサが、
前記複数のシードのサブセットであって、少なくとも前記所定の数のシードを有する前記サブセット、を受信し、
前記複数のシードの前記サブセットを使用してシードグルーピングを生成し、
前記定義されたシードグルーピングに対応する前記持続性メモリユニット内の複合シード暗号を識別し、
前記定義されたシードグルーピングを使用して、前記複合シード暗号を復号し、
前記複合シードと前記決定論的鍵生成方法とを使用して、前記公開鍵と前記秘密鍵とを含む前記鍵ペアを再生成し、
前記非持続性メモリユニットに前記秘密鍵を記録する、
ようにさらに構成されている、先行請求項のいずれか１項に記載のデバイス。
【請求項８】
前記複合シード暗号が、前記シードグルーピングから生成された識別タグを使用して識

別される、請求項６または請求項７に記載のデバイス。
【請求項９】
前記プロセッサが、
秘密分散方法を使用して前記複合シードの複数のシェアを生成し、
少なくとも閾値数の前記複数のユーザに、前記複合シードのシェアを提供する、
ようにさらに構成されている、請求項１から５のいずれか１項に記載のデバイス。
【請求項１０】
前記プロセッサが、
閾値数の前記複合シードのシェアを受信し、
前記閾値数のシェアを使用して前記複合シードを決定し、
前記複合シードと前記決定論的鍵生成方法とを使用して、前記公開鍵と前記秘密鍵とを含む前記鍵ペアを再生成し、
前記非持続性メモリユニットに前記秘密鍵を記録する、
ようにさらに構成されている、請求項９に記載のデバイス。
【請求項１１】
前記シェアが、シャミアの秘密分散技術、フェルドマンの秘密分散技術、ペダーソンの秘密分散技術、またはスタドラーの秘密分散技術から選択された技術を使用して生成される、請求項９または請求項１０に記載のデバイス。
【請求項１２】
前記鍵ペアを生成及び格納するためのトラステッドプラットフォームモジュールを備える、先行請求項のいずれか１項に記載のデバイス。
【請求項１３】
暗号鍵ペアを生成するための方法であって、
それぞれの複数のユーザから複数のシードを受信することと、
前記シードを組み合わせて複合シードを定義することと、
前記複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵を含む前記鍵ペアを生成することと、
を含む、前記方法。
【請求項１４】
前記複数のシードの特定のシードが前記複合シードを定義するために使用されるという暗号証明を生成することと、
前記それぞれのユーザに前記証明を提供することと、
をさらに含む、請求項１３に記載の方法。
【請求項１５】
前記複数のシードの各サブセットであって、少なくとも所定の数のシードを含む前記各サブセット、をグループ化して、シードグルーピングを定義することと、
前記シードグルーピングを使用して前記複合シードを暗号化することにより、シードグルーピングごとに複合シード暗号を生成することと、
各複合シード暗号を持続性メモリユニットに記録することと、
をさらに含む、請求項１３または請求項１４に記載の方法。
【請求項１６】
前記複数のシードのサブセットであって、少なくとも前記所定の数のシードを有する前記サブセット、を受信することと、
前記複数のシードの前記サブセットを使用してシードグルーピングを生成することと、
前記定義されたシードグルーピングに対応する前記持続性メモリユニット内の複合シード暗号を識別することと、
前記定義されたシードグルーピングを使用して、前記複合シード暗号を復号することと、
前記複合シードと前記決定論的鍵生成方法とを使用して、前記公開鍵と前記秘密鍵とを含む前記鍵ペアを再生成することと、

前記非持続性メモリユニットに前記秘密鍵を記録することと、
をさらに含む、請求項１３から１５のいずれか１項に記載の方法。
【請求項１７】
秘密分散方法を使用して前記複合シードの複数のシェアを生成することと、
少なくとも閾値数の前記複数のユーザに、前記複合シードのシェアを提供することと、
をさらに含む、請求項１３または請求項１４に記載の方法。
【請求項１８】
前記閾値数の複合シードのシェアを受信することと、
前記閾値数のシェアを使用して前記複合シードを決定することと、
前記複合シードと前記決定論的鍵生成方法とを使用して、前記公開鍵と前記秘密鍵とを含む前記鍵ペアを再生成することと、
前記非持続性メモリユニットに前記秘密鍵を記録することと、
をさらに含む、請求項１７に記載の方法。
【請求項１９】
実行されるとプロセッサに請求項１３から１８のいずれか１項に記載の方法を実行させるソフトウェア命令を格納するように構成された、非一時的なコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０１９年８月２３日に出願された豪州仮特許出願第２０１９９０３０８３号の優先権を主張するものであり、その内容の全てが参照により本明細書に組み込まれる。
【０００２】
本開示は、暗号鍵を生成するためのデバイス及び方法を示す。
【背景技術】
【０００３】
様々なシステムが、重要なデータまたは機能へのアクセスを保護するために暗号化プロトコルに依存している。プロトコルは通常、重要なデータまたは機能への不正アクセスを防ぐために使用できる暗号鍵ペアを利用する。鍵ペアは、数学的に関連する公開鍵と秘密鍵を含む。関連する秘密鍵を秘密にしながら、公開鍵を自由に配布することができる。送信者は、受信者に関連付けられた公開鍵を使用してデータを暗号化でき、受信者は、関連する秘密鍵を使用してデータを復号できる。
【０００４】
同様のプロセスを使用して、デジタルオブジェクトの真正性を検証できる。このプロセスには、ユーザがユーザの秘密鍵を使用してデジタルオブジェクトに署名することが含まれる。署名されたオブジェクトは、次にユーザの秘密鍵に関連付けられた公開鍵を使用して、任意の他の当事者が検証できる。ユーザが秘密鍵の機密性を維持していると仮定して、検証されたデジタル署名は、オブジェクトのソースならびにその完全性を認証する。ソースの真正性は、ユーザの公開鍵に関連付けられた秘密鍵を使用してのみ署名を作成できるという事実によって保証される。したがって、検証により、署名を作成するエンティティが秘密鍵（秘密が保たれていると想定される）にアクセスできたことが保証される。
【０００５】
デジタル署名の作成後にオブジェクトを変更しても、検証を成功させることができないという事実によって、デジタルオブジェクトの完全性が保証される。
【０００６】
これらの暗号化プロトコルは、スマートコントラクトの実行、支払いの開始、及び暗号通貨などのデジタル資産の管理に使用される。
【０００７】
このようなシステムでは、暗号鍵ペアの公開鍵は自由に配布されるが、秘密鍵はシステ

ムに認識されないままであり、ユーザ自身がセキュアに管理していると見なされる。
【発明の概要】
【０００８】
第１の態様によれば、暗号鍵ペアを生成及び格納するためのデバイスが提供され、そのデバイスは
非持続性メモリユニットと、
プロセッサであって、
それぞれの複数のユーザから複数のシードを受信し、
シードを組み合わせて複合シードを定義し、
複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵を含む鍵ペアを生成し、
非持続性メモリユニットに秘密鍵を記録する、
ように構成されたプロセッサと、を備える。
【０００９】
このデバイスの利点は、複数のユーザからの複数のシードから暗号鍵ペアを生成できることである。複数のシードを使用することにより、単一のシードを使用して暗号鍵ペアを生成する場合よりも、暗号鍵ペアのセキュリティが向上する。
【００１０】
プロセッサは、
複数のシードの特定のシードが複合シードを定義するために使用されるという暗号証明を生成し、
それぞれのユーザに証明を提供する
ように、さらに構成することができる。
【００１１】
このデバイスの利点は、各ユーザが自分のシードが複合シードを定義するために使用されたという証明を受信することである。
【００１２】
シードは、複数のシードをアルファベット順に並べ、それらを連結することによって組み合わせることができる。
【００１３】
このデバイスの利点は、シードを計算効率の良い方法で組み合わせることができ、それによってデバイスの速度が向上することである。
【００１４】
複数のシードのそれぞれは、受信される前に、デバイスの公開鍵を使用して、それぞれのユーザによって暗号化され得る。
【００１５】
このデバイスの利点は、シードをデバイスにセキュアに送信できることである。
【００１６】
プロセッサは、秘密鍵を非持続性メモリユニットに記録する前に暗号化するようにさらに構成することができる。
【００１７】
このデバイスの利点は、秘密鍵が非持続性メモリに、よりセキュアに格納されることである。
【００１８】
プロセッサは、
複数のシードの各サブセットであって、少なくとも所定の数のシードを含む各サブセット、をグループ化して、シードグルーピングを定義し、
シードグルーピングを使用して複合シードを暗号化することにより、シードグルーピングごとに複合シード暗号を生成し、
各複合シード暗号を持続性メモリユニットに記録する、

