

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2018-201217

(P2018-201217A)

(43) 公開日 平成30年12月20日 (2018. 12. 20)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 9/32 (2006.01)	H04L 9/00 675A	5J104
G09C 1/00 (2006.01)	G09C 1/00 640E	
H04L 9/08 (2006.01)	H04L 9/00 601C	

審査請求 有 請求項の数 22 O L 外国語出願 (全 23 頁)

(21) 出願番号	特願2018-144795 (P2018-144795)	(71) 出願人	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, Californ ia 95014, U. S. A.
(22) 出願日	平成30年8月1日 (2018. 8. 1)	(74) 代理人	100094569 弁理士 田中 伸一郎
(62) 分割の表示	特願2016-189123 (P2016-189123) の分割	(74) 代理人	100088694 弁理士 弟子丸 健
原出願日	平成27年8月27日 (2015. 8. 27)	(74) 代理人	100067013 弁理士 大塚 文昭
(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	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	米国 (US)		

最終頁に続く

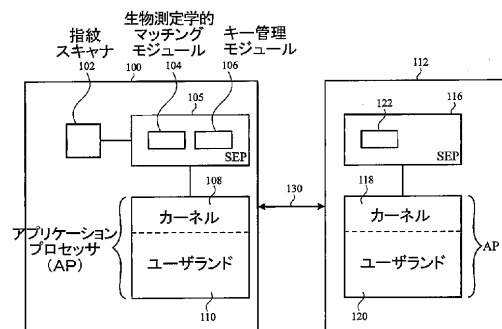
(54) 【発明の名称】 ある装置を使用して別の装置をアンロックする方法

(57) 【要約】 (修正有)

【課題】 第1装置を使用して第2装置をアンロックする方法を提供する。

【解決手段】 第1装置100は、第2装置112とペアリングした後、第2装置と相互認証を行い、第2装置との信頼関係を確立する。ここで第2装置は、装置キーを使用して第1装置を認証する。第1装置は、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、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。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装置キーを認証することを含む。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

第 1 装置から第 2 装置をアンロックする方法であって、
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。

10

【請求項 2】

前記第 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、請求項 1 に記載の方法。

【請求項 3】

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、請求項 2 に記載の方法。

【請求項 4】

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 装置へ送送することを含む、請求項 1 に記載の方法。

20

【請求項 5】

前記第 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パブリックキーを有効なものとするを更に含む、請求項 4 に記載の方法。

【請求項 6】

前記第 2 装置に関連した装置キーを使用して前記第 2 装置を認証することを更に含む、請求項 1 に記載の方法。

【請求項 7】

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であって、
第 1 装置からパブリック装置キーを受け取り、
前記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、

30

第 1 装置へ秘密キーを伝送し、
パスコードを受け取り、
前記パスコードからマスターキーを導出し、
前記秘密キーで前記マスターキーを暗号化し、
第 1 装置から前記秘密キーを受け取り、
前記受け取った秘密キーを使用して前記マスターキーを検索し、及び
前記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。

40

【請求項 8】

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、請求項 7 に記載の方法。

【請求項 9】

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、請求項 7 に記載の方法。

【請求項 10】

前記秘密キーは、ランダムキーを含む、請求項 7 に記載の方法。

【請求項 11】

前記秘密装置キーは、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

50

るよう構成される、請求項 7 に記載の方法。

【請求項 1 2】

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であって、プロセッサの実行時に、

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命令を記憶した記憶媒体。

10

【請求項 1 3】

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を検出することを更に含む、請求項 1 2 に記載の記憶媒体。

【請求項 1 4】

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、請求項 1 2 に記載の記憶媒体。

【請求項 1 5】

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、請求項 1 4 に記載の記憶媒体。

【請求項 1 6】

20

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、請求項 1 2 に記載の記憶媒体。

【請求項 1 7】

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であって、プロセッサの実行時に、

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、

30

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命令を記憶した記憶媒体。

【請求項 1 8】

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、請求項 1 7 に記載の記憶媒体。

【請求項 1 9】

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、請求項 1 7 に記載の記憶媒体。

40

【請求項 2 0】

第 2 装置をアンロックすることのできる第 1 装置であって、

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よう構成された送出モジュールと、

50

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。

【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ン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

10

20

30

40

50

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；ユーザ入力に回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。

【 0 0 0 7 】

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。

10

【 図面の簡単な説明 】

【 0 0 0 8 】

【 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。

20

【 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。

30

【 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 1 0 】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 】

【 0 0 0 9 】

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。

40

【 0 0 1 0 】

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。

【 0 0 1 1 】

図 1 は、第 1 装置 1 0 0 及び第 2 装置 1 1 2 を示す。この実施形態では、第 1 装置 1 0 0 は、第 2 装置 1 1 2 をアンロックするのに使用される。第 1 装置は、例えば、スマートフォン、タブレット P C、ラップトップ、デスクトップ P C、M a c、電子リーダー、スマ

