(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6571250号
(P6571250)

(45)発行日　令和1年9月4日(2019.9.4)　(24)登録日　令和1年8月16日(2019.8.16)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640E
H04L	9/08	(2006.01)	H04L	9/00	601C

請求項の数 22　外国語出願　(全 19 頁)

(21)出願番号　特願2018-144795 (P2018-144795)
(22)出願日　平成30年8月1日 (2018.8.1)
(62)分割の表示　特願2016-189123 (P2016-189123)の分割
原出願日　平成27年8月27日 (2015.8.27)
(65)公開番号　特開2018-201217 (P2018-201217A)
(43)公開日　平成30年12月20日 (2018.12.20)
審査請求日　平成30年8月31日 (2018.8.31)
(31)優先権主張番号　62/044,907
(32)優先日　平成26年9月2日 (2014.9.2)
(33)優先権主張国・地域又は機関　米国 (US)
(31)優先権主張番号　14/810,395
(32)優先日　平成27年7月27日 (2015.7.27)
(33)優先権主張国・地域又は機関　米国 (US)

(73)特許権者　503260918
アップル　インコーポレイテッド
Ａｐｐｌｅ　Ｉｎｃ.
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　アップル　パーク　ウェイ　ワン
One Apple Park Way, Cupertino, California 95014, U. S. A.
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100067013
弁理士　大塚　文昭

最終頁に続く

(54)【発明の名称】ある装置を使用して別の装置をアンロックする方法

(57)【特許請求の範囲】
【請求項１】
第１装置と第２装置をペアリングする方法であって、
前記第１装置と前記第２装置との間に通信チャンネルを確立し、
前記通信チャンネル経由で前記第２装置からの第１のキーを前記第１装置で受信し、
第２のキーを生成し、
前記第１のキーに署名して、署名された第１のキーを生成し、
前記署名された第１のキー、及び前記第２のキーを用いて、セッションを生成し、
前記セッションの生成に応答して、第３のキーを生成し、
前記通信チャンネル経由で、前記第２のキー及び前記第３のキーを前記第２装置へ送信し、
前記通信チャンネル経由で前記第２装置からの第４のキーを前記第１装置で受信し、前記第４のキーは前記第３のキーを用いて生成され、
前記第４のキーの受信に応答して、前記第１装置が前記第４のキーを用いて前記第２装置をアンロックするよう構成されている、方法。
【請求項２】
前記第１装置は第１のセキュアなプロセッサを備え、前記第２装置は第２のセキュアなプロセッサを備える、請求項１に記載の方法。
【請求項３】
前記第１装置は第１のセキュアなプロセッサを備え、

前記第１装置は、第１のセキュアなプロセッサのセキュア領域に前記第４のキーを記憶する、請求項１に記載の方法。
【請求項４】
前記第１装置は、生体認証センサと通信する第１のセキュアなプロセッサを備え、
前記生体認証センサ経由で、前記第１装置のユーザに関連する第１の生体認証データを検知し、
前記第１のセキュアなプロセッサで、前記第１の生体認証データを受信し、
前記第１の生体認証データと合致する出力データから、前記第１の生体認証データが認証されているかを判定し、
前記第１の生体認証データが認証されているという判定に応答して、前記第１装置にアクセスすることを許可し、
前記第１の生体認証データが認証されていないという判定に応答して、前記第１装置へのアクセスを制限する、ことを特徴とする請求項１に記載の方法。
【請求項５】
前記第１装置にアクセスすることを許可することは、前記第４のキーへのアクセスを許可することを含み、
前記第１装置へのアクセスを制限することは、前記第４のキーへのアクセスを制限することを含む、請求項４に記載の方法。
【請求項６】
前記第１装置と前記第２装置との間の通信チャンネルは、
前記第１装置が第１のセキュアなプロセッサを備え、及び前記第２装置が第２のセキュアなプロセッサを備えていることに応答して確立される、請求項１に記載の方法。
【請求項７】
前記第１装置と前記第２装置との間の通信チャンネルは、
前記第１装置が第１タイプの第１のセキュアなプロセッサを備え、及び前記第２装置が当該第１タイプの第２のセキュアなプロセッサを備えていることに応答して確立される、請求項１に記載の方法。
【請求項８】
前記第２装置で、パスワードを含むユーザ入力を受信することに応答して、前記第１のキーが前記第２装置によって生成される、請求項１に記載の方法。
【請求項９】
前記第２装置が前記第２のキー及び前記第３のキーを用いてセッションを生成することに応答して、前記第４のキーが前記第２装置によって生成される、請求項１に記載の方法。
【請求項１０】
第１装置から第２装置をアンロックする方法であって、前記第１装置は第１のセキュアなプロセッサを備え、
前記第２装置と信頼関係を確立し、
装置キーを用いて前記第１装置を認証し、
前記第２装置から秘密キーを受信し、
入出力装置からユーザ入力を受信し、
前記ユーザ入力の受信に応答し、受信した前記秘密キーを前記第２装置に送信して、前記前記第２装置をアンロックし、
前記第２装置と信頼関係を確立することは、前記第１のセキュアなプロセッサに関連するハードウェアキーから生成されるキーを用いて前記装置キーを認証することを含む、方法。
【請求項１１】
前記第２装置は第２のセキュアなプロセッサを備え、
前記ハードウェアキーは、前記第１のセキュアなプロセッサ及び前記第２のセキュアなプロセッサによって共有される、請求項１０に記載の方法。