ようにさらに構成され得る。
【００１９】
プロセッサは、
複数のシードのサブセットであって、少なくとも所定の数のシードを有するサブセット、を受信し、
複数のシードのサブセットを使用してシードグルーピングを生成し、
定義されたシードグルーピングに対応する持続性メモリユニット内の複合シード暗号を識別し、
定義されたシードグルーピングを使用して、複合シード暗号を復号し、
複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵とを含む鍵ペアを再生成し、
非持続性メモリユニットに秘密鍵を記録する、
ようにさらに構成され得る。
【００２０】
このデバイスの利点は、シードのサブセットを使用して鍵ペアを再生成できることである。これにより、鍵ペアを再生成する場合に、全てのユーザがシードを提供する必要がなくなる。
【００２１】
複合シード暗号は、シードグルーピングから生成された識別タグを使用して識別できる。
【００２２】
プロセッサは、
秘密分散方法を使用して複合シードの複数のシェアを生成し、
少なくとも閾値数の複数のユーザに、複合シードのシェアを提供する、ようにさらに構成され得る。
【００２３】
プロセッサは、
閾値数の複合シードのシェアを受信し、
閾値数のシェアを使用して複合シードを決定し、
複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵とを含む鍵ペアを再生成し、
非持続性メモリユニットに秘密鍵を記録する、
ようにさらに構成され得る。
【００２４】
このデバイスの利点は、複合シードのシェアを使用して鍵ペアを再生成できることである。これにより、鍵ペアを再生成する場合に、全てのユーザが入力を提供する必要がなくなる。
【００２５】
シェアは、シャミアの秘密分散技術、フェルドマンの秘密分散技術、ペダーソンの秘密分散技術、またはスタドラーの秘密分散技術から選択された技術を使用して生成できる。
【００２６】
デバイスは、鍵ペアを生成及び格納するためのトラステッドプラットフォームモジュールを備え得る。
【００２７】
別の態様によれば、暗号鍵ペアを生成するための方法が提供され、その方法は
それぞれの複数のユーザから複数のシードを受信することと、
シードを組み合わせて複合シードを定義することと、
複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵を含む鍵ペアを生成することと、
を含む。

【００２８】
方法は、
複数のシードの特定のシードが複合シードを定義するために使用されるという暗号証明を生成することと、
それぞれのユーザに証明を提供することと、
をさらに含み得る。
【００２９】
方法は、
複数のシードの各サブセットであって、少なくとも所定の数のシードを含む各サブセット、をグループ化して、シードグルーピングを定義することと、
シードグルーピングを使用して複合シードを暗号化することにより、シードグルーピングごとに複合シード暗号を生成することと、
各複合シード暗号を持続性メモリユニットに記録することと、
をさらに含み得る。
【００３０】
方法は、
複数のシードのサブセットであって、少なくとも所定の数のシードを有するサブセット、を受信することと、
複数のシードのサブセットを使用してシードグルーピングを生成することと、
定義されたシードグルーピングに対応する持続性メモリユニット内の複合シード暗号を識別することと、
定義されたシードグルーピングを使用して、複合シード暗号を復号することと、
複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵とを含む鍵ペアを再生成することと、
非持続性メモリユニットに秘密鍵を記録することと、
をさらに含み得る。
【００３１】
方法は、
秘密分散方法を使用して複合シードの複数のシェアを生成することと、
少なくとも閾値数の複数のユーザに、複合シードのシェアを提供することと、
をさらに含み得る。
【００３２】
方法は、
閾値数の複合シードのシェアを受信することと、
閾値数のシェアを使用して複合シードを決定することと、
複合シードと決定論的鍵生成方法とを使用して、公開鍵と秘密鍵とを含む鍵ペアを再生成することと、
非持続性メモリユニットに秘密鍵を記録することと、
をさらに含み得る。
【００３３】
別の態様によれば、実行されるとプロセッサに上記の方法を実行させるソフトウェア命令を格納するように構成された、非一時的なコンピュータ可読媒体が提供される。
【図面の簡単な説明】
【００３４】
【図１】暗号鍵ペアをセキュアに生成するためのシステムの概略図である。
【図２】暗号鍵ペアを生成する方法を示すフローチャートである。
【図３】暗号鍵ペアを生成する方法を示すフローチャートである。
【図４】暗号鍵ペアを生成する方法を示すフローチャートである。
【図５】図４の方法の例示的な実装の概略図である。
【図６】暗号鍵ペアを再生成する方法を示すフローチャートである。

【図７】暗号鍵ペアを生成する方法を示すフローチャートである。
【図８】暗号鍵ペアを再生成する方法を示すフローチャートである。
【図９】暗号鍵ペアをセキュアに生成するための例示的なシステムの概略図である。
【図１０】暗号鍵ペアを生成す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】
【００３５】
ユーザが自分自身の鍵を管理する場合、秘密鍵の紛失や盗難のリスクが高く、劇的な結果を招く可能性がある。これらには、暗号通貨の完全な喪失、データの喪失または盗難、アイデンティティの盗難によるシステムへの不正アクセス、またはユーザがシステムから永久にロックアウトされることが含まれ得る。システムが複数のデバイスからアクセスされる場合、ユーザは各デバイスに秘密鍵のコピーを持っていることが多いため、このリスクはさらに高くなる可能性がある。さらに、ユーザのグループが同じデータにアクセスするためにシステムを使用する場合、多くの場合、全てのユーザがシステム／データにアクセスできるように秘密鍵のコピーを持っている必要があり、これにより、鍵が盗まれる可能性がさらに高くなる。
【００３６】
秘密鍵は盗難の標的になる可能性があるだけでなく、それらを生成するために使用されるシードでもある。シードは、ユーザまたは他のシステムによって任意に定義された情報であり、通常は覚えやすいものである。多くの場合、ユーザは紛失した場合に鍵ペアを再生成するためにシードをバックアップとして格納し、また、これらのシードバックアップは盗難に対して脆弱である。
【００３７】
本明細書で説明するシステムと方法は、ユーザがデータの暗号化、復号、署名、検証、及び暗号鍵の使用を必要とするその他の操作のために暗号鍵のペアをセキュアに生成して使用することを可能にすると同時に、紛失や盗難の可能性を減らす、暗号化サービスを提供する。
【００３８】
概要
図１は、暗号鍵ペアの秘密鍵のセキュアな生成、格納、及び使用のためのシステム１００の概略図を示している。システム１００は、エンティティ１０６に代わって暗号鍵ペアの秘密鍵１０４を生成及び格納するためのデバイス１０２を備える。実際には、エンティティ１０６は複数のユーザを含み、それぞれが秘密鍵１０４を使用する所有権の主張また権利を有する。例えば、エンティティ１０６は、取締役会または事業のパートナーであり得る。
【００３９】
デバイス１０２は、鍵１０４を適用して、支払い、デジタルオブジェクトの署名、またはデータの暗号化／復号などのトランザクションを承認する権限を与えられている。承認は、個々の事柄についてエンティティ１０６（または適切な代表者）によって明示的に提供することができる。承認はまた、トリガー１０８によって示されるように、これらの条件が満たされたときに、デバイス１０２が鍵１０４を適用するように、所定の条件を使用して自動化することができる。例えば、完了した作業の証拠が提示された後、鍵１０４を使用して支払いを承認できる。いくつかの実施形態では、これらのトリガーは、スマートコントラクト１１２または暗号通貨などの他のデジタルオブジェクトを記録することもできるブロックチェーン１１０に記録される。
【００４０】
デバイス１０２は、プロセッサ１１４、非持続性メモリユニット１１６、及び持続性メモリユニット１１８を備える。プロセッサ１１４は、秘密鍵１０４を生成及び格納するために、図２の方法２００を実行するように構成される。最初に、ステップ２０２で、デバイス１０２は複数のシードを受信する。各シードは、通信ネットワーク１２０を介してエンティティ１０６に属するそれぞれのユーザによって提供される。例えば、シードを提供

するようにユーザを招待するために、ユーザには電子メールで連絡がある。シードの提供は、シーディングプロセスとも呼ばれる。

【００４１】

通信ネットワーク１２０は、インターネット、パッケージネットワーク、ローカルエリアネットワーク（ＬＡＮ）、無線ＬＡＮなどの任意の適切な通信チャネルであり得る。シードは、ユーザによって任意に定義された情報の断片である。例えば、シードフォーマットは次のようなものであり得る。