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

一)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。

10

【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。

20

【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時に入手できる)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。

30

40

【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なく、装置がユーザにより以前にアンロックされていた

50

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。

10

20

30

40

50

【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。まず、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、QR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。まず、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、許可もを行い、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。

10

【0027】

登録が首尾良く終わった場合には、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。まず、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。

20

30

40

【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ン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

50

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、まず、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

10

20

30

40

50

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。

10

【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ため、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。

20

30

【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。

40

【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

50

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。

10

【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。

20

【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。

30

【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ク（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）

40

50

(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。

10

【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装置へ送付することを含み。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。

20

30

40

【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；ことを含み方法、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

50

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を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。

10

20

【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。

30

【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更に含む、第1装置に向けられる。

40

【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；

50

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。

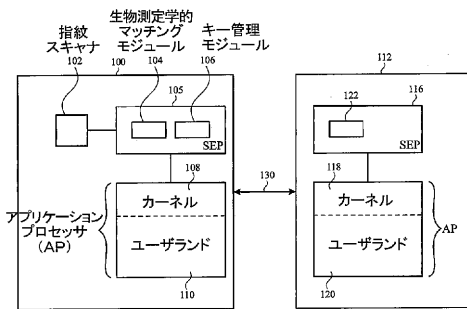
【符号の説明】

【0049】

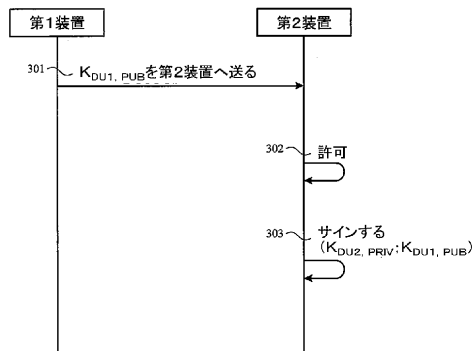
100	：第1装置	
102	：指紋スキャナ	
104	：生物測定学的マッチングモジュール	
105	：セキュアなエンクレーププロセッサ (S E P)	
106、122	：キー管理モジュール	
108、118	：カーネル	
110、120	：ユーザランド	
112	：第2装置	
500	：装置	
501	：検出モジュール	20
502	：ペアリングモジュール	
503	：キーサインモジュール	
504	：送出モジュール	
505	：受け取りモジュール	
506	：認証モジュール	
507	：キー発生モジュール	
508	：ユーザ入力処理モジュール	
800	：第2装置	
801	：パスワード受け取りモジュール	
802	：キー発生モジュール	30
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	40
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 (C P U)	50

