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

特許第6237363号
(P6237363)

(45)発行日　平成29年11月29日(2017.11.29)　(24)登録日　平成29年11月10日(2017.11.10)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601C
H04L	9/10	(2006.01)	H04L	9/00	621A

請求項の数 12　(全 23 頁)

(21)出願番号	特願2014-52006(P2014-52006)
(22)出願日	平成26年3月14日(2014.3.14)
(65)公開番号	特開2015-177329(P2015-177329A)
(43)公開日	平成27年10月5日(2015.10.5)
審査請求日	平成28年2月4日(2016.2.4)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎
(72)発明者　作本　紘一
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法及びコンピュータプログラム

(57)【特許請求の範囲】

【請求項１】

所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得するセンサデータ取得部と、

前記センサデータ取得部が所定の期間において取得した前記情報に基づいて、認証処理に用いられる鍵情報を生成する鍵生成部と、

前記センサからの前記情報の取得が完了するまでの進捗情報を算出する進捗情報算出部と、

を備え、

前記センサデータ取得部は、前記情報を取得してから、前記所定の期間の前に前記センサからの情報の平均取得間隔を用いて決定した所定時間が経過した後に新たな前記情報を取得する、情報処理装置。

【請求項２】

前記進捗情報算出部は、前記鍵生成部での鍵情報の生成に用いられる前記情報の取得が完了するまでの進捗情報を算出する、請求項１に記載の情報処理装置。

【請求項３】

前記進捗情報算出部が算出した進捗情報を出力する出力部をさらに備える、請求項１または２に記載の情報処理装置。

【請求項４】

前記センサデータ取得部が取得した前記情報は前記鍵生成部での鍵情報の生成に有効な

情報か否かを判定する判定部をさらに備える、請求項１～３のいずれかに記載の情報処理装置。
【請求項５】
前記判定部は、前記センサデータ取得部が取得した前記情報の単位時間あたりの変化量を用いて判定する、請求項４に記載の情報処理装置。
【請求項６】
前記判定部は、前記センサデータ取得部が取得した前記情報の絶対値を用いて判定する、請求項４に記載の情報処理装置。
【請求項７】
前記センサデータ取得部が取得する前記情報は、加速度情報である、請求項１～６のいずれかに記載の情報処理装置。
【請求項８】
前記鍵生成部は、前記センサデータ取得部が取得した前記情報と、自装置固有の情報を用いて鍵情報を生成する、請求項１～７のいずれかに記載の情報処理装置。
【請求項９】
前記鍵生成部が生成する鍵情報は秘密鍵である、請求項１～８のいずれかに記載の情報処理装置。
【請求項１０】
所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得するセンサデータ取得部と、
前記センサデータ取得部が所定の期間において取得した前記情報に基づいて、認証処理に用いられる鍵情報を生成する鍵生成部と、
前記鍵生成部での鍵情報の生成に用いられる前記情報の取得が完了するまでの進捗情報を算出する進捗情報算出部と、
を備え、
前記センサデータ取得部は、前記情報を取得してから、前記所定の期間の前に前記センサからの情報の平均取得間隔を用いて決定した所定時間が経過した後に新たな前記情報を取得する、情報処理装置。
【請求項１１】
所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得することと、
所定の期間において取得された前記情報に基づいて、認証処理に用いられる鍵情報を生成することと、
前記センサからの前記情報の取得が完了するまでの進捗情報を算出することと、
前記情報を取得してから、前記所定の期間の前に前記センサからの情報の平均取得間隔を用いて決定した所定時間が経過した後に新たな前記情報を取得することと、
を含む、情報処理方法。
【請求項１２】
コンピュータに、
所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得することと、
所定の期間において取得された前記情報に基づいて、認証処理に用いられる鍵情報を生成することと、
前記センサからの前記情報の取得が完了するまでの進捗情報を算出することと、
前記情報を取得してから、前記所定の期間の前に前記センサからの情報の平均取得間隔を用いて決定した所定時間が経過した後に新たな前記情報を取得することと、
を実行させる、コンピュータプログラム。