・英数字のシーケンス。

・ピン（Ｎ桁、Ｎ＝４、６、８以上）。

・パターン（携帯電話でパターンを形成する方法に類似したもの、または他のタイプのパターン）。

【００４２】

使用されるフォーマットに関係なく、全てのシードフォーマットは最終的に所定のフォーマットに変換される。例えば、いくつかの実施形態では、シードは、英数字のシーケンスとして表されるように変換される。他の実施形態では、シードは、１６進数で表されるように変換される。さらなる実施形態では、シードは、バイナリフォーマットで表されるように変換される。シードの所定のフォーマットへの変換は、クライアントデバイス１２２またはデバイス１０２によって実行することができる。

【００４３】

いくつかの実施形態では、シードは、ユーザがそれらをデバイス１０２に提供する前に、ユーザによって暗号化される。これは、シードをデバイス１０２に送信する前に、デバイス１０２の公開鍵を使用して達成することができる。この方法により、悪意のあるエージェントがシードを傍受した場合にシードを解読できないように保証する。

【００４４】

ユーザからデバイス１０２へのシードの暗号化及び通信は、アプリケーション１２４及びブラウザ１２６をホストするクライアント端末１２２によって容易にされる。アプリケーション１２４は、クライアント端末１２２とデバイス１０２との間の通信の確立を容易にし、ユーザを認証し、通信ネットワーク１２０を介して送信する前にシードを暗号化するための電子メール機能ならびに暗号化機能を含み得る。複数のクライアント端末を使用できることが理解されよう。例えば、各ユーザは、それら自身の端末１２２を有することができる。

【００４５】

ステップ２０４で、複数のシードが組み合わされて、複合シードを定義する。シードの組み合わせには、様々な方法を使用できる。いくつかの実施形態では、決定論的プロセスが使用され、他の実施形態では、非決定論的方法が使用される。所定のフォーマットが英数字である場合に使用するための例示的な決定論的方法は、各シードをアルファベット順に並べ、その後にシードを連結することである。このプロセスは、スティッチングアプローチと呼ばれる。例えば、デバイス１０２によって受信されている次のシードについて考えてみる。

Ｓ１＝「ＡＢＣ」

Ｓ２＝「ＸＹＺ」

Ｓ３＝「ＥＦＧ」

【００４６】

複合シードはＳ１＋Ｓ３＋Ｓ２＝「ＡＢＣ」＋「ＥＦＧ」＋「ＸＹＺ」＝「ＡＢＣＥＦＧＸＹＺ」によって与えられる。スティッチングアプローチには、実装が簡単で、計算量が多くないという利点がある。他の決定論的アプローチも可能である。例えば、複合シードが長くなるのを避けるために、シードを垂直方向に組み合わせることができ、つまり、全てのシードのｎ番目の文字が複合シードのｎ番目の文字に結合される。複数の文字を１つに結合することは、それらの数値表現の平均に基づくことができる（例えば、ＡＳＣＩＩコードを使用する）。これにより、長さが正確に最長のシードの長さである複合シード

が生成される。上記と同じ例を考えると、「Ａ」＋「Ｅ」＋「Ｘ」＝ＡＳＣＩＩ（（６５＋６９＋８８）／３）＝ＡＳＣＩＩ（７４）＝「Ｊ」である。この方法をシードのｎ番目ごとの文字に適用すると、複合シードは「ＪＫＬ」になる。

【００４７】

決定論的方法は、同じ複合シードが同じセットのシードから（再シーディングによって）取得でき、それが次に同じ鍵１０４を再生成できることを必要とする実施形態に適している。これは、同じ複合シードを取得するためにシードのサブセットのみを必要とする実施形態にも使用できる。これらのプロセスについては、以下で詳しく説明する。

【００４８】

いくつかの実施形態では、非決定論的方法を使用して、複数のシードを組み合わせて、複合シードを定義することができる。例えば、シードは受信した順序で連結できる。上記の例を使用すると、複合シードは「ＡＢＣＸＹＺＥＦＧ」になる。別の方法は、ランダムな順序でシードを連結することであり得る。他の非決定論的方法も可能である。非決定論的方法は、鍵１０４を再生成するためにシードのサブセットのみを必要とする実施形態に適している。このプロセスについては、以下でより詳細に説明する。

【００４９】

ステップ２０６において、ステップ２０４からの複合シードは、決定論的鍵生成方法と併せて使用され、公開鍵及び秘密鍵１０４を含む暗号鍵ペアを生成する。ステップ２０６の目的には、決定論的で非対称な鍵生成アルゴリズムが適している。例えば、いくつかの実施形態では、楕円曲線鍵を採用することができ、楕円曲線統合暗号化スキーム（ＥＣＩＥＳ）を暗号化／復号のために使用することができ、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）を、データの署名／検証のために使用することができる。他の例には、暗号化／復号及びデータの署名／検証の両方に使用できるＲｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ（ＲＳＡ）アルゴリズムが含まれる。

【００５０】

次に、秘密鍵１０４が非持続性メモリユニット１１６に記録され、公開鍵が使用可能にされる。例えば、公開鍵をブロックチェーン１１０に記録して、他の人がデバイス１０２を介してエンティティ１０６とセキュアに通信できるようにすることができる。

【００５１】

非持続性メモリに秘密鍵１０４を格納することは、鍵１０４のセキュリティをさらに改善する。これは、非持続性メモリユニット１１６を改ざんすると、ユニット１１６への電力が失われ、それによって鍵１０４が消去される可能性が高いために達成される。非持続性メモリは、キャッシュやランダムアクセスメモリ（ＲＡＭ）などの任意の揮発性メモリとすることができる。

【００５２】

いくつかの実施形態では、プロセッサ１１４は、秘密鍵１０４を、非持続性メモリユニット１１６に記録する前に暗号化するようにさらに構成される。ユニット１１６に記録する前に鍵１０４を暗号化すると、悪意のあるエージェントがユニット１１６から鍵１０４を正常に読み取ることに成功しても、依然として暗号化されており使用できないため、セキュリティがさらに強化される。

【００５３】

いくつかの実施形態では、トラステッドプラットフォームモジュールは、ステップ２０６を実行し、鍵１０４を格納するために使用される。

【００５４】

いくつかの実施形態では、方法２００は、図３に概略的に示されている方法２００’に置き換えられる。方法２００と共通の方法２００’のステップには、同一の参照番号が与えられており、再度説明しない。

【００５５】

方法２００’のステップ３０２において、プロセッサ１１６は、ステップ２０２で受信された複数のシードのうちの特定のシードが、対応するユーザによって作成されたという

暗号証明（発信証明）を取得する。このような暗号証明は、シード自体がユーザ自身の秘密鍵によって署名されている形式であり得る。これにより、悪意のあるエージェントがシードを傍受する、及び／またはシードをその独自のシードに置き換えるのを防ぐことができる。次に、プロセッサ１１６は、ステップ２０６を実行して、暗号鍵ペアを生成する。次に、プロセッサ１１６は、ステップ３０４を実行し、ユーザによって提供されたシードが複合シードの生成に使用され、続いて暗号鍵ペアの生成に使用されたことの第２の暗号証明をユーザに提供する。このような使用の第２の暗号証明は、シード自体が新たに作成された秘密鍵によって署名されている形式であり得る。

【００５６】

鍵ペアの再生成

前述のように、その生成後、秘密鍵１０４は、非持続性メモリユニット１１６に記録される。電源障害、ハードウェアの交換、またはデバイス１０２の再起動など、メモリユニット１１６への電力が失われる状況では、ユニット１１６に格納されている秘密鍵１０４は失われる。この場合、秘密鍵１０４を再生成する必要がある。秘密鍵１０４を再生成するための方法は、以下に詳述するように、特定の実施形態に応じて変化する。

【００５７】

全てのシードの使用

いくつかの実施形態では、鍵１０４の再生成は、鍵１０４を生成するために最初に使用されたのと同じプロセスに従うことによって達成される。すなわち、各ユーザは、そのシードを上記のようにデバイス１０２に提供する。次に、デバイス２００は、方法２００または方法２００’のいずれかを実行して、鍵１０４を再生成する。上記のように、この実施形態は、鍵１０４の再生成に使用される複合シードが最初に使用された複合シードと同じであることを保証するために、シードを組み合わせるための決定論的方法の使用を必要とする。これにより、再生成された鍵１０４が初期鍵と同じであることを保証する。

【００５８】

この実施形態は、各ユーザがそのシードを鍵１０４の再生成のために提供することを必要とする。これはある程度のセキュリティを提供するが、特定の状況では不便な場合もある。例えば、鍵１０４を再生成する必要があり、ユーザの１人以上がシードを提供できない場合、全てのユーザがシードを提供できるようになるまで、鍵１０４の再生成が遅延される。