【請求項１２】
前記ハードウェアキーは、前記第１のセキュアなプロセッサに関連する、デバイス固有のハードウェアキーである、請求項１０に記載の方法。
【請求項１３】
前記装置キーは前記第１のセキュアなプロセッサによって生成される、請求項１０に記載の方法。
【請求項１４】
前記第１のセキュアなプロセッサは、生体認証センサと通信する第１のセキュアなプロセッサを備え、
前記生体認証センサ経由で、前記第１装置のユーザに関連する第１の生体認証データを検知し、
前記第１のセキュアなプロセッサで、前記第１の生体認証データを受信し、
前記第１の生体認証データと合致する出力データから、前記第１の生体認証データが認証されているかを判定し、
前記第１の生体認証データが認証されているという判定に応答して、前記第１装置にアクセスすることを許可し、
前記第１の生体認証データが認証されていないという判定に応答して、前記第１装置へのアクセスを制限する、ことを特徴とする請求項１０に記載の方法。
【請求項１５】
前記第１装置は、１以上のスマートフォン、タブレット型コンピュータ、ラップトップ型コンピュータ、デスクトップ型コンピュータ、電子リーダー端末、スマートＴＶ、ハンドヘルド端末、ウェアラブル端末、ゲームコンソールのいずれかである、請求項１に記載の方法。
【請求項１６】
前記第２装置は、１以上のスマートフォン、タブレット型コンピュータ、ラップトップ型コンピュータ、デスクトップ型コンピュータ、電子リーダー端末、スマートＴＶ、ハンドヘルド端末、ウェアラブル端末、ゲームコンソールのいずれかである、請求項１５に記載の方法。
【請求項１７】
前記第１装置はハンドヘルド端末、前記第２装置はウェアラブル端末である、請求項１に記載の方法。
【請求項１８】
前記第１装置はハンドヘルド端末、前記第２装置はハンドヘルド端末である、請求項１に記載の方法。
【請求項１９】
前記第１装置は、１以上のスマートフォン、タブレット型コンピュータ、ラップトップ型コンピュータ、デスクトップ型コンピュータ、電子リーダー端末、スマートＴＶ、ハンドヘルド端末、ウェアラブル端末、ゲームコンソールのいずれかである、請求項１０に記載の方法。
【請求項２０】
前記第２装置は、１以上のスマートフォン、タブレット型コンピュータ、ラップトップ型コンピュータ、デスクトップ型コンピュータ、電子リーダー端末、スマートＴＶ、ハンドヘルド端末、ウェアラブル端末、ゲームコンソールのいずれかである、請求項１９に記載の方法。
【請求項２１】
前記第１装置はハンドヘルド端末、前記第２装置はウェアラブル端末である、請求項１０に記載の方法。
【請求項２２】
前記第１装置はハンドヘルド端末、前記第２装置はハンドヘルド端末である、請求項１０に記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、全般的に、装置のアンロック方法及びシステムに関するもので、より詳細には、ある装置を使用して別の装置をアンロックすることに関する。
【背景技術】
【０００２】
スマートホンやタブレットＰＣのような近代的な電子装置は、典型的に、装置を安全に保つために１つ以上のロック／アンロックメカニズムを有している。装置をアンロックするために、ユーザは、装置のログインスクリーンにパスコードを入力するか又は指紋スキャナで自分の指紋をスキャニングするような異なるメカニズムを使用することができる。これらのメカニズムは、典型的に、アンロックされる装置において直接的に実行される。
【発明の概要】
【０００３】
本発明は、全般的に、ある装置を使用して別の装置をアンロックすることに関する。本書において、別の装置をアンロックできる装置を第１装置と称し、そしてある装置によりアンロックされる装置を第２装置と称する。
【０００４】
ある実施形態では、第１装置を使用して第２装置をアンロックする方法が開示される。例えば、ハンドヘルド電子装置は、秘密キーの交換によりアンロックされないウェアラブル装置をアンロックすることができる。この方法は、第１装置を第２装置とペアにし；第２装置との信頼関係を確立し；各装置の個別の装置キー（装置から除去できない）を使用して両装置を相互に認証し（即ち、装置間の信頼関係を構築し）；セットアップ中に第２装置から秘密キーを受け取ってそれを記憶し；そしてユーザ入力を受け取るのに応答してその受け取った秘密キーを第２装置へ伝送して第２装置をアンロックする；ことを含む。換言すれば、第１装置は、最初、第２装置と連絡を取る。次いで、第２装置は、第１装置に秘密キーを送って、ユーザにパスコードを尋ねる。このパスコードで、第２装置は、マスターキーを導出し、アンロックを有効とし、そしてエスクローレコードを記憶することができる。このエスクローレコードは、アンロックキーにより暗号化されたマスターキーと、マスターキーにより暗号化されたアンロックキーとを含み、マスターキーが変化するたびに、レコードを更新することができる。
【０００５】
別の実施形態では、第１装置により第２装置をアンロックする方法が開示される。例えば、あるハンドヘルド装置は、別のハンドヘルド装置をアンロックすることができる。この方法は、第２装置との信頼関係を確立し；各装置の個別の装置キーを使用して両装置を相互に認証し；登録中に第１装置へ秘密キーを伝送し；パスコードを受け取った後に第２装置をアンロックし；パスコードからマスターキーを導出し；第１装置へ以前に伝送された秘密キーでマスターキーを暗号化し；第１装置から秘密キーを受け取り；その受け取った秘密キーを使用してマスターキーを検索し；そしてマスターキーを使用してアンロック動作を遂行する；ことを含む。換言すれば、第１装置は、先ず、チェックインして、相互認証を遂行し、そして第２装置と秘密キーを交換する。第２装置が初めて（ブートアップ以来）アンロックされるときは、第２装置は、交換した秘密キーにマスターキーをラップした状態に保つ。
【０００６】
更に別の実施形態では、第２装置をアンロックできる第１装置が開示される。第１装置は、第２装置とペアにするように構成されたペアリングモジュールと；装置キーを使用してそれ自身を認証するように構成された認証モジュールと；第２装置から秘密キーを受け取るように構成された受け取りモジュールと；第１装置の入力／出力装置から受け取られたユーザ入力を処理するように構成されたユーザ入力処理モジュールと；ユーザ入力に応答してその受け取った秘密キーを第２装置へ伝送して第２装置をアンロックするように構

成された伝送モジュールと；を備えている。
【０００７】
更に別の実施形態では、第１装置によりアンロックできる第２装置が開示される。第２装置は、第１装置とペアにするように構成されたペアリングモジュールと；第１装置からパブリック装置キー及び秘密キーを受け取るように構成された受け取りモジュールと；その受け取られたパブリック装置キーに、第２装置に関連したプライベート装置キーでサインするように構成されたキーサインモジュールと；第１装置へ秘密キーを伝送するように構成された伝送モジュールと；パスコードを処理するように構成されたユーザ入力処理モジュールと；パスコードからマスターキーを導出するように構成された導出モジュールと；マスターキーを秘密キーで暗号化するように構成された暗号化モジュールと；受け取った秘密キーを使用してマスターキーを検索するように構成された検索モジュールと；マスターキーを使用してアンロック動作を遂行するように構成されたアンロックモジュールと；を備えている。
【図面の簡単な説明】
【０００８】
【図１】本開示の実施形態により第１装置が第２装置をアンロックできる第１装置及び第２装置を示す。
【図２】本開示の実施形態により第１装置を使用して第２装置をアンロックする方法の規範的ステップを示すフローチャートである。
【図３】本開示の実施形態による登録プロセスの規範的ステップを示すフローチャートである。
【図４】本開示の実施形態により第１装置を使用して第２装置をアンロックする方法の規範的ステップを示すフローチャートである。
【図５】本開示の実施形態による図１の第１装置又は第２装置のような装置の規範的モジュールを示すブロック図である。
【図６】本開示の実施形態により２つの装置をペアリングする規範的ステップを示す。
【図７】本開示の実施形態により第１装置を使用して第２装置をアンロックする方法の規範的ステップを示す。
【図８】本開示の実施形態により、別の装置によって遠隔アンロックできる第２装置の規範的モジュールを示すブロック図である。
【図９】本開示の実施形態により、別の装置の遠隔アンロックを実行できる第１装置の規範的モジュールを示すブロック図である。
【図１０】本開示の実施形態に述べられた第１装置又は第２装置のようなコンピューティングシステムの規範的コンポーネントを示す。
【発明を実施するための形態】
【０００９】
規範的実施形態の以下の説明において、具現化できる特定の実施形態が例示された添付図面を参照する。種々の実施形態の範囲から逸脱せずに他の実施形態も使用でき且つ構造上の変化もなし得ることを理解されたい。
【００１０】
本発明は、一般的に、ある装置を使用して別の装置をアンロックすることに関する。本書において、別の装置をアンロックできる装置を第１装置と称し、そしてある装置によりアンロックされる装置を第２装置と称する。
【００１１】
図１は、第１装置１００及び第２装置１１２を示す。この実施形態では、第１装置１００は、第２装置１１２をアンロックするのに使用される。第１装置は、例えば、スマートホン、タブレットＰＣ、ラップトップ、デスクトップＰＣ、Ｍａｃ、電子リーダー、スマートＴＶ又はゲームコンソール、或いは別の装置と通信できる他の装置である。第１装置１００は、セキュアなエンクレーブプロセッサ（ＳＥＰ）１０５のようなセキュアなプロセッサと、カーネル１０８及びユーザランド１１０（通常ユーザスペースとも称される）

を含むアプリケーションプロセッサと、を備えている。ＳＥＰ１０５は、カーネル１０８及びユーザランド１１０を含むアプリケーションプロセッサ（ＡＰ）とは個別のプロセッサである。ユーザランド１１０は、装置における第三者アプリケーションの動作を促進することができる。カーネル１０８は、ＯＳのコアであり、ユーザランドへの多数のインターフェイスを与えると共に、アプリケーションからの入力／出力（Ｉ／Ｏ）要求を管理する。又、ある実施形態では、カーネル１０８は、装置１００のデータを保護するためにキー管理動作も遂行することができる。ＳＥＰ１０５は、キー管理モジュールがその中にあるセキュリティ境界を画成する比較的小さなプロセッサである。キーは、アンロックされるとき又は以前にアンロックされたときに入手できる。カーネル１０８は、ＳＥＰ１０５と通信することができる。

【００１２】

この実施形態では、ＳＥＰ１０５内に多数のプロセスがある。図１に示すように、ＳＥＰは、生物測定学的マッチングモジュール１０４及びキー管理モジュール１０６を備えている。