- 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

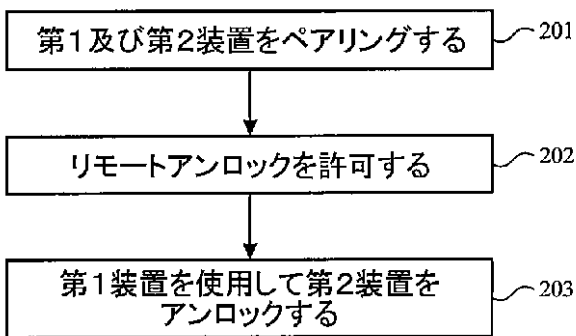
【図1】



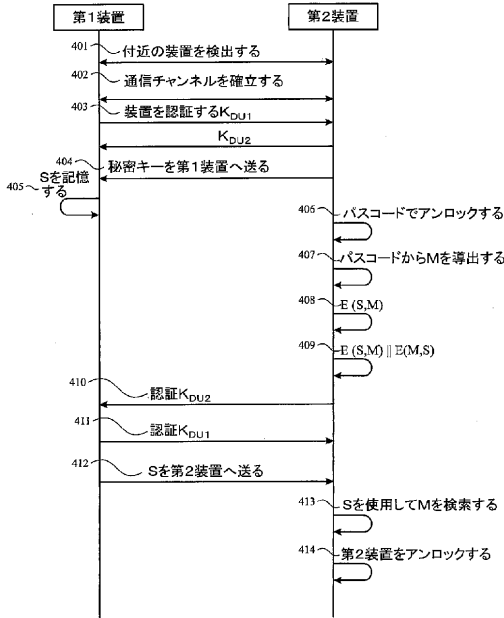
【図3】



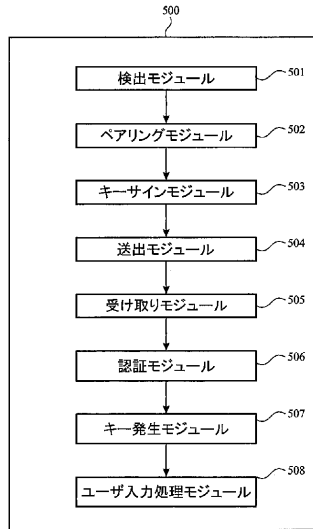
【図2】



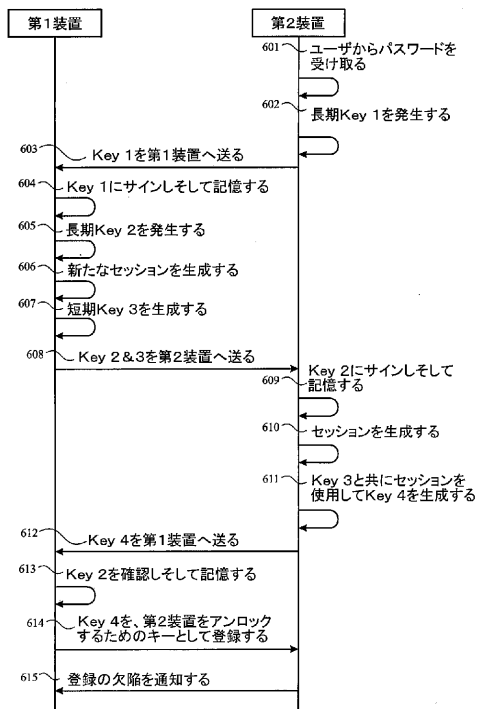
【 図 4 】



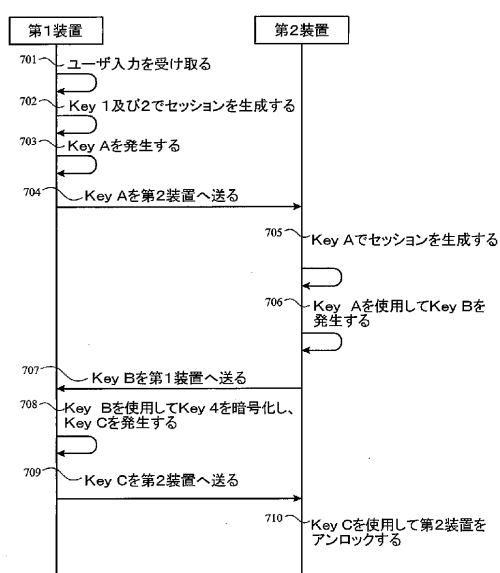
【 図 5 】



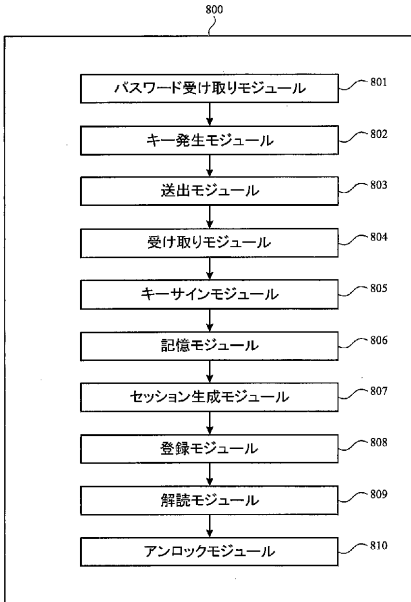
【 図 6 】



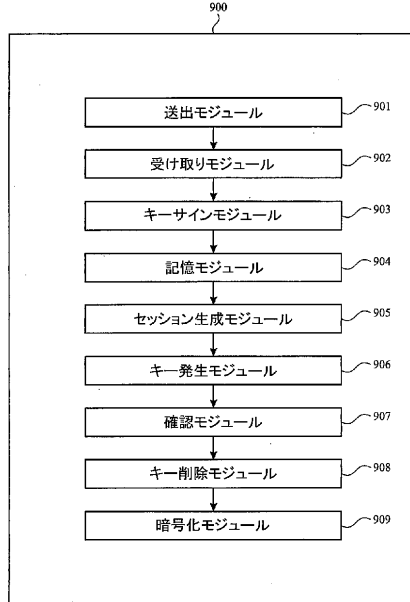
【 図 7 】



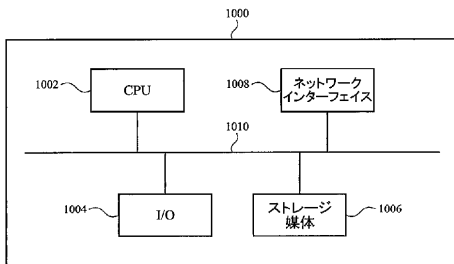
【 図 8 】



【 図 9 】



【 図 10 】



【手続補正書】

【提出日】平成30年8月31日(2018.8.31)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

第1装置から第2装置をアンロックする方法であって、
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み、方法。

【手続補正書】

【提出日】平成30年9月11日(2018.9.11)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

第1装置と第2装置をペ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ตอบสนอง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ตอบสนอง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ตอบสนอง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ตอบสนอง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ตอบสนอง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ตอบสนอง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ตอบสนอง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。

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

Fターム(参考) 5J104 AA07 AA16 EA17 KA02 KA04

【外国語明細書】

2018201217000001.pdf