【００５９】

シードのサブセットの使用

いくつかの実施形態では、秘密鍵１０４は、初期シードのサブセットのみを使用して再生成することができる。これらの実施形態は、鍵１０４の初期生成のために修正された方法２００を利用する。これらの修正された方法は、図４の方法２００’’及び図６の方法２００’’’として示され、以下ではそれぞれサブセット方法１及びサブセット方法２として説明される。

【００６０】

サブセット方法１

サブセット方法１を使用する実施形態では、図４の方法２００’’が、鍵１０４の初期生成に使用される。方法２００’’は、方法２００の全てのステップを含み、これらは同じ参照番号が与えられており、ここで再び説明することはない。方法２００’’は、ステップ４０２から４０６をさらに含み、図５を参照した例として説明される。

【００６１】

ステップ４０２で、ステップ２０２からのシードは、各可能な組み合わせのシードグルーピングを定義するために、所定の数のシードを有するサブセットにグループ化される。図５に示される例では、シードＳ１、Ｓ２、及びＳ３は、ステップ２０２で受信され、組み合わされて、ステップ２０４で複合シード５０２を定義する。次に、シードは２つのシードのサブセットにグループ化されて、シードグルーピング５０４から５０８を定義する。一般に、Ｎ個のシードを受信し、所定のシード数がＭ（Ｍ≦Ｎ）の場合、ステップ４０

２は、Ｍ個のシードの全ての可能な順序付けられていないグルーピングを見つける。順序付けされていないグルーピングの数は、少なくとも次のようになる。

【数１】

$$\binom{N}{M} = \frac{N!}{M!\,(N-M)!}$$

【００６２】

次に、ステップ４０４でこれらのグルーピングごとに複合シード暗号が生成され、図５に複合シード暗号５１０から５１４として示される。複合シード暗号は、これらのグルーピング５０４から５０８の１つでステップ２０４からの複合シード５０２を暗号化することによって生成され、少なくとも

【数２】

$$\binom{N}{M}$$

複合シード暗号になる。次に、これらの複合シード暗号は、ステップ４０６でデバイス１０２の持続性メモリ１１８に記録される。

【００６３】

いくつかの実施形態では、複合シード暗号は、複合シード暗号を作成するために使用されたシードグルーピングから生成されたタグに関連付けて格納される。これらのタグを使用して、特定のグルーピングによって生成された複合シード暗号を識別できる。

【００６４】

鍵１０４の再生成が必要な場合、デバイス１０２は、図６の方法６００を実行する。ステップ２０２’で、デバイス１０２は、ユーザのサブセットからシードのサブセットを受信する。サブセットのサイズは、少なくとも所定の数Ｍでなければならない。次に、デバイス１０２は、ステップ６０２を実行し、受信したシードのサブセットをグルーピングに組み合わせる。このグルーピングは、方法２００’’のステップ４０２で最初に生成されたグルーピングの１つと一致する。ステップ６０４で、このグルーピングを使用して生成された複合シード暗号は、持続性メモリ１１８内で識別され、その後、ステップ６０６でこのグルーピングを使用して復号される。復号された複合シード暗号は、最初に鍵１０４を生成するために使用された複合シードと同じであり、ステップ２０６’で再び使用されて鍵１０４を再生成する。

【００６５】

アイデンティティタグが使用されない実施形態では、方法６００は、潜在的に網羅的な検索を通じて正しい複合シード暗号を見つけなければならないので、計算集約的である。しかしながら、特定の状況では、再シーディングプロセスに対する総当たり攻撃が防止されるため、これは有益であり得る。

【００６６】

サブセット方法２

サブセット方法２を使用する実施形態では、図７の方法２００’’’が、鍵１０４の初期生成に使用される。方法２００’’’は、方法２００の全てのステップを含み、これらは同じ参照番号が与えられており、ここで再び説明することはない。方法２００’’’はまた、ステップ７０２及び７０４を含む。

【００６７】

ステップ７０２で、プロセッサ１１４は、秘密分散方法を使用して、複合シードのシェ

ア（フラグメントとも呼ばれる）を生成する。少なくとも閾値数のシェアが必要である。シェアを生成するための例示的な方法を以下に説明するが、他の方法も可能である。

【００６８】

この実施形態では、複合シードは、ここではa_0として示される数に変換される。次に、複合シードの各シェアは、多項式を使用して生成される。

【数３】

$$f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_{k-1}x^{k-1}$$

【００６９】

ここで、係数a_1からa_{k-1}はランダムに割り当てることができる。多項式の次数は、複合シードを決定するために必要なフラグメントの閾値数を決定し、システムの設計パラメータである。閾値数が大きいほど、秘密鍵１０４を再生成するためにより多くのシェアが必要とされる。この特定の例では、必要なシェアの閾値数はｋである。

【００７０】

フラグメントまたはシェアは、ｘの所与の値に対してｆ（ｘ）を評価することによって生成される。この方法で、任意の数のフラグメントを生成できる。しかしながら、少なくとも閾値数のフラグメントが一意のｘ値から生成される必要がある。つまり、ｆ（ｘ）は少なくともｋ個のｘの一意の値について評価される。次に、フラグメントは、ステップ７０４で格納するためにユーザに提供される。いくつかの実施形態では、これらのシェアは、それらがユーザに提供される前に暗号化される。

【００７１】

他の鍵秘密分散技術を使用して鍵フラグメントを生成できることが理解されよう。例えば、いくつかの実施形態では、フェルドマンの秘密分散技術が使用され、他の実施形態では、ペダーソンの秘密分散技術が使用される。さらに別の実施形態では、スタドラーの秘密分散技術が使用される。

【００７２】

鍵１０４の再生成が必要な場合、デバイス１０２は、図８の方法６００’を実行する。最初に、ステップ８０２で、デバイス１０２は、鍵１０４を再生成しようとするユーザから閾値数のシェアを受信する。これらのユーザは、方法２００’’’のステップ７０４で鍵１０４の初期生成中にこれらのシェアを受信しており、そして今、鍵１０４を再生成しようとするときにそれらをデバイス１０２に戻す。次に、デバイス１０２は、ステップ８０４を実行し、シェアから初期複合シードを決定する。これは、受信したシェアを補間して上記の多項式を復元することによって達成される。多項式から、ステップ２０６’で鍵１０４を再生成するために使用できる初期複合シードa_0を決定するのは簡単である。

【００７３】

この方法には、複合シードが持続性メモリに記録されず、暗号化された形式でも記録されず、鍵１０４を再生成するために閾値数のシェアが必要なだけであるという利点がある。シェアが生成された後、元のシードは冗長になる。

【００７４】

例示的な実装

実際には、デバイス１０２は、上記の方法論を実行するために複数のモジュールを使用して動作するように構成される。デバイス１０２の例示的な構成は、図９にデバイス１０２’として概略的に示されている。鍵１０４を最初に確立するプロセスは、デバイス１０２のこの例示的な構成及び図１０の方法１０００を参照して以下に説明される。

【００７５】

デバイス１０２は、セキュア暗号化マシン（ＳＣＭ）９０２、データリポジトリ９０４、マネージャモジュール９０６、ブートストラップモジュール９０８、及びコントローラモジュール９１０を備える。

【００７６】

モジュール９０６から９１０は、メモリモジュール１１８に格納されたソフトウェアアプリケーションであり得、これが実行されると、以下に概説される方法を実行する。例えば、モジュール９０６から９１０は、Ｃ＋＋またはＪａｖａ（登録商標）などのプログラミング言語で記述された関数またはクラスであり得る。

【００７７】

いくつかの実施形態では、モジュール９０６から９１０は、記載された方法を実行するように構成されたフィールドプログラマブルゲートアレイ（ＦＰＧＡ）である。

【００７８】

ＳＣＭ９０２は、堅牢な暗号化メカニズムを使用して複合シードから秘密鍵１０４を生成し、それを非持続性メモリに格納するハードウェアデバイスである。例えば、ＳＣＭ９０２は、ＡＭＤ Ｓｅｃｕｒｅ ＰｒｏｃｅｓｓｏｒをＳＣＭ９０２の中央処理装置（ＣＰＵ）として使用するＡＭＤ Ｓｅｃｕｒｅ Ｅｎｃｒｙｐｔｅｄ Ｖｉｒｔｕａｌｉｚａｔｉｏｎ（ＳＥＶ）であり得る。ＳＣＭ９０２の暗号化メカニズムは、非持続性メモリ内のデータが完全に暗号化され、ＳＣＭ９０２のＣＰＵのみがアクセスできることを保証する。ＳＣＭ９０２はさらに、生成または再生成された秘密鍵が持続性ストレージに決して格納されず、ＳＣＭ９０２の外部に送信されないように構成されている。