【００１３】

第１装置１００は、１つ以上のロック／アンロックメカニズムを備えている。第１装置をアンロックするそれらメカニズムの１つは、タッチスクリーン又は物理的キーパッドのようなＩ／Ｏ装置にパスコードを入力することによるものである。入力されると、パスコードは、ユーザランド１１０、カーネル１０８を通してＳＥＰ１０５へ搬送される。ＳＥＰは、パスコードに基づいて導出を行って、第１装置１００をアンロックできるかどうか決定し、そしてユーザデータキーのセットをアンロックするよう試みる。第１装置がアンロックされると、キー管理モジュール１０６のユーザデータキーが装置１００に入手できるようになる。

【００１４】

又、第１装置１００は、ユーザの指紋で装置をアンロックするように設計された指紋スキャナ１０２も備えている。この指紋スキャナ１０２は、指紋の画像を捕獲しそしてその画像を処理のために生物測定学的マッチングモジュール１０４へ伝送する。生物測定学的マッチングモジュールは、捕獲した指紋画像を有効と決めると、ランダムキーをキー管理モジュール１０６へ配布し、キー管理モジュール１０６のキーを装置１００で入手できるように促す。生物測定学的マッチングモジュール１０４は、指紋の分析を終了した後に、ランダムキーをメモリに任意に保持することができる。

【００１５】

図１に示すように、第２装置１１２は、第１装置と同じコンポーネントを備えている。例えば、第２装置１１２は、ＳＥＰ１１６と、カーネル１１８及びユーザランド１２０を含むアプリケーションプロセッサと、を備えている。ＳＥＰ１１６、カーネル１１８及びユーザランド１２０は、第１装置１００の対応部分と同様に動作する。第１装置とは異なり、この実施形態では、第２装置は、指紋スキャナを備えていない。或いは又、第２装置が指紋スキャナを有してもよい。ある実施形態では、第２装置１１２は、ＳＥＰ１１６及び生物測定学的マッチングモジュールを有しておらず、そしてキー管理モジュール１２２は、カーネル１１８に存在する。

【００１６】

一例において、第１装置は、指紋スキャナをもつｉＰｈｏｎｅ（登録商標）であり、そして第２装置は、指紋スキャナをもたないｉＰａｄ（登録商標）、ウェアラブル装置又は他の装置である。

【００１７】

上述したように、第１装置の生物測定学的マッチングモジュール１０４は、パスコードでアンロックされたときにキー管理モジュール１０６から秘密キー（例えば、ランダムキー）を受け取り、そしてそれを、第１装置が指紋一致によりアンロックされたときにキー管理モジュールへ配布する。以下に述べる実施形態では、第１装置１００は、同様の原理に基づいて第２装置１１２をアンロックする。特に、指紋センサにより受け取られる指紋

画像は、第１装置１００の生物測定学的マッチングモジュール１０４が秘密キーを配布するようにさせる。これは、第１装置をアンロックするのではなく、キー管理モジュール１０６が他の装置１１２のキー管理モジュール１２２へ秘密キーを解放するようにさせる。この秘密キーは、第１装置１００のユーザランド１１０を通り、２つの装置１００、１１２の両キー管理モジュール１０６、１２２を接続する通信チャンネル１３０を経、そして第２装置１１２のユーザランド１２０を通して、第２装置１１２のＳＥＰ１１６へ通過される。次いで、以下の実施形態で詳細に述べるように、秘密キーを使用して、第２装置１１２をアンロックする。

【００１８】

装置の一方がＳＥＰを備えそして他方がそれを備えていない場合には、保護が弱い装置が、保護が強い装置をアンロックできることを回避するために、ＳＥＰをもつ装置が、ＳＥＰを持たない装置へそのキーを送ることを拒絶する。従って、装置間に情報（例えば、他の装置を遠隔アンロックするための１つ以上のキー）が送信される前に、装置は、信頼できる装置（例えば、ＳＥＰをもつ装置）として互いに認証することができる。

【００１９】

先ず、共通のキーを使用して、第１及び第２装置の各々に関連した装置キー（以下に述べる）を、信頼できる装置のＳＥＰが所有していることを確認する。例えば、ある実施形態では、リモートアンロック動作は、同じ形式のＳＥＰ（例えば、アップルのＳＥＰ）を有する装置間でしか行えない。ある実施形態では、共通のキー、例えば、$K_{SEP\ GLOBAL}$は、２つの装置のＳＥＰが共有する対称的なハードウェアキーから導出される。次いで、リモートアンロック処理中に使用できる１つ以上の他のキーにサインするために、$K_{SEP\ GLOBAL}$が使用される。共通のキー、$K_{SEP\ GLOBAL}$によりサインされるキーは、ＳＥＰをもつ装置、即ち信頼できる装置から発生されると考えられる。別の実施形態では、共通の当局により承認された装置特有の非対称的キーが使用される。承認は、保護レベルを決定するのに使用できる装置の分類を含む。

【００２０】

$K_{SEP\ GLOBAL}$により有効にできるキーの１つは、装置ごとに独特で且つ装置の識別に使用できる装置キーK_dである。以下、第１装置を識別するキーをK_{d1}と称し、第２装置を識別するキーをK_{d2}と称する。ある実施形態では、K_dは、このペアリングのためにランダムに発生される秘密キー、ランダムに発生される普遍的に独特の識別子（ＵＵＩＤ）（例えば、ユーザキーの現在セットを識別するＫｅｙＢａｇ　ＵＵＩＤ）、及び装置特有のハードウェアキー、例えば、$K_{SEP\ LOCAL}$から導出される。$K_{SEP\ LOCAL}$は、装置に関連したデータを保護するのに使用できる装置のキー管理モジュールの装置キーの１つである。ランダムに発生される秘密キーは、キーのエントロピー及び独特さを与えるために生成時にキーストアにより発生されるランダム値である。ＵＵＩＤは、メカニズムによりアンロックされるＫｅｙＢａｇのためのものである。装置特有のハードウェアキーは、特定の入手性（例えば、いつでも、アンロックされた後に、又は装置がアンロックされるときに入手できる）を伴うデータ保護クラスキーである。第１装置は、「アンロックされる(is-unlocked)」装置キーを使用し、従って、それ自身アンロックされる間でなければ認証できない。第２装置は、「アンロックされている(been-unlocked)」装置キーを使用し、これは、遠隔アンロックされる前にアンロックされていることを要求する。アンロックプロセスの間に、K_{d1}及びK_{d2}は、各々、第１装置及び第２装置を認証する。ある実施形態では、K_{d1}及びK_{d2}は、第２装置が以前にアンロックされていないときに第１装置が第２装置をアンロックするのに使用される。

【００２１】

第２装置が以前にアンロックされている実施形態では、装置アンロックキー、K_{du}は、装置の認証に使用されるだけではなく、装置がユーザにより以前にアンロックされていたかどうか識別するのにも使用される。K_{du}は、対応する装置のＳＥＰにおいて発生され、装置に関連したパスコードを使用して保護される。以下、K_{du1}は、第１装置に関連した装置アンロックキーと称し、そしてK_{du2}は、第２装置に関連した装置アンロックキーと

称される。ある実施形態では、K_{du}は、装置が以前にアンロックされている場合しか導出されず、これは、正しいパスコードをもつ者によりアクセスされたことを意味する。装置が失われた場合には、新たなユーザは、おそらく、装置をアンロックするためのパスコードを有していない。新たなユーザが装置の全データを消去することにより装置をその元の状態に回復するよう試みる場合には、K_{du}が失われる。K_{du}がないと、装置は、それが同じユーザの制御下に依然あることを別の装置に証明することがもはやできない。換言すれば、K_{du}は、装置が信頼できる装置であることを証明するだけでなく、まだ同じユーザの制御下にあることを証明するのにも使用できる。従って、第１装置は、第２装置がもはやユーザの所有でなく且つ再ブートされたときに第２装置を誤ってアンロックしないことを保証するためにK_{du2}の存在に依存する。