【発明の詳細な説明】

【技術分野】
【０００１】
本開示は、情報処理装置、情報処理方法及びコンピュータプログラムに関する。
【背景技術】
【０００２】
電子データの暗号化、装置やサービスの利用時の認証、電子署名等の暗号技術に利用される秘密情報（鍵）は、他者から推測されない値でなければならない。秘密情報をユーザや装置ごとに自力で生成する際には、その秘密情報は、秘密情報を生成するプログラムのリバースエンジニアリングによっても、予測の付かない値となることが望ましい。
【０００３】
そのような秘密情報をユーザや装置ごとに自力で生成する技術として、例えば特許文献１～４が開示されている。下記特許文献１～４は、情報処理装置の姿勢、勢い、加速度等の情報をセンシングし、その情報を秘密情報の生成の際のランダムネスとして用いて秘密情報を生成し、また他の装置と共有する技術が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１１－１３０２２４号公報
【特許文献２】特開２０１０－１８７２８２号公報
【特許文献３】特開２００８－３１１７２６号公報
【特許文献４】国際公開第２００８／０７５６３８号
【発明の概要】
【発明が解決しようとする課題】
【０００５】
上記特許文献で開示されている技術は、複数の装置で同時にセンシングした情報に基づいて、同じ秘密情報を共有するものである。秘密情報を複数の装置で共有する際には、その複数の装置で秘密情報が同じにならなければならない。複数の装置で共有される秘密情報を、センシングした情報に基づいて生成する場合には、センサの個体差の影響があるため、センシングした情報を各装置で完全に一致させることが困難であり、センシングした情報を解析して装置間で類似する情報を用いて秘密情報を生成している。
【０００６】
従って、わずかに違うデータがセンシングされても、生成される秘密情報は同一になると考えられる。このようにセンシングした情報を解析して類似する情報を用いる方法では、センシングした情報を秘密情報の生成の際のランダムネスとして用いる場合には望ましくない。
【０００７】
そこで本開示では、秘密情報の生成の際のランダムネスとしてセンシングした情報を用いる際に、ユーザの負担が少なく、かつ手軽に充分なランダムネスを得ることが可能な、新規かつ改良された情報処理装置、情報処理方法及びコンピュータプログラムを提案する。
【課題を解決するための手段】
【０００８】
本開示によれば、所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得するセンサデータ取得部と、前記センサデータ取得部が所定の期間において取得した前記情報に基づいて、認証処理に用いられる鍵情報を生成する鍵生成部と、を備える、情報処理装置が提供される。
【０００９】
また本開示によれば、所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得することと、所定の期間において取得された前記情報に基づいて、認証処理に用いられる鍵情報を生成することと、を含む、情報処理方法が提供される。

【００１０】
また本開示によれば、コンピュータに、所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得することと、所定の期間において取得された前記情報に基づいて、認証処理に用いられる鍵情報を生成することと、を実行させる、コンピュータプログラムが提供される。
【発明の効果】
【００１１】
以上説明したように本開示によれば、秘密情報の生成の際のランダムネスとしてセンシングした情報を用いる際に、ユーザの負担が少なく、かつ手軽に充分なランダムネスを得る、新規かつ改良された情報処理装置、情報処理方法及びコンピュータプログラムが提供される。
【００１２】
なお、上記の効果は必ずしも限定的なものではなく、上記の効果とともに、または上記の効果に代えて、本明細書に示されたいずれかの効果、または本明細書から把握され得る他の効果が奏されてもよい。
【図面の簡単な説明】
【００１３】
【図１】本開示の一実施形態に係る情報処理装置１００の機能構成例を示す説明図である。
【図２】本開示の一実施形態に係る情報処理装置１００に含まれる制御部１１０の機能構成例を示す説明図である。
【図３】本開示の一実施形態に係る情報処理装置１００の動作例を示す流れ図である。
【図４】本開示の一実施形態に係る情報処理装置１００が出力部１３０に出力する画面の例を示す説明図である。
【図５】本開示の一実施形態に係る情報処理装置１００が出力部１３０に出力する画面の例を示す説明図である。
【図６】本開示の一実施形態に係る情報処理装置１００が出力部１３０に出力する画面の例を示す説明図である。
【図７】３軸の加速度センサからの出力データの一例をグラフで示す説明図である。
【図８】３軸の加速度センサからの出力データの、単位時間あたりの変化量の一例をグラフで示す説明図である。
【図９】本開示の一実施形態に係る情報処理装置１００の動作例を示す流れ図である。
【図１０】本開示の一実施形態に係る情報処理装置１００の動作例を示す流れ図である。
【図１１】本開示の一実施形態に係る情報処理装置１００の動作例を示す流れ図である。
【図１２】ハードウェア構成例を示す説明図である。
【発明を実施するための形態】
【００１４】
以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
【００１５】
なお、説明は以下の順序で行うものとする。
１．本開示の一実施形態
　１．１．情報処理装置の機能構成例
　１．２．情報処理装置の動作例
２．ハードウェア構成例
３．まとめ
【００１６】
＜１．本開示の一実施形態＞
［１．１．情報処理装置の機能構成例］