【００７９】

データリポジトリ９０４は、非持続性的メモリユニット１１６及び持続性メモリユニット１１８を表し、したがって、持続性及び非持続性的ストレージの両方のうちの少なくとも１つを備える。リポジトリ９０４は、ファイル、キーバリューストア、文書、ソフトウェア命令、または複合シード暗号などのデータ項目９０５を持続性メモリに記録し、秘密鍵を非持続性メモリに記録するために使用される。

【００８０】

マネージャモジュール９０６は、デバイス１０２’が最初に起動されたときに利用可能な唯一のコンポーネントである。マネージャモジュール９０６は、サインインした代表者がブートストラップを作成、更新、または削除することを可能にするマネージャウェブインタフェースを備える。

【００８１】

ブートストラップモジュール９０８は、マネージャモジュール９０６によって生成されたウェブインタフェースを介してエンティティ代表者９２０によって作成される。ブートストラップ９０８は、コントローラモジュール９１０、ユーザのセット、データリポジトリ９０４のセット、及びデータを処理し、ＳＣＭ９０２内で実行されるプログラムであるデータプロセッサ９１６のセットを作成するために使用される設定のリストを含む。そのようなエンティティが作成される前に、方法２００、２００’、２００’’または２００’’’などの鍵生成方法が、コントローラ９１０のための一意の鍵ペアを生成するために必要とされる。

【００８２】

コントローラモジュール９１０は、データコネクタを使用してデータリポジトリ９０４に接続し、様々なデジタルオブジェクトへの秘密鍵１０４の適用を管理する。例えば、コントローラモジュール９１０はＳＣＭ９０２のデータプロセッサ９１６を呼び出し、ユーザを認証し、デバイス１０２’への格納、処理、及びデータ配信などのデータサービスを提供することによる、データの暗号化／復号、署名などを管理する。認証プロセスについては、図１０を参照して以下でより詳しく説明する。

【００８３】

コントローラモジュール９１０は、ウェブインタフェース、及び／または、ユーザ９１４とデバイス１０２’との間の通信を容易にするアプリケーションプログラミングインタフェース（ＡＰＩ）９１２を含む。ユーザ９１４は、鍵生成のためのシードを提供するユーザ、またはエンティティ１０６との取引に関心のある消費者であり得る。すなわち、コントローラ９１０は、ＡＰＩのセット及びウェブインタフェースを可能にして、ユーザがデバイス１０２’の暗号化、復号、及び署名機能にセキュアにアクセスできるようにする

。ＡＰＩ９１２は、Ｒｅｐｒｅｓｅｎｔａｔｉｏｎ Ｓｔａｔｅ Ｔｒａｎｓｆｅｒ（ＲＥＳＴ）ＡＰＩである。

【００８４】

データプロセッサ９１６は、専用Ｄｏｃｋｅｒインスタンスなどの ＳＣＭ９０２で実行されるスクリプト９１８を実行し、そこでは、コントローラモジュール９１０を介して特定のデータリポジトリ９０４へのアクセスが許可される。データプロセッサ９１６は、秘密鍵１０４を使用してＳＣＭ９０２の暗号化機能（暗号化／復号／署名／検証）への制御されたアクセスを行う。いくつかの実施形態では、ＳＣＭ９０２は、それらのフルメモリ暗号化機能の恩恵を受けて、ＡＭＤ Ｒｙｚｅｎ ＰｒｏまたはＡＭＤ Ｅｐｙｃプロセッサ上で実行することができる。データプロセッサ９１６は、その環境で実行され、追加された機能を実行することができる「アドオン」と見なすことができる。デフォルトでは、データプロセッサのセットが任意のデバイス１０２に含まれている（例えば、トリガーは、ブロックチェーンネットワークと相互作用することを可能にするデータプロセッサとして実行することができる）。ユーザはまた、そのようなセキュアな環境上で独自のコードを実行し、デバイス１０２の制限されたＡＰＩにアクセスして、例えば、鍵１０４の自動使用を実装することができる。例えば、ＳＣＭ９０２は、Ｄｏｃｋｅｒコンテナまたは他の仮想化技術を使用して、ユーザ定義のコードを分離して実行できる。データプロセッサ９１６は、データリポジトリ９０４を入力として受信し、集約された形式または分析結果のいずれかで新しいデータを生成する。新しいデータは、データプロセッサ９１６に関連付けられたデータリポジトリ９０４に戻されて格納される。

【００８５】

図１０は、デバイス１０２’にシードを提供するための方法１０００の概略図である。ステップ１００２で、エンティティ代表者は、デバイス１０２’のマネージャモジュール９０６を介して自分自身を認証する。

【００８６】

いくつかの実施形態では、認証ステップ１００２は、サードパーティのアイデンティティプロバイダを使用して達成される。例えば、これらには、企業交換アカウント、Ｇｏｏｇｌｅアカウント、ソーシャルメディアアカウントなどが含まれる。

【００８７】

他の実施形態では、ブロックチェーンアイデンティティを使用して、秘密鍵チャレンジ（ＰＫＣ）を介して認証することができる。ＰＫＣは、ユーザのブロックチェーンアドレスを要求することから始まる。そのアドレスを使用して、マネージャモジュール９０６は、ブロックチェーンネットワークからユーザの公開鍵を検索する。次に、ランダムメッセージがデバイス１０２’によって生成され、ユーザに送信され、そこでユーザは、秘密鍵でメッセージに署名し、検証のためにデバイス１０２’に送信するように要求される。次に、署名されたメッセージは、認証のためにユーザの公開鍵に対して検証される。

【００８８】

次に、認証された代表者は、ステップ１００４で、マネージャモジュール９１０を介して、シーダとも呼ばれる他のユーザに関する情報を含むリストを提供する。シーダのリストは、代表者によって、アイデンティティ（例えば、ブロックチェーンまたはその他の認証システムのＩＤ）とその連絡先の詳細（例えば、電子メールアドレス）と併せたセットとして定義される。この情報を使用して、ステップ１００６で、ブートストラップ９０８が、マネージャモジュール９０６ウェブインタフェース上で認証された代表者によって作成される。

【００８９】

各シーダは、ステップ１００８で、ブートストラップ上のシーディングプロセスに参加するための招待リンクを受信する。全てのシーダは、シーディングプロセスに参加するように招待するために（例えば、電子メールで）連絡される。

【００９０】

ステップ１０１０で、例えば、代表者に対するのと同様の認証方法に従うことによって

、各シーダが認証される。複数のシードは、ステップ１０１２で、各シーダからデバイス１０２’への秘密メッセージの形で、それぞれの複数のシーダから提供される。シーダは、暗号化証明及びデバイス１０２’で使用される検証ソフトウェアのプロセスを使用して、シードが含まれていることを保証される。

【００９１】

シードは、従来の暗号化手段を使用してデバイス１０２’に安全に通信できる。説明の例として、デバイス１０２’が起動すると、その一意の公開鍵を公開して利用可能にする。ＳＣＭ９０２のトラステッドプラットフォームモジュール（ＴＰＭ）を使用して、関連する秘密鍵がデバイス１０２’に物理的かつ恒久的にリンクされた専用ハードウェアに安全に格納されることを保証することができる。デバイス１０２’に送信されるあらゆるデータは、デバイス１０２’の公開鍵を使用して暗号化する必要がある。したがって、デバイス１０２’のみがそのようなデータを復号することができる。

【００９２】

複数のシードが受信されると、デバイス１０２’は、方法２００、２００’、２００’’、２００’’’、６００または６００’のうち１つを実行して、秘密鍵１０４を生成する。

【００９３】

鍵１０４を取得しようとする悪意のあるエンティティが利用できる攻撃ベクトルは２つだけであると予想される。これらは、（ｉ）代表者及び十分な数のシーダを同時に侵害すること、または（ｉｉ）デバイス１０２のハードウェア暗号化メカニズムを侵害することである。

【００９４】

ユースケース

デバイス１０２は、企業環境または個人的な使用のために使用することができる。いくつかの実施形態では、デバイス１０２は、クラウドサンドボックス、物理マシンとして、または仮想アプライアンス上に展開することができる。