【００２２】

図２－５は、本開示の実施形態による遠隔アンロック方法の種々の段階における規範的なアルゴリズムステップを示す。以下の実施形態は、一方向のアンロックプロセス（例えば、第１装置を使用して第２装置をアンロックする）を述べるが、ここに開示するシステム及び方法は、本開示の精神から逸脱せずに、両方向（例えば、第２装置を使用して第１装置をアンロックする）にアンロックを遂行するように容易に変更できることも理解されたい。

【００２３】

図２に示す実施形態では、リモートアンロックプロセス（例えば、第１装置を使用して第２装置をアンロックする）のアルゴリズムは、３つの主要ステップを含む。先ず、第１装置及び第２装置がペアリングされる（ステップ２０１）。次いで、第２装置が第１装置による遠隔アンロックを許可する（ステップ２０２）。最終的に、第１装置は、第１装置におけるユーザ入力に応答して第２装置をアンロックする（ステップ２０３）。これらのステップの各々を以下に詳細に述べる。

【００２４】

第１ステップにおいて、２つの装置がペアリングされる（ステップ２０１）。装置は、それらが互いに接近したときにＢｌｕｅｔｏｏｔｈ（登録商標）のような適当なペアリングメカニズムを使用してペアリングされる。ある実施形態では、Ｂｌｕｅｔｏｏｔｈ（登録商標）ペアリングは、Ｂｌｕｅｔｏｏｔｈ（登録商標）帯域外キーを使用したセキュアなペアリングである。例えば、装置は、一方の装置のカメラを使用して、他方の装置のディスプレイに表示されるコンピュータ読み取り可能なコード（例えば、ＯＲコード又はバーコード）を捕獲することにより、ペアリングされる。このコードは、２つの装置をペアリングするのに必要な装置ＩＤのような情報及び他の情報（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）帯域外キー）を含む。これらの実施形態では、接近ペアリングについて述べるが、２つの装置のペアリングは、必ずしも、装置が接近していることを要求するものではないことを理解されたい。実際に、このステップでは、いずれの距離にある装置をペアリングするように設計されたいずれのペアリングメカニズムも使用できる。

【００２５】

ペアリングされた後に、装置は、一方の装置が他方の装置により安全にアンロックできるように２つの装置間に信頼関係を確立できる登録プロセスへと進む。換言すれば、装置間のリモートアンロックを許可することができる（ステップ２０２）。特に、登録は、２つの装置のキーのコントローラ（例えば、ＳＥＰ）をペアリングし、そして２つの装置のＳＥＰを潜在的に結合することも含む。このステップは、例えば、装置が、登録プロセス中に認証するときに使用できる彼等のパブリックキーを交換し及びクロスサインし、共有キーをセットアップし、そしてアンロックプロセス中にその共有キーを使用することを含む。ある例では、ペアリングは、両装置において対称的に遂行される。

【００２６】

図３は、図２の登録ステップ２０２における規範的なアルゴリズムステップを示すフローチャートである。先ず、第１装置（即ち、アンロックを行う装置）は、パブリックキー、例えば、$K_{du1,pub}$を第２装置（即ち、アンロックされる装置）へ送出する（ステップ

３０１）。このパブリックキーは、第１装置が第２装置のアンロックを試みるときに第１装置が信頼できる装置であることを確認するのに使用される。又、第２装置は、許可も行い、これは、ユーザからパスコードを受け取り、そして任意であるが、ユーザが第２装置をローカルでアンロックするときに帯域外確認を行うことを含む（ステップ３０２）。パスコードは、K_{du2}を保護するので、装置がユーザの所有であることを証明するのに使用される。第２装置は、次いで、パブリックキー$K_{du1,pub}$にそのプライベートキー$K_{du2,private}$でサインする（ステップ３０３）。その結果、第２装置は、アンロック動作中に$K_{du1,pub}$を使用して認証する装置は、信頼できる装置であると決定できる。

【００２７】

登録が首尾良く終った場合には、第１装置は、次のように第２装置をアンロックするのに使用される。図４は、本開示の実施形態により第１装置を使用して第２装置をアンロックする規範的アルゴリズムステップ（即ち、図２のステップ２０３）を示す。ある例では、第１装置は、ハンドヘルド装置であり、そして第２装置は、ウェアラブル装置である。先ず、２つの装置は、それらが互いに近くにあることを検出する（ステップ４０１）。ある実施形態では、このステップは、装置が互いに接近することを要求せずに互いに位置付けできることしか要求しない。２つの装置間にはＢｌｕｅｔｏｏｔｈ（登録商標）又はＷｉ－Ｆｉチャンネルのような通信チャンネルが確立される（ステップ４０２）。第１装置は、K_{du1}を使用して認証される（ステップ４０３）。それに加えて又はそれとは別に、第２装置は、K_{du2}を使用して認証される。相互に認証され且つ暗号化されるトンネルをセットアップするためにステーション対ステーションプロトコルが使用される。ある実施形態では、両装置は、ペアリング中に交換されたサインキーを使用してプロセス中に認証される一時的暗号キーを使用する。第１装置は認証されているので、第２装置は、例えば、両装置により使用される一時的暗号キーから導出されるネゴシエート型セッションキーを使用して、ランダム秘密キーＳを第１装置へ送出する（ステップ４０４）。第１装置は、秘密キーを記憶する（ステップ４０５）。その後、第２装置は、パスコードでアンロックされる（ステップ４０６）。マスターキーＭが第２装置によりパスコードから導出される（ステップ４０７）。第２装置は、マスターキーＭを秘密キーＳで暗号化することによりトークンを構築し（ステップ４０８）、従って、第１装置が秘密キーＳを第２装置へ返送するとき、第２装置は、Ｓを使用してトークンを解読し、マスターキーＭを検索することができる。それに加えて、第２装置は、トークンを、マスターキーＭを使用して暗号化された秘密キーＳと連結し、そしてこの連結をエスクローレコードとして記憶する（ステップ４０９）。これは、マスターキーＭが変化して新たなトークンを構築するときに第２装置が秘密キーＳを回復できるようにする。別の実施形態では、第２装置は、秘密キーＳを使用して第１装置のためのエスクローレコードを発生して、秘密キーＳにラップされたマスターキーＭを記憶し、これは、以前にアンロックされることなく装置をアンロックできるようにする。換言すれば、第１の実施形態では、固定の秘密キー及びエスクローレコードをセットアップ中に確立することができ、そして別の実施形態では、ランダムな秘密キー及び一時的なエスクローレコードを登録中に装置のアンロックに応答して確立することができる。

【００２８】

図４を再び参照すれば、ユーザが第１装置で第２装置をアンロックすると決定したときに、第２装置は、K_{du2}を使用して認証される（ステップ４１０）。第１装置は、K_{du1}で認証される（ステップ４１１）。認証されると、それら装置は、互いに秘密キーを交換する。例えば、第１装置は、第２装置から受け取った秘密キーＳを第２装置へ返送する（ステップ４１２）。これは、第１装置の指紋スキャナを使用してユーザが自分の指紋をスキャニングするのに応答して行われる。第２装置は、秘密キーＳでトークンを解読することによりマスターキーＭを検索する（ステップ４１３）。マスターキーＭは、第２装置をアンロックできるようにする（ステップ４１４）。

【００２９】

第２装置が以前にアンロックされていない実施形態では、図４について述べた方法にお

いてK_{du2}に代わってK_{d2}が使用される。ある実施形態では、第２装置は、秘密キーＳを使用して第１装置のためのエスクローレコードを発生して、秘密キーＳにラップされたマスターキーＭを記憶し、これは、以前にアンロックされることなく装置をアンロックできるようにする。第１装置が第２装置のアンロックを試みるとき、第２装置は、装置キーを使用して、エスクローレコード及び秘密キーＳを探索して、マスターキーＭをアンラップし、これは、第２装置をアンロックするのに使用される。