まず、図面を参照しながら本開示の一実施形態に係る情報処理装置の機能構成例について説明する。図１は、本開示の一実施形態に係る情報処理装置１００の機能構成例を示す説明図である。以下、図１を用いて本開示の一実施形態に係る情報処理装置１００の機能構成例について説明する。

【００１７】

図１に示した情報処理装置１００は、例えばスマートフォン、タブレット型端末、携帯電話、ＰＨＳのような機器であってもよく、腕時計型、リストバンド型、指輪型、メガネ型その他のウェアラブルデバイス、キーホルダー型の機器等の装置であってもよい。図１に示した情報処理装置１００は、電子データの暗号化、装置やサービスの利用時の認証、電子署名等の暗号技術に利用される秘密情報（秘密鍵）を、ユーザに振ってもらうことによって得られるセンサデータを用いて生成する装置である。

【００１８】

図１に示したように、本開示の一実施形態に係る情報処理装置１００は、制御部１１０と、入力部１２０と、出力部１３０と、通信部１４０と、記憶部１５０と、センサ部１６０と、を含んで構成される。

【００１９】

制御部１１０は、情報処理装置１００の動作を制御する。すなわち、図１に示した情報処理装置１００の各構成要素は、制御部１１０の制御により動作する。制御部１１０は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、不揮発性メモリ部、インターフェース部を備えたマイクロコンピュータにより構成され、本実施形態の全体を制御する制御部として機能し得る。本実施形態では、制御部１１０は、ユーザが情報処理装置１００を振ったことに応じて得られるセンサデータを用いて鍵情報（例えば共通鍵暗号方式における共通鍵や、公開鍵暗号方式における秘密鍵）を生成する機能を有する。なお、制御部１１０の詳細な機能構成例については後述する。

【００２０】

入力部１２０は、ユーザの入力操作を受け付ける入力デバイスである。入力部１２０を構成するものとしては、例えばタッチパネル、キーボード、電源ボタン、操作ボタン、マイク等があり得る。

【００２１】

出力部１３０は、情報処理装置１００で処理された情報を出力する出力デバイスである。出力部１３０を構成するものとしては、例えば液晶ディスプレイ、有機ＥＬディスプレイ、スピーカ、ＬＥＤインジケータ、バイブレータ等があり得る。出力部１３０からの出力内容は、例えば制御部１１０によって生成され得る。

【００２２】

通信部１４０は、外部機器との間でデータの送受信を行う。外部機器としては、コンピュータ装置、スマートフォン、スマートウォッチ、ネットワークサーバ装置などが想定される。通信部１４０は、無線ＬＡＮ、ブルートゥース（登録商標）などの方式で、例えばネットワークアクセスポイントに対する近距離無線通信を介してネットワーク通信を行う構成としても良いし、対応する通信機能を備えた外部機器との間で直接無線通信を行う構成としても良い。通信部１４０は、制御部１１０が生成した秘密鍵を用いた、外部機器との間の認証処理に関する情報を送受信する。なお通信部１４０は、外部機器との間の認証処理に関する情報の他にも、例えば動画コンテンツ、静止画コンテンツ、電子書籍等のデータ、情報処理装置１００で生成された画像データ、テキストデータ、表計算データ等のコンピュータユースのデータ、ゲーム画像など、表示対象となるあらゆるデータを通信対象とし得る。

【００２３】

記憶部１５０は、例えばＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、不揮発性メモリ部等で構成され得る。記憶部１５０は、制御部１１０が情報処理装置１００の制御に用いる情報や、情報処理装置１０

０で生成された画像データ、テキストデータ、表計算データ等のコンピュータユースのデータ、情報処理装置１００で実行されるアプリケーションのデータ等を格納する。また記憶部１５０は、制御部１１０が生成した秘密鍵を格納する。制御部１１０が生成した秘密鍵が格納される記憶部１５０の領域は、耐タンパ性を有することが望ましい。