【００９５】

一実施形態では、デバイス１０２は、セキュアな分散環境上のオンラインサービスとしてのクラウドサンドボックスとして展開され、評価トライアルの開始点として利用することができる。クラウドサンドボックスとしてのデバイス１０２は、本番環境での使用を意図したものではなく、その理由は、サンドボックスで生成された秘密鍵は、ハードウェア攻撃（ハードウェアがクラウドサードパーティによって管理されている）に対して持続性または完全に保護されることが保証されていないためである。ただし、多くのクラウドプロバイダは、クラウドサンドボックス環境でもセキュリティ対策を有効にするために、将来的にデバイス１０２で使用できるハードウェアソリューションの展開を開始している。これにより、デバイス１０２をクラウドサービスとして配信し、物理アプライアンスと仮想アプライアンスのセキュリティレベルを一致させることができる。

【００９６】

別の実施形態では、デバイス１０２は、中小企業及び個人的な使用に利用される物理マシンである。つまり、事前構成された物理マシンにハードウェアセキュリティが提供される。さらなる実施形態では、デバイス１０２はまた、プライベートデータセンター上の仮想アプライアンスとして展開され得、企業環境にとって理想的である。物理マシンまたは仮想アプライアンスとしてのデバイス１０２は、ハードウェアベースのフルメモリ暗号化をサポートし、追加のセキュリティを提供し、秘密鍵が盗難の危険にさらされないようにする。

【００９７】

クラウドサンドボックスとしてのデバイス１０２は、パブリックＵＲＬを介してアクセスできる。物理マシンとしてのデバイス１０２は、一意のＩＰアドレスを介してアクセスできるが、仮想アプライアンスとしてのデバイス１０２は、ネットワーク構成に応じて、企業環境の内部でアクセスできる。

【００９８】

別の実施形態では、デバイス１０２は、「コールド」暗号ウォレットとは対照的に、「ホット」暗号ウォレットとして使用することができる。デバイス１０２は秘密鍵を保持し、常にライブで実行し続けるので、デバイス１０２は、スマートコントラクトを使用せずに、ユーザに代わって自動的に、したがって、デバイス１０２の「ホット」な性質で動作（例えば、毎月のサブスクリプション料金の支払い、慈善団体への定期的な寄付の送信、市場の変動に基づいた暗号通貨の売買など）するように構成できる。

【００９９】

別の実施形態では、デバイス１０２は、複数のユーザが同じ秘密鍵で安全に取引することを可能にする「分散」暗号ウォレットとして使用し、それでも責任を負うことができる。デバイス１０２は、誰がいつ取引するかを監視し、取引が署名される前に発行される投票プロセスまたは「管理者承認要求」を実施することができる。これは、より合理化された透明性のある経費管理のために企業環境で役立つ。また、行為を承認するために最小数の取締役が必要とされる状況においても有用であり得、デバイス１０２は、この最小数の取締役が行為のための秘密鍵の使用を承認することを必要とする。またそれは、銀行部門で同じ銀行口座への同時アクセス（パートナー、親戚、フィンテックサービスプロバイダなど）を安全に管理するために使用することもできる。

【０１００】

別の実施形態では、デバイス１０２は、暗号化された形式でデータを格納するためのセキュアなデータサイロとして使用することができ、それでも、指定された参加者とデータを分散することができる。クラウドベースのデバイス１０２は、既存のクラウドベースのストレージサービスに対するよりセキュアな代替手段などの機能を提供することができる。

【０１０１】

さらに別の実施形態では、デバイス１０２は、セキュアなアイデンティティプロバイダとして使用することができる。各ユーザは、サードパーティのオンラインサービスへの認証に使用できるセキュアに生成された秘密鍵を有している。デバイス１０２は、全てのユーザの秘密鍵を保持し、常にライブで実行し続けるので、全ての認証アクティビティを監視し、使用されていないサービスからユーザを自動的にログアウトすることさえできる。

【０１０２】

デバイス１０２は、秘密鍵を公開することなく、デバイス１０２内でホストされるセキュアな環境内で制限されたＡＰＩを提供する。そのようなセキュアな環境は、図９に示すようにデータプロセッサ９１６をホストする。データプロセッサは、その環境で実行され、追加された機能を実行することができる「アドオン」と見なすことができる。デフォルトでは、データプロセッサのセットがデバイス１０２のいくつかの実施形態に含まれている（例えば、トリガーは、ブロックチェーンネットワークと相互作用することを可能にするデータプロセッサとして実行することができる）。ユーザはまた、そのようなセキュアな環境上で独自のコードを実行し、デバイス１０２の制限されたＡＰＩにアクセスすることができる。例えば、ＳＣＭ９０２は、Ｄｏｃｋｅｒコンテナまたは他の仮想化技術を使用して、ユーザ定義のコードを分離して実行できる。

【０１０３】

ユーザ定義のデータプロセッサは、市場で取引され得る。例えば、ウェブベースの文書編集サービスは、デバイス１０２上で実行され、市場で購入されたバックエンドを使用することができる。別の例としては、暗号通貨の変動に迅速に対応してビットコインを自動的に取引できるデータプロセッサがあり得る。このようなデータプロセッサは、市場で購入できる可能性がある。市場自体はデバイス１０２上で実行されていることが可能であり、デバイス１０２の安全機能を継承する。

【０１０４】

本開示の技術は、様々な技術を使用して実施され得ることを理解されたい。例えば、本明細書で説明される方法は、適切なコンピュータ可読媒体上に存在する一連のコンピュータ実行可能命令によって実施され得る。適切なコンピュータ可読媒体には、揮発性（例え

ば、ＲＡＭ）及び／または不揮発性（例えば、ＲＯＭ、ディスク）メモリ、搬送波、伝送メディアが含まれ得る。例示的な搬送波は、ローカルネットワークまたはインターネットなどの公衆アクセス可能なネットワークに沿ってデジタルデータストリームを伝達する電気信号、電磁信号、または光信号の形をとることができる。

【０１０５】

以下の議論から明らかであるように特に明記しない限り、説明全体を通して、「推定」または「処理」または「計算」または「算出」、「最適化」または「決定」または「表示」または「最大化」などの用語を利用する議論は、コンピュータシステムのレジスタ及びメモリ内の物理的（電子的）量として表されるデータを、コンピュータシステムのメモリもしくはレジスタまたは他のそのような情報記憶、送信もしくは表示デバイス内の物理的量として同様に表される他のデータへ処理及び変換する、コンピュータシステムまたは同様の電子コンピューティングデバイスの動作及びプロセスを指すことが認識されるべきである、ということも理解されたい。

【０１０６】

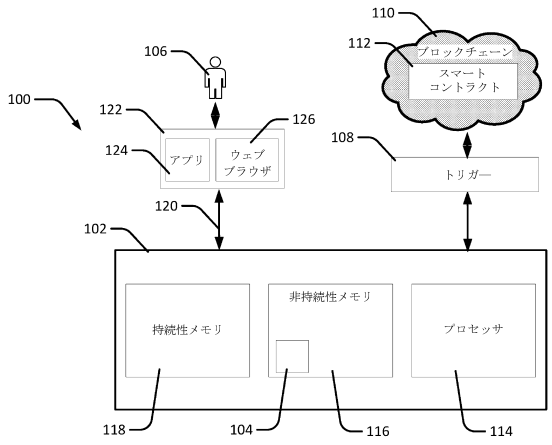
したがって、本発明の実施形態は、あらゆる点において例示的であり、制約的ではないと見なすべきである。

【０１０７】

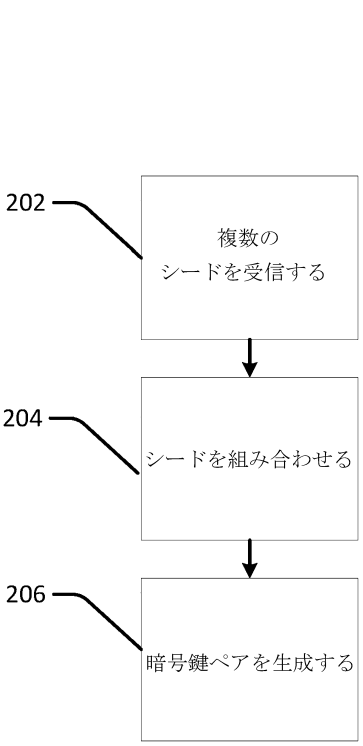
本開示の広範な一般的範囲から逸脱することなく、多数の変形及び／または修正が、上記の実施形態に行われ得ることは、当業者には理解されよう。したがって、本発明の実施形態は、全ての点で例示的であり、限定的ではないと見なされるべきである。