【００３０】

図５は、別の装置をアンロックできるか又は別の装置によってアンロックされるか又はその両方である図１の第１装置１００又は第２装置１１２のような装置５００の規範的モジュールを示すブロック図である。この装置５００は、例えば、検出モジュール５０１、ペアリングモジュール５０２、キーサインモジュール５０３、送出モジュール５０４、受け取りモジュール５０５、認証モジュール５０６、キー発生モジュール５０７及びユーザ入力処理モジュール５０８を備えている。検出モジュール５０１は、第２装置を検出する（例えば、第２装置が付近にあるとき）。ペアリングモジュール５０２は、第１装置と第２装置をペアにする。キーサインモジュール５０３は、１つ以上のキーに別のキーでサインする。送出モジュール５０４は、１つ以上のキー（例えば、K_{du1}、Ｓ）を別の装置へ送出する。受け取りモジュール５０５は、別の装置から１つ以上のキー（例えば、Ｓ）を受け取る。認証モジュール５０６は、装置５００を認証する。キー発生モジュール５０７は、導出モジュールを含み、パスコードからマスターキーを導出し、そしてアンロックプロセスに使用できる１つ以上のハードウェアキー（例えば、$K_{SEP\ GLOBAL}$）を発生する。ユーザ入力処理モジュール５０８は、これに限定されないがパスコード及び／又は指紋を含むユーザ入力を処理する。

【００３１】

種々の実施形態において、図５のモジュールの幾つかは任意であり、そして装置５００には付加的なモジュールを含ませることができる。各モジュールは、ソフトウェア、ハードウェア又はその両方で実施することができる。ある実施形態では、装置５００のモジュールは、ここに開示するアルゴリズムを遂行するためのソフトウェアモジュールである。ある実施形態では、装置５００のモジュールは、ここに開示するアルゴリズムを遂行するためのコンピュータ読み取り可能なインストラクションを記憶するメモリに結合された１つ以上のプロセッサを表す。ある実施形態では、装置５００のモジュールは、前記機能を遂行するためのシステム・オン・チップのようなＡＳＩＣのハードウェア及びソフトウェアエレメントを含む。

【００３２】

図６及び７は、前記実施形態で述べた第１装置による第２装置の遠隔アンロックにおいてキー（又はレコード）の交換を促進することのできるトランスポートプロトコルアルゴリズムの実施形態を示す。

【００３３】

図６は、２つの装置のペアリングにおける規範的アルゴリズムステップを示す。このペアリングプロセスは、２つの装置間に通信チャンネルが既に確立された後に行うことができる。図６に示すように、２つの装置をペアにするために、先ず、第２装置は、ユーザが入力したパスワードを受け取る（ステップ６０１）。このパスワードは後で使用される。第２装置は、長期キーＫｅｙ　１を発生する（ステップ６０２）。ある実施形態では、長期キーの発生は、一方を別の装置へ送ることのできるキー対の生成と称される。ここで、Ｋｅｙ　１（即ち、キー対の一方のキーＫｅｙ　１）は、通信チャンネルを経て第１装置へ送られる（ステップ６０３）。第１装置は、Ｋｅｙ　１にサインしそしてそれを記憶する（ステップ６０４）。第１装置は、次いで、それ自身の長期キーＫｅｙ　２を発生する（ステップ６０５）。次いで、第２装置から受け取ったサイン済Ｋｅｙ　１、及び新たに発生された短期Ｋｅｙ　２を使用して、第１装置にセッションが生成される（ステップ６０６）。長期キーＫｅｙ　１と、Ｋｅｙ　２は、他のセッションを将来生成するために保持される。セッションが生成されると、別の短期キーＫｅｙ　３が生成される（ステップ

６０７）。次いで、通信チャンネルを横切って第２装置へＫｅｙ　２及び３が送られる（ステップ６０８）。

【００３４】

図６を参照すれば、Ｋｅｙ　２及びＫｅｙ　３を受け取った後、第２装置は、Ｋｅｙ　２にサインしそしてそれを記憶する（ステップ６０９）。次いで、第２装置は、Ｋｅｙ　２及びＫｅｙ　３の両方を使用してその終わりにセッションを生成する。セッションが生成された状態で、第２装置は、第１装置から受け取ったＫｅｙ　３を使用してＫｅｙ　４を発生する（ステップ６１１）。Ｋｅｙ　４は、次いで、通信チャンネルを横切って第１装置へ送られる（ステップ６１２）。第１装置がＫｅｙ　４を確認しそしてそれを記憶した後に、Ｋｅｙ　４は、第２装置をアンロックするためのキーとして登録される（ステップ６１４）。登録が失敗した場合には、メッセージが第１装置へ返送されて、第１装置にＫｅｙ　４を削除させる（ステップ６１５）。さもなければ、装置のペアリングが成功となり、そして装置は、遠隔アンロック動作（例えば、第１装置を使用して第２装置をアンロックする）を遂行するようにセットアップされる。

【００３５】

図７は、第１装置を使用して第２装置をアンロックする方法の規範的なアルゴリズムステップを示す。図７に示すように、先ず、第１装置は、第２装置をアンロックするためのユーザ入力を受け取る（ステップ７０１）。それに応答して、第１装置は、長期キーＫｅｙ　１及び２を使用してセッションを生成する（ステップ７０２）。新たに生成されたセッションから別の短期キーＫｅｙ　Ａが発生される（ステップ７０３）。次いで、第１装置は、通信チャンネルを横切って第２装置へＫｅｙ　Ａを送出する（ステップ７０４）。この実施形態では、ステップ７０３及び７０４は、第１装置と第２装置との間で短期キー合意をセットアップし、第２装置をアンロックするために後でＫｅｙ　４を送出できるようにする。短期キー（例えば、Ｋｅｙ　Ａ）は、セッションごとに独特で、Ｋｅｙ　４を暗号化するために一度しか使用されないので、短期キーの交換は、Ｋｅｙ　４が通信チャンネルを横切って送られるときに捕獲され、次いで、第１装置以外の装置から、第２装置をアンロックするために第２装置へ再送されるリプレイ攻撃を防止することができる。

【００３６】

短期Ｋｅｙ　Ａは、次いで、第２装置へ送られて（ステップ７０４）、第２装置にセッションを生成する（ステップ７０５）。次いで、第２装置は、Ｋｅｙ　Ａを使用して、別のキーＫｅｙ　Ｂを生成する（ステップ７０６）。図７を参照すれば、Ｋｅｙ　Ｂは、第１装置へ返送される（ステップ７０７）。第１装置は、Ｋｅｙ　Ｂを使用して、Ｋｅｙ　４を暗号化し、新たなキーＫｅｙ　Ｃを発生する（ステップ７０８）。暗号化されたＫｅｙ　４（即ち、Ｋｅｙ　Ｃ）は、第２装置へ送られ（ステップ７０９）、そして第２装置をアンロックするのに使用される（ステップ７１０）。アンロックプロセスは、Ｋｅｙ　Ｃを解読してＫｅｙ　４を検索しそしてＫｅｙ　４を使用して第２装置をアンロックすることを含む。

【００３７】

図８は、別の装置（例えば、第１装置）により遠隔アンロックされる図６及び７の第２装置８００の規範的モジュールを示すブロック図である。第２装置８００は、例えば、パスワード受け取りモジュール８０１、キー発生モジュール８０２、送出モジュール８０３、受け取りモジュール８０４、キーサインモジュール８０５、記憶モジュール８０６、セッション生成モジュール８０７、登録モジュール８０８、解読モジュール８０９、及びアンロックモジュール８１０を備えている。パスワード受け取りモジュール８０１は、ユーザからパスワード（又は他の入力）を受け取る。キー発生モジュール８０２は、長期及び／又は短期キー（例えば、図６及び７のＫｅｙ　１、４及びＢ）を発生する。送出モジュール８０３は、１つ以上の暗号化又は解読されたキーを別の装置（例えば、第１装置）へ送出する。受け取りモジュール８０４は、１つ以上の暗号化又は解読されたキーを別の装置（例えば、第１装置）から受け取る。キーサインモジュール８０５は、別の装置から受け取ったキー（例えば、Ｋｅｙ　２）にサインする。記憶モジュール８０６は、ローカル