【００２４】

センサ部１６０は、情報処理装置１００の動きを検出するセンサである。センサ部１６０は、例えば加速度センサ、重力センサ、ジャイロセンサ、照度センサ、線形加速度センサ、地磁気センサ、近接センサ、回転ベクトルセンサ等のセンサで構成され得る。センサ部１６０のセンシングによって得られるセンサデータは、制御部１１０で取得される。本実施形態では、センサ部１６０のセンシングによって得られるセンサデータが、制御部１１０での秘密鍵の生成に用いられる。センサ部１６０のセンシングによって得られるセンサデータを制御部１１０での秘密鍵の生成に用いることで、本開示の一実施形態に係る情報処理装置１００は、秘密鍵の生成の際にユーザの負担を軽減させ、かつ秘密鍵の生成の際に手軽に充分なランダムネスを得ることが出来る。

【００２５】

以上、図１を用いて本開示の一実施形態に係る情報処理装置１００の機能構成例について説明した。続いて、本開示の一実施形態に係る情報処理装置１００に含まれる制御部１１０の機能構成例について説明する。

【００２６】

図２は、本開示の一実施形態に係る情報処理装置１００に含まれる制御部１１０の機能構成例を示す説明図である。以下、図２を用いて本開示の一実施形態に係る情報処理装置１００に含まれる制御部１１０の機能構成例について説明する。

【００２７】

図２に示したように、制御部１１０は、センサデータ取得部１１１と、判定部１１２と、進捗情報算出部１１３と、鍵生成部１１４と、出力制御部１１５と、を含んで構成される。

【００２８】

センサデータ取得部１１１は、センサ部１６０のセンシングによって得られるセンサデータを取得する。センサデータ取得部１１１は、所定の期間において、センサ部１６０のセンシングによって得られるセンサデータを取得してもよい。例えばセンサデータ取得部１１１は、ユーザがセンサデータの取得開始を指示してからセンサデータの取得を開始しても良い。センサデータの取得開始指示は、例えば、後述の出力制御部１１５の制御によって出力部１３０から出力される画面に対するユーザの操作に基づいて発生し得る。出力制御部１１５の制御によって出力部１３０から出力される画面の例については後述する。そして、センサデータ取得部１１１がセンサ部１６０から取得したセンサデータは、判定部１１２、進捗情報算出部１１３、鍵生成部１１４、出力制御部１１５での処理に、それぞれ用いられ得る。

【００２９】

判定部１１２は、センサデータ取得部１１１が取得したセンサデータを用いて、そのセンサデータが、後述の進捗情報算出部１１３での進捗率の算出に有効なデータであるかどうかを判定する。進捗情報算出部１１３での進捗率の算出に有効なデータであるかを判定することで、判定部１１２は、センサデータ取得部１１１が取得したセンサデータが、ユーザが情報処理装置１００を振ったことで得られたセンサデータなのかどうか、または単なるノイズに起因するものなのかどうかを判定することが可能となる。

【００３０】

例えば、センサデータ取得部１１１が取得したセンサデータが３軸の加速度センサから取得したデータである場合、判定部１１２は、各軸について値の絶対値が所定の閾値を超えている場合、その時点でユーザが情報処理装置１００を振ったと判断してもよい。また判定部１１２は、各軸について値の単位時間あたりの変化量の絶対値が所定の閾値を超えている場合、その時点でユーザが情報処理装置１００を振ったと判断してもよい。判定部

１１２のセンサデータに対する判定結果は、進捗情報算出部１１３、鍵生成部１１４、出力制御部１１５での処理に、それぞれ用いられ得る。

【００３１】

進捗情報算出部１１３は、鍵生成部１１４での秘密鍵の生成に用いられる情報の取得が完了するまでの進捗情報を算出する。進捗情報算出部１１３は、進捗情報として、例えば鍵生成部１１４での秘密鍵の生成に用いられるセンサデータがどの程度まで取得できているかを意味する進捗率を算出する。以下では、進捗情報算出部１１３は、進捗情報として進捗率ｐを算出するとして説明する。進捗情報算出部１１３による進捗率の算出処理の一例を挙げれば、例えば以下の通りである。