【図面】

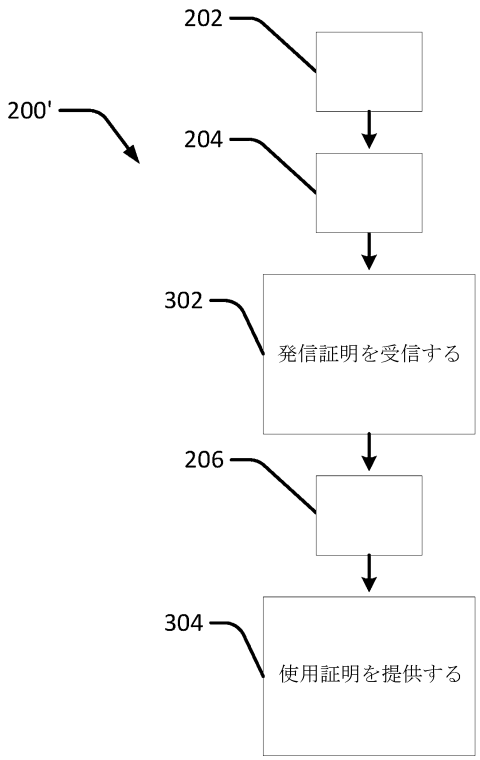
【図１】



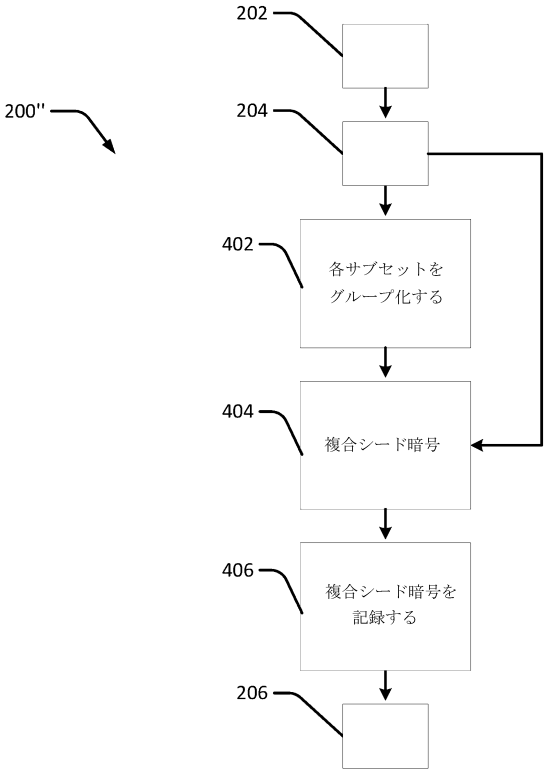
【図２】



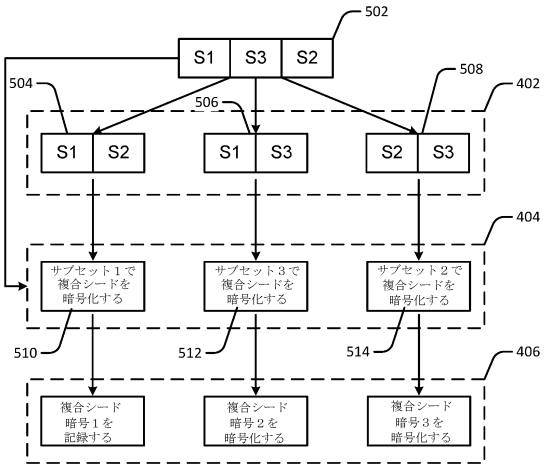
【図３】


202
200'
204
302
発信証明を受信する
206
304
使用証明を提供する

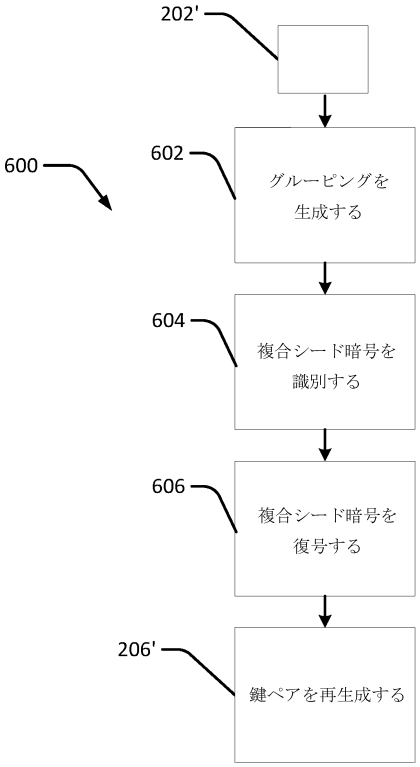
【図４】


202
200''
204
402
各サブセットを
グループ化する
404
複合シード暗号
406
複合シード暗号を
記録する
206

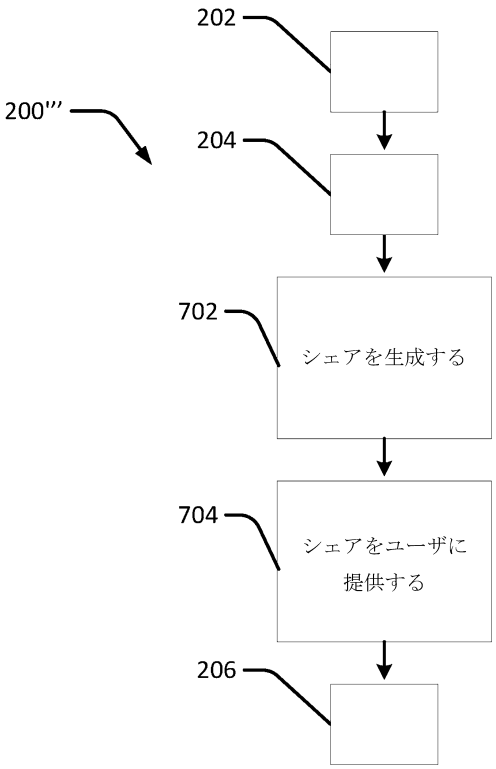
【図５】


502
S1
S3
S2
504
508
402
506
S1
S2
S1
S3
S2
S3
404
サブセット１で
複合シードを
暗号化する
サブセット３で
複合シードを
暗号化する
サブセット２で
複合シードを
暗号化する
510
512
514
406
複合シード
暗号１を
記録する
複合シード
暗号２を
暗号化する
複合シード
暗号３を
暗号化する