で発生されるか又は別の装置から受け取られたキーを記憶する。セッション生成モジュール８０７は、別の装置から受け取ったキー（例えば、Ｋｅｙ　２及びＫｅｙ　Ａ）を使用してセッションを生成する。登録モジュール８０８は、キー（例えば、Ｋｅｙ　４）を、第２装置をアンロックするキーとして登録する。解読モジュール８０９は、別の装置から受け取った解読キー（例えば、Ｋｅｙ　Ｃ）を解読する。アンロックモジュール８１０は、キー（例えば、Ｋｅｙ　Ｃを解読することにより得たＫｅｙ　４）を使用して第２装置をアンロックすることができる。

【００３８】

図９は、別の装置（例えば、第２装置）のリモートアンロックを遂行できる図６及び７の第１装置９００の規範的モジュールを示すブロック図である。第１装置９００は、例えば、送出モジュール９０１、受け取りモジュール９０２、キーサインモジュール９０３、記憶モジュール９０４、セッション生成モジュール９０５、キー発生モジュール９０６、確認モジュール９０７、キー削除モジュール９０８、及び暗号化モジュール９０９を備えている。送出モジュール９０１は、１つ以上のキー（例えば、Ｋｅｙ　２、３、Ａ、Ｃ）を別の装置（例えば、図６及び７の第２装置）へ送出する。受け取りモジュール９０２は、別の装置（例えば、第２装置）から１つ以上のキー（例えば、Ｋｅｙ　１、４、Ｂ）を受け取る。キーサインモジュール９０３は、別の装置から受け取ったキー（例えば、Ｋｅｙ　１）にサインする。記憶モジュール９０４は、ローカルで発生されるか又は別の装置から受け取られた１つ以上のキーを記憶する。セッション生成モジュール９０５は、１つ以上のキー（例えば、Ｋｅｙ　１及び２）を使用してセッションを生成する。キー発生モジュール９０６は、１つ以上の長期及び／又は短期キー（例えば、Ｋｅｙ　２、３、Ａ、Ｃ）を発生する。確認モジュール９０７は、キー（例えば、Ｋｅｙ　４）を、別の装置をアンロックするキーとして確認する。キー削除モジュール９０８は、装置からキーを削除する。暗号化モジュール９０９は、別のキー（例えば、Ｋｅｙ　Ｂ）を使用してキー（例えば、Ｋｅｙ　４）を暗号化し、暗号化されたキー（例えば、Ｋｅｙ　Ｃ）を発生する。

【００３９】

種々の実施形態において、図８及び９のモジュールの幾つかは任意であり、そして装置８００及び９００には付加的なモジュールを含ませることができる。各モジュールは、ソフトウェア、ハードウェア又はその両方で実施することができる。ある実施形態では、装置８００及び９００のモジュールは、ここに開示するアルゴリズムを遂行するためのソフトウェアモジュールである。ある実施形態では、装置８００及び９００のモジュールは、ここに開示するアルゴリズムを遂行するためのコンピュータ読み取り可能なインストラクションを記憶するメモリに結合された１つ以上のプロセッサを表す。ある実施形態では、装置８００及び９００のモジュールは、前記機能を遂行するためのシステム・オン・チップのようなＡＳＩＣのハードウェア及びソフトウェアエレメントを含む。

【００４０】

ある実施形態では、装置５００、８００及び９００のモジュールの１つ以上は、インストラクション実行システム、装置、又はデバイス、例えば、コンピュータベースのシステム、プロセッサ収容システム、或いはそのインストラクション実行システム、装置、又はデバイスからインストラクションをフェッチしてそのインストラクションを実行する他のシステムにより又はそれに関連して使用するために不揮発性コンピュータ読み取り可能な記憶媒体内に記憶され及び／又はその中でトランスポートされる。本書において、「不揮発性コンピュータ読み取り可能な記憶媒体」とは、インストラクション実行システム、装置又はデバイスにより又はそれに関連して使用するためにプログラムを収容し又は記憶できる媒体である。不揮発性コンピュータ読み取り可能な媒体は、電子、磁気、光学、電磁、赤外線又は半導体システム、装置又はデバイス、ポータブルコンピュータディスケット（磁気）、ランダムアクセスメモリ（ＲＡＭ）（磁気）、リードオンリメモリ（ＲＯＭ）（磁気）、消去可能なプログラマブルリードオンリメモリ（ＥＰＲＯＭ）（磁気）、ポータブル光学ディスク、例えば、ＣＤ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ、ＤＶＤ－Ｒ又はＤＶＤ－ＲＷ、或いはフラッシュメモリ、例えば、コンパクトフラッシュ（登録商標）カー

ド、セキュアなデジタルカード、ＵＳＢメモリデバイス、メモリスティック、等を含むが、それらに限定されない。

【００４１】

不揮発性のコンピュータ読み取り可能な記憶媒体は、第１装置又は第２装置として働くコンピュータシステムの一部分である。図１０は、１つのそのようなコンピューティングシステムの規範的共通コンポーネントを示す。図示されたように、システム１０００は、中央処理ユニット（ＣＰＵ）１００２；これに限定されないが、ディスプレイ、キーパッド、タッチスクリーン、スピーカ、及びマイクロホンの１つ以上を含むＩ／Ｏコンポーネント１００４；最後の段落にリストされたような記憶媒体１００６；及びネットワークインターフェイス１００８を備え、これらは、全て、システムバス１０１０を経て互いに接続される。記憶媒体１００６は、図５、８及び９のモジュールを含む。

【００４２】

それ故、以上のことから、本開示の幾つかの実施例は、第１装置から第２装置をアンロックする方法において、第２装置との信頼関係を確立し；装置キーを使用して第１装置を認証し；第２装置から秘密キーを受け取り；入力／出力装置からユーザ入力を受け取り；及びユーザ入力を受け取るのに応答して前記受け取った秘密キーを第２装置へ伝送して第２装置をアンロックする；ことを含み、前記第２装置との信頼関係を確立することは、第１装置に関連したハードウェアキーから発生されるキーを使用して前記装置キーを認証することを含む方法、に向けられる。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、第１装置との信頼関係を確立する前に、前記方法は、第２装置により捕獲されるべき表示にコードを表示することにより第１装置と第２装置をペアにすることを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記第２装置とペアにすることは、Ｂｌｕｅｔｏｏｔｈ（登録商標）帯域外キーで行われる。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記第２装置との信頼関係を確立することは、パブリックキーを第２装置へ送出することを含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記パブリックキーは、インスタンス秘密、１組のキーを識別するＵＵＩＤ、及びプライベート装置ハードウェアキーから発生された装置キーを含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、第１装置に関連したハードウェアキーから発生されるキーを使用してパブリックキーを有効なものとすることを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、ハードウェアキーは、第２装置と共有される。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、パブリックキーは、共有当局により承認される。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、第２装置に関連した装置キーを使用して第２装置を認証することを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、第２装置に関連した装置キーは、第２装置が以前にアンロックされたかどうか指示するように構成される。

【００４３】

又、本開示の幾つかの実施例は、第１装置によりアンロックするために第２装置で実行される方法において、第１装置からパブリック装置キーを受け取り；受け取ったパブリック装置キーを第２装置に関連したプライベート装置キーでサインし；第１装置へ秘密キーを伝送し；パスコードを受け取り；パスコードからマスターキーを導出し；秘密キーでマスターキーを暗号化し；第１装置から秘密キーを受け取り；その受け取った秘密キーを使用してマスターキーを検索し；及びマスターキーを使用してアンロック動作を遂行する；ことを含む方法、に向けられる。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、第１装置に関連した装置ＩＤを使用して第１装置を認証することを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、パスコードを使用して第２装置をアンロックすることを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、

秘密キーは、ランダムキーを含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、秘密装置キーは、第２装置がパスコードで以前にアンロックされたかどうか指示するように構成される。

【００４４】

本開示の幾つかの実施例は、第２装置をアンロックすることのできる第１装置の不揮発性コンピュータ読み取り可能な記憶媒体において、プロセッサにより実行されたときに、装置キーを使用して第１装置を認証し；第２装置から秘密キーを受け取り；第１装置の入力／出力装置から受け取ったユーザ入力を処理し；及び前記ユーザ入力に応答して前記受け取った秘密キーを第２装置へ送出して第２装置をアンロックする；ことを含む方法を遂行するインストラクションを記憶する記憶媒体、に向けられる。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、第２装置が第１装置のＢｌｕｅｔｏｏｔｈ（登録商標）範囲内にあるかどうか検出することを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、第１キーを第２キーでサインすることを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記第１キーは、装置キーを含み、そして前記第２キーは、ＳＥＰグローバルキーを含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、ＳＥＰグローバルキー、装置キー、及び装置アンロックキーのうちの少なくとも１つを発生することを更に含む。