【００３２】

進捗情報算出部１１３は、進捗率ｐを算出するにあたって、例えば単位時間あたりに所定の値を加算する。例えば進捗情報算出部１１３は、１秒毎に５％、進捗率ｐに加算する。そして進捗情報算出部１１３は、単位時間あたりに所定の値を加算する処理に加え、センサデータ取得部１１１が取得したセンサデータが、進捗情報算出部１１３での進捗率の算出に有効なデータであると判定部１１２で判定されると、その判定毎に、所定の値をさらに加算する。例えば進捗情報算出部１１３は、進捗情報算出部１１３での進捗率の算出に有効なデータであると判定部１１２で判定される毎に所定の値（例えば、１％）を進捗率ｐに加算する。すなわち、センサデータ取得部１１１が取得したセンサデータが、進捗情報算出部１１３での進捗率の算出に有効なデータであると判定部１１２で判定されればされるほど、進捗情報算出部１１３は、進捗率ｐが上昇するように進捗率ｐを算出する。そして進捗情報算出部１１３が算出する進捗率ｐが１００％に達すると、センサデータ取得部１１１がセンサデータの取得を開始してから、進捗率ｐが１００％になった時点までのセンサデータが鍵生成部１１４に送られる。もちろん、センサデータ取得部１１１は、取得したセンサデータを鍵生成部１１４に逐次送り、鍵生成部１１４は、進捗情報算出部１１３によって進捗率ｐが１００％に達した時点までのセンサデータを用いて鍵を生成するようにしてもよい。

【００３３】

進捗情報算出部１１３が算出する進捗率ｐの情報は、出力制御部１１５にも逐次送られ得る。出力制御部１１５は、進捗情報算出部１１３が算出する進捗率ｐの情報を用いて状況をリアルタイムで出力部１３０から提示する制御を実行し得る。

【００３４】

鍵生成部１１４は、センサデータ取得部１１１が取得したセンサデータを用いた秘密鍵の生成処理を実行する。鍵生成部１１４は、センサデータ取得部１１１がセンサデータの取得を開始してから、進捗情報算出部１１３が算出する進捗率ｐが１００％になった時点までのセンサデータの値を用いた演算処理により、秘密鍵を生成する。鍵生成部１１４による秘密鍵の生成処理の一例を挙げれば、以下の通りである。

【００３５】

鍵生成部１１４は、センサデータ取得部１１１が取得したセンサデータの各取得時の値に、情報処理装置１００に固有の情報、例えばＭＡＣアドレスを連結し、その連結後のデータをＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ）等で圧縮することで、秘密鍵を生成してもよい。また鍵生成部１１４は、センサデータ取得部１１１が取得したセンサデータの各取得時の値を連結したビット列をエントロピーとして設定し、擬似乱数生成アルゴリズムのシードを初期化、またはリシードし、その初期化、またはリシードされた乱数シードを基に擬似乱数生成アルゴリズムを適用して生成した乱数を秘密鍵としてもよい。なお、擬似乱数生成アルゴリズムの例としては、ＮＩＳＴ　ＳＰ８００－９０Ａ等のＤＲＢＧ（Ｄｅｔｅｒｍｉｎｉｓｔｉｃ　Ｒａｎｄｏｍ　Ｂｉｔ　Ｇｅｎｅｒａｔｏｒ；決定性乱数生成器）がある。このアルゴリズムは、シード初期化、リシード、乱数生成の３つから構成される。シード初期化とは、エントロピーなどを入力し、乱数を生成するためのシードを初期化することである。リシードとは、現在のシードに、エントロピーを追加することで、新たなシードに更新することである。乱数生成とは、乱数シードを入力

し、実際に乱数を生成することである。

【００３６】

出力制御部１１５は、出力部１３０で提示する各種情報の出力を制御する。例えば出力制御部１１５は、センサデータ取得部１１１が取得したセンサデータや、進捗情報算出部１１３が算出した進捗情報に基づく情報を出力部１３０から出力するための制御を実行する。出力制御部１１５は、センサデータ取得部１１１が取得したセンサデータや、進捗情報算出部１１３が算出した進捗情報に基づく情報を出力部１３０から出力するための制御を実行することで、ユーザに対してセンサデータの状態や、秘密鍵の作成処理の進捗状況を分かりやすく提示することができる。出力制御部１１５によって出力部１３０から出力される情報の例は後に詳述する。

【００３７】

本開示の一実施形態に係る制御部１１０は、図２に示したような構成を有することで、ユーザが情報処理装置１００を振ったり、情報処理装置１００に振動を加えたりしたことに応じて得られるセンサデータを用いた秘密鍵の生成を可能にする。また本開示の一実施形態に係る制御部１１０は、図２に示したような構成を有することで、ユーザに対してセンサデータの状態や、秘密鍵の作成処理の進捗状況を分かりやすく提示することができる。