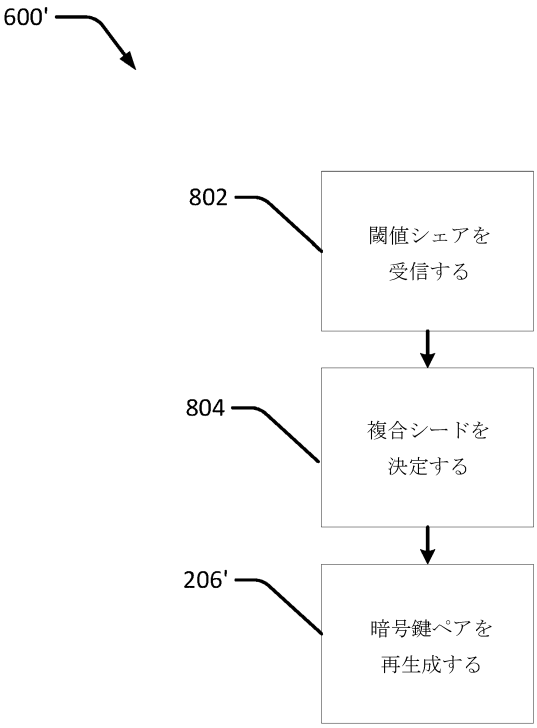
【図６】


202'
600
602
グルーピングを
生成する
604
複合シード暗号を
識別する
606
複合シード暗号を
復号する
206'
鍵ペアを再生成する

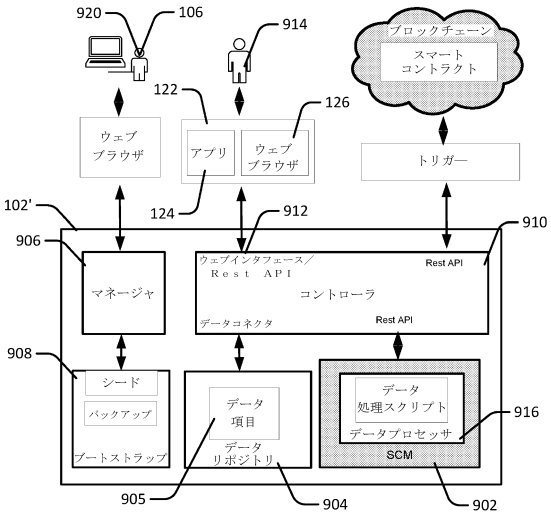
【図７】


202
200'''
204
702
シェアを生成する
704
シェアをユーザに
提供する
206

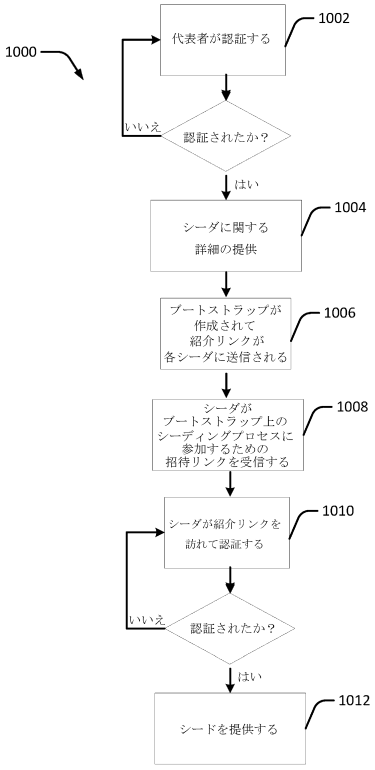
【図８】


600'
802
閾値シェアを
受信する
804
複合シードを
決定する
206'
暗号鍵ペアを
再生成する

【図９】


920
106
914
ブロックチェーン
スマート
コントラクト
122
126
ウェブ
ブラウザ
アプリ
ウェブ
ブラウザ
トリガー
102'
124
912
910
906
ウェブインタフェース／
Ｒｅｓｔ ＡＰＩ
Rest API
マネージャ
コントローラ
データコネクタ
Rest API
908
シード
バックアップ
ブートストラップ
データ
項目
データ
リポジトリ
データ
処理スクリプト
データプロセッサ
916
SCM
905
904
902

【図１０】


1000
代表者が認証する
1002
いいえ
認証されたか？
はい
シーダに関する
詳細の提供
1004
ブートストラップが
作成されて
紹介リンクが
各シーダに送信される
1006
シーダが
ブートストラップ上の
シーディングプロセスに
参加するための
招待リンクを受信する
1008
シーダが紹介リンクを
訪れて認証する
1010
いいえ
認証されたか？
はい
シードを提供する
1012

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2020/050888

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (2013.01) H04L 9/00 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PATENW, INSPEC: IPC/ CPC: H04L9/00/-, G06F21/00/-

Keywords: generate, cryptographic, key, pair, multiple, seed, combine and similar terms.

Google, Google Patents and Espacenet: Keywords as above.

Applicant/Inventor Name Search: External and internal databases provided by IP Australia.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October 2020	20 October 2020

Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Kevin Cai AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61262833159

Form PCT/ISA/210 (fifth sheet) (July 2019)

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. PCT/AU2020/050888
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017/0063531 A1 (CLOUDFLARE, INC.) 02 March 2017 See entire document and especially see abstract, paragraphs 20-24, 30-32, 51, 54 and Fig. 1	1-19
X	US 2014/0047237 A1 (GREY HERON TECHNOLOGIES) 13 February 2014 See entire document and especially abstract, paragraphs 3-8, 32, 34-36 and 45	1-19
X	WO 2017/006115 A1 (PIPA SOLUTIONS LTD) 12 January 2017 See entire document and especially abstract, page 2 lines 31-35, page 3 lines 17-33 and Fig. 1	1-19
X	WO 2013/171507 A1 (OMLIS LIMITED) 21 November 2013 See entire document and especially abstract, page 3 lines 20-24, page 5 lines 18-29	1-19
A	US 2002/0091640 A1 (GUPTA) 11 July 2002 See entire document	1-19
A	WO 2018/199963 A1 (HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P) 01 November 2018 See entire document	1-19
A	US 2009/0185677 A1 (BUGBEE) 23 July 2009 See entire document	1-19
A	US 2010/0153701 A1 (SHENOY ET AL.) 17 June 2010 See entire document	1-19
A	US 6381695 B2 (KUDO ET AL.) 30 April 2002 See entire document	1-19
A	US 8467533 B2 (HAMMERSMITH) 18 June 2013 See entire document	1-19

Form PCT/ISA/210 (fifth sheet) (July 2019)

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. PCT/AU2020/050888

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2017/0063531 A1	02 March 2017	US 2017063531 A1	02 Mar 2017
		US 9639687 B2	02 May 2017
		US 2017237566 A1	17 Aug 2017
		US 9942044 B2	10 Apr 2018
		US 2019116039 A1	18 Apr 2019
		US 10484176 B2	19 Nov 2019
		US 2020186351 A1	11 Jun 2020
US 2014/0047237 A1	13 February 2014	US 2014047237 A1	13 Feb 2014
		US 8914635 B2	16 Dec 2014
		US 2013028410 A1	31 Jan 2013
		US 8488779 B2	16 Jul 2013
		US 2013308774 A1	21 Nov 2013
		US 9270462 B2	23 Feb 2016
		US 2015180843 A1	25 Jun 2015
		US 9584495 B2	28 Feb 2017
WO 2017/006115 A1	12 January 2017	WO 2017006115 A1	12 Jan 2017
		EP 3320646 A1	16 May 2018
		US 2018198609 A1	12 Jul 2018
WO 2013/171507 A1	21 November 2013	WO 2013171507 A1	21 Nov 2013
		CN 104662570 A	27 May 2015
		EP 2852925 A1	01 Apr 2015
		EP 2853059 A1	01 Apr 2015
		EP 2853059 B1	13 May 2020
		GB 2502140 A	20 Nov 2013
		US 2015102104 A1	16 Apr 2015
		US 9509498 B2	29 Nov 2016
		US 2015131796 A1	14 May 2015
		US 9608805 B2	28 Mar 2017
		WO 2013171506 A1	21 Nov 2013
US 2002/0091640 A1	11 July 2002	US 2002091640 A1	11 Jul 2002
		US 7058605 B2	06 Jun 2006
		EP 0936805 A1	18 Aug 1999
		JP 2000066588 A	03 Mar 2000
		US 6446051 B1	03 Sep 2002

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. PCT/AU2020/050888

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
WO 2018/199963 A1	01 November 2018	WO 2018199963 A1	01 Nov 2018
		US 2020044843 A1	06 Feb 2020
US 2009/0185677 A1	23 July 2009	US 2009185677 A1	23 Jul 2009
		US 8503679 B2	06 Aug 2013
US 2010/0153701 A1	17 June 2010	US 2010153701 A1	17 Jun 2010
		US 8271775 B2	18 Sep 2012
US 6381695 B2	30 April 2002	US 2001052071 A1	13 Dec 2001
		US 6381695 B2	30 Apr 2002
		JP H11136230 A	21 May 1999
		JP 3542895 B2	14 Jul 2004
US 8467533 B2	18 June 2013	US 2003026429 A1	06 Feb 2003
		US 8467533 B2	18 Jun 2013
		AU 5303401 A	08 Oct 2001
		EP 1279249 A1	29 Jan 2003
		EP 1279249 B1	01 Aug 2007
		EP 1808977 A1	18 Jul 2007
		JP 2004501532 A	15 Jan 2004
		US 2014369498 A1	18 Dec 2014
		US 9450749 B2	20 Sep 2016
		US 2003016821 A1	23 Jan 2003
		US 2003026431 A1	06 Feb 2003
		WO 0174005 A1	04 Oct 2001

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(74)代理人 100219542
弁理士 大宅 郁治
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100162570
弁理士 金子 早苗
(72)発明者 グアブトニ、アドネネ
オーストラリア国、オーストラリアン・キャピタル・テリトリー ２６０１、アクトン、クルーニーズ・ロス・ストリート（番地なし）、コモンウェルス サイエンティフィック アンド インダストリアル リサーチ オーガナイゼーション気付
(72)発明者 オコナー、ヒューゴ
オーストラリア国、オーストラリアン・キャピタル・テリトリー ２６０１、アクトン、クルーニーズ・ロス・ストリート（番地なし）、コモンウェルス サイエンティフィック アンド インダストリアル リサーチ オーガナイゼーション気付
(72)発明者 ウェバー、インゴ
オーストラリア国、オーストラリアン・キャピタル・テリトリー ２６０１、アクトン、クルーニーズ・ロス・ストリート（番地なし）、コモンウェルス サイエンティフィック アンド インダストリアル リサーチ オーガナイゼーション気付