【００４５】

本開示の幾つかの実施例は、第１装置でアンロックできる第２装置の不揮発性コンピュータ読み取り可能な記憶媒体において、プロセッサにより実行されたときに、第１装置からパブリック装置キー及び秘密キーを受け取り；第２装置に関連したプライベート装置キーで前記受け取ったパブリック装置キーをサインし；第１装置へ秘密キーを送出し；パスコードを処理し；パスコードからマスターキーを導出し；秘密キーでマスターキーを暗号化し；前記受け取った秘密キーを使用してマスターキーを検索し；及びマスターキーを使用してアンロック動作を遂行する；ことを含む方法を遂行するインストラクションを記憶する記憶媒体、に向けられる。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、第１装置に関連した装置ＩＤを使用して第１装置を認証することを更に含む。以上に開示した１つ以上の実施例に加えて又はそれとは別に、ある実施例では、前記方法は、パスコードを使用して第２装置をアンロックすることを更に含む。

【００４６】

本開示の幾つかの実施例は、第２装置をアンロックできる第１装置において、第２装置と信頼関係を確立しそして装置キーを使用して第１装置を認証するように構成された認証モジュールと；第２装置から秘密キーを受け取るように構成された受け取りモジュールと；入力／出力装置から受け取られたユーザ入力を処理するように構成されたユーザ入力処理モジュールと；ユーザ入力を受け取るのに応答して前記受け取られた秘密キーを第２装置へ送出して第２装置をアンロックするように構成された送出モジュールと；を備え、前記第２装置と信頼関係を確立することは、第１装置に関連したハードウェアキーから発生されたキーを使用して装置キーを認証することを含む、第１装置に向けられる。

【００４７】

本開示の幾つかの実施形態は、第１装置によってアンロックできる第２装置において、第１装置からパブリック装置キーを受け取るように構成された受け取りモジュールと；その受け取ったパブリック装置キーに、第２装置に関連したプライベート装置キーでサインするように構成されたキーサインモジュールと；秘密キーを第１装置に送出するように構成された送出モジュールと；パスコードを処理するように構成されたユーザ入力処理モジュールと；パスコードからマスターキーを導出するように構成された導出モジュールと；マスターキーを秘密キーで暗号化するように構成された暗号化モジュールと；第１装置から秘密キーを受け取りそして受け取った秘密キーを使用してマスターキーを検索するための受け取りモジュールと；マスターキーを使用してアンロック動作を遂行するように構成

されたアンロックモジュールと；を備えた第２装置に向けられる。

【００４８】

添付図面を参照して実施形態を完全に説明したが、当業者であれば、種々の変更や修正が明らかであることに注意されたい。そのような変更や修正は、特許請求の範囲で規定される種々の実施形態の範囲内に包含されるものと理解されたい。

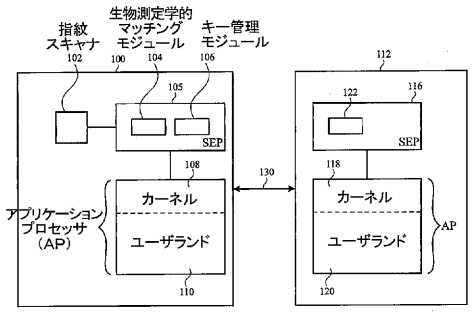
【符号の説明】

【００４９】

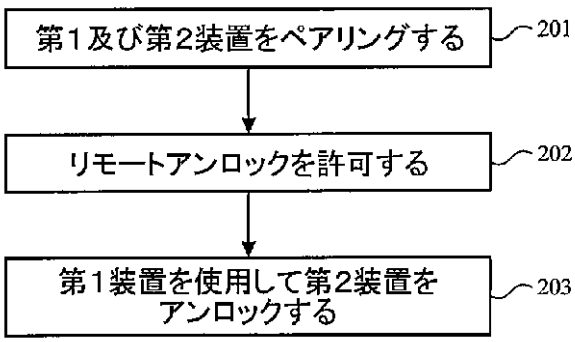
１００：第１装置
１０２：指紋スキャナ
１０４：生物測定学的マッチングモジュール
１０５：セキュアなエンクレーブプロセッサ（ＳＥＰ）
１０６、１２２：キー管理モジュール
１０８、１１８：カーネル
１１０、１２０：ユーザランド
１１２：第２装置
５００：装置
５０１：検出モジュール
５０２：ペアリングモジュール
５０３：キーサインモジュール
５０４：送出モジュール
５０５：受け取りモジュール
５０６：認証モジュール
５０７：キー発生モジュール
５０８：ユーザ入力処理モジュール
８００：第２装置
８０１：パスワード受け取りモジュール
８０２：キー発生モジュール
８０３：送出モジュール
８０４：受け取りモジュール
８０５：キーサインモジュール
８０６：記憶モジュール
８０７：セッション生成モジュール
８０８：登録モジュール
８０９：解読モジュール
８１０：アンロックモジュール
９００：第１装置
９０１：送出モジュール
９０２：受け取りモジュール
９０３：キーサインモジュール
９０４：記憶モジュール
９０５：セッション生成モジュール
９０６：キー発生モジュール
９０７：確認モジュール
９０８：キー削除モジュール
９０９：暗号化モジュール
１０００：システム
１００２：中央処理ユニット（ＣＰＵ）
１００４：Ｉ／Ｏコンポーネント
１００６：記憶媒体
１００８：ネットワークインターフェイス