【００３８】

以上、図２を用いて本開示の一実施形態に係る情報処理装置１００に含まれる制御部１１０の機能構成例について説明した。続いて、本開示の一実施形態に係る情報処理装置１００の動作例について説明する。

【００３９】

［１．２．情報処理装置の動作例］

図３は、本開示の一実施形態に係る情報処理装置１００の動作例を示す流れ図である。図３に示したのは、ユーザが情報処理装置１００を振ったり、情報処理装置１００に振動を加えたりしたことに応じて得られるセンサデータを用いた秘密鍵の生成処理を実行する際の、情報処理装置１００の動作例である。以下、図３を用いて本開示の一実施形態に係る情報処理装置１００の動作例について説明する。

【００４０】

情報処理装置１００は、ユーザが情報処理装置１００を振らせたり、情報処理装置１００に振動を加えさせたりすることに応じて得られるセンサデータを用いた秘密鍵の生成処理を実行するにあたり、出力部１３０へ所定の処理開始画面を出力する（ステップＳ１０１）。ステップＳ１０１の処理開始画面の出力処理は、例えば出力制御部１１５が実行し得る。また、出力部１３０に出力される所定の処理開始画面は、例えば秘密鍵を生成するアプリケーションの実行によって出力部１３０に出力されるものであり得る。

【００４１】

図４は、本開示の一実施形態に係る情報処理装置１００が出力部１３０に出力する処理開始画面の例を示す説明図である。図４に示したのは、情報処理装置１００が秘密鍵を生成するアプリケーションを実行したことによって出力部１３０に出力される画面の一例である。図４に示した画面には、キャンセルボタン１２１と、開始ボタン１２２と、が表示されている。開始ボタン１２２は、情報処理装置１００で鍵生成処理を開始させるためのボタンであり、ユーザが開始ボタン１２２をタッチしたことを検出すると、情報処理装置１００は鍵生成処理を開始する。一方のキャンセルボタン１２１は、秘密鍵を生成するアプリケーションを終了するためのボタンである。ユーザがキャンセルボタン１２１をタッチしたことを検出すると、情報処理装置１００は秘密鍵を生成するアプリケーションを終了する。本開示の一実施形態に係る情報処理装置１００は、図４に示したような処理開始画面を出力部１３０に出力することで、ユーザに鍵生成処理を開始させることが出来る。

【００４２】

なお図４に示したような処理開始画面が出力部１３０に出力されている際に、ユーザが開始ボタン１２２をタッチしたことを検出しなくても、ユーザが所定の加速度以上で情報

処理装置１００を振ったことを、センサデータ取得部１１１が取得したセンサデータから判定すると、情報処理装置１００は鍵生成処理を開始するようにしてもよい。

【００４３】

ステップＳ１０１で処理開始画面を出力し、ユーザが鍵生成処理の開始を情報処理装置１００に通知すると、情報処理装置１００は、センサ部１６０で取得される加速度データを逐次取得する（ステップＳ１０２）。ステップＳ１０２の加速度データの取得処理は、例えばセンサデータ取得部１１１が実行し得る。

【００４４】

上記ステップＳ１０２で、センサ部１６０で取得される加速度データを逐次取得すると、続いて情報処理装置１００は、時間の経過や、加速度データの取得状況に応じて進捗率ｐを増加させる（ステップＳ１０３）。ステップＳ１０３の進捗率ｐの算出処理は、例えば進捗情報算出部１１３が実行し得る。

【００４５】

情報処理装置１００は、ステップＳ１０３での進捗率ｐの算出にあたって、例えば単位時間あたりに所定の値を加算する。例えば情報処理装置１００は、ステップＳ１０３での進捗率ｐの算出にあたって、１秒毎に５％、進捗率ｐに加算する。そして情報処理装置１００は、単位時間あたりに所定の値を加算する処理に加え、センサデータ取得部１１１が取得したセンサデータがステップＳ１０３での進捗率ｐの算出に有効なデータである場合は、さらに所定の値を加算する。

【００４６】

例えば情報処理装置１００は、ステップＳ１０３での進捗率ｐの算出に有効なデータである場合は、さらに１％を進捗率ｐに加