１０１０：システムバス

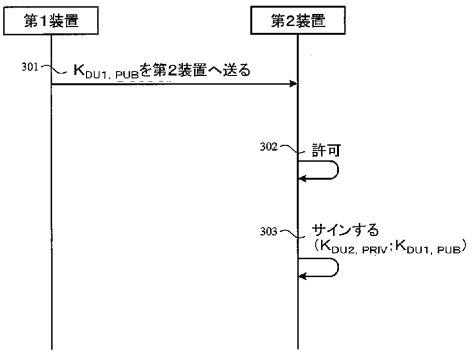
【図１】



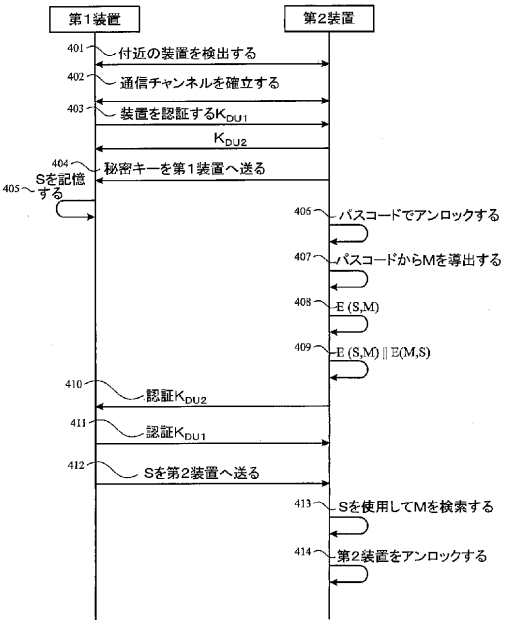
【図２】



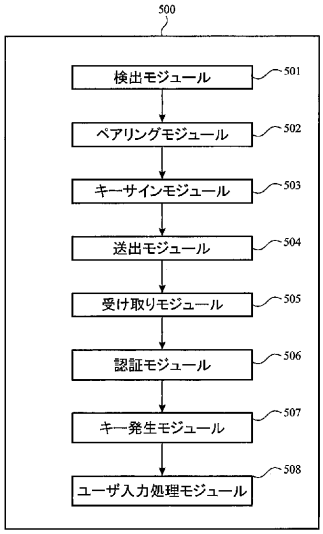
【図３】



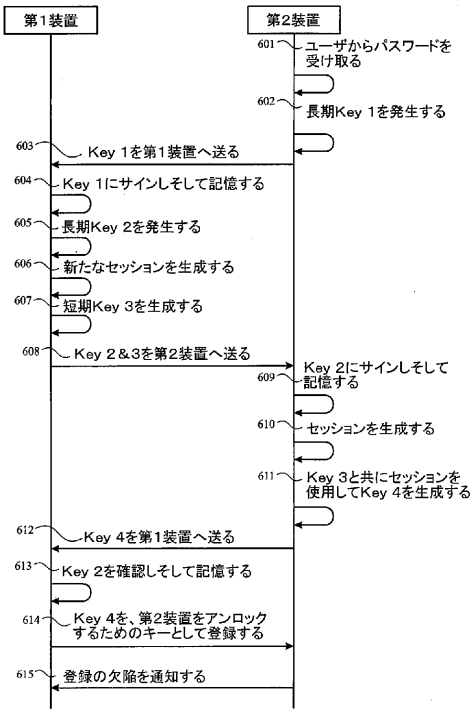
【図４】


第1装置
第2装置
401 付近の装置を検出する
402 通信チャンネルを確立する
403 装置を認証するK_DU1
K_DU2
404 秘密キーを第1装置へ送る
405 Sを記憶する
405 パスコードでアンロックする
407 パスコードからMを導出する
408 E(S,M)
409 E(S,M)||E(M,S)
410 認証K_DU2
411 認証K_DU1
412 Sを第2装置へ送る
413 Sを使用してMを検索する
414 第2装置をアンロックする

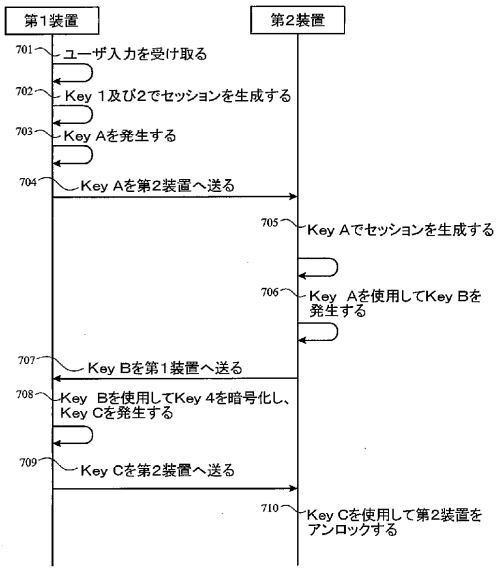
【図５】


500
検出モジュール 501
ペアリングモジュール 502
キーサインモジュール 503
送出モジュール 504
受け取りモジュール 505
認証モジュール 506
キー発生モジュール 507
ユーザ入力処理モジュール 508

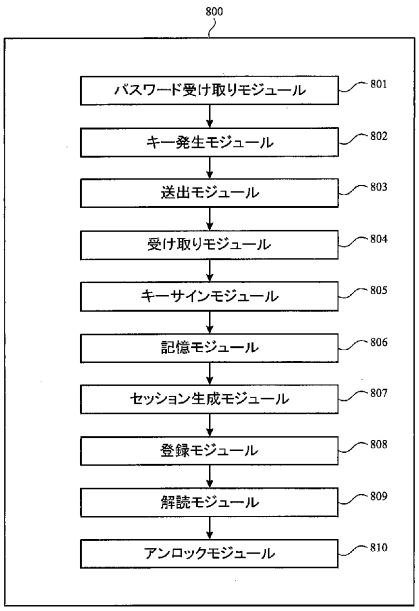
【図６】


第1装置
第2装置
601 ユーザからパスワードを受け取る
602 長期Key 1を発生する
603 Key 1を第1装置へ送る
604 Key 1にサインしそして記憶する
605 長期Key 2を発生する
606 新たなセッションを生成する
607 短期Key 3を生成する
608 Key 2&3を第2装置へ送る
609 Key 2にサインしそして記憶する
610 セッションを生成する
611 Key 3と共にセッションを使用してKey 4を生成する
612 Key 4を第1装置へ送る
613 Key 2を確認しそして記憶する
614 Key 4を、第2装置をアンロックするためのキーとして登録する
615 登録の欠陥を通知する

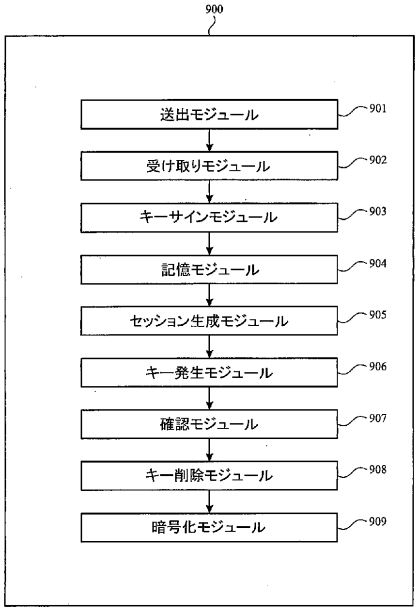
【図７】


第1装置
第2装置
701 ユーザ入力を受け取る
702 Key 1及び2でセッションを生成する
703 Key Aを発生する
704 Key Aを第2装置へ送る
705 Key Aでセッションを生成する
706 Key Aを使用してKey Bを発生する
707 Key Bを第1装置へ送る
708 Key Bを使用してKey 4を暗号化し、Key Cを発生する
709 Key Cを第2装置へ送る
710 Key Cを使用して第2装置をアンロックする

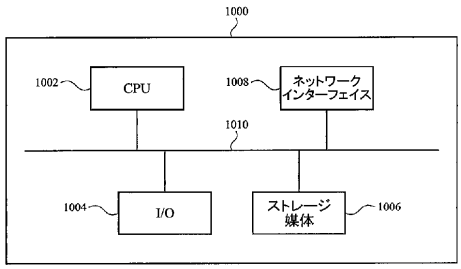
【図８】


800
パスワード受け取りモジュール
801
キー発生モジュール
802
送出モジュール
803
受け取りモジュール
804
キーサインモジュール
805
記憶モジュール
806
セッション生成モジュール
807
登録モジュール
808
解読モジュール
809
アンロックモジュール
810

【図９】


900
送出モジュール
901
受け取りモジュール
902
キーサインモジュール
903
記憶モジュール
904
セッション生成モジュール
905
キー発生モジュール
906
確認モジュール
907
キー削除モジュール
908
暗号化モジュール
909

【図１０】


1000
1002
CPU
1008
ネットワーク
インターフェイス
1010
1004
I/O
ストレージ
媒体
1006

フロントページの続き

(74)代理人 100086771
弁理士 西島 孝喜
(74)代理人 100122563
弁理士 越柴 絵里
(72)発明者 コンラッド サウアーヴァルト
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス ３０１－２シーオーエス アップル インコーポレイテッド内
(72)発明者 アレクサンダー レッドウィズ
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス ３０２－４エイピーピー アップル インコーポレイテッド内
(72)発明者 ジョン ジェイ イアロッチ
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ アップル インコーポレイテッド内
(72)発明者 マルク ジェイ クロクマル
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ アップル インコーポレイテッド内
(72)発明者 ウェイド ベンソン
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス ３－シーオーエス アップル インコーポレイテッド内
(72)発明者 グレゴリー ノヴィック
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス ６０－２イーティーエフ アップル インコーポレイテッド内
(72)発明者 ノア エイ ウィザースプーン
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ インフィニット ループ １ エムエス ６０－２イーティーエフ アップル インコーポレイテッド内

審査官 中里 裕正

(56)参考文献 特開２０１４－１２３２０４（ＪＰ，Ａ）
特開２０１２－１０８６９８（ＪＰ，Ａ）
特開２００６－３１１２９１（ＪＰ，Ａ）
特開２００４－１５７８７３（ＪＰ，Ａ）
特表２００７－５３５８２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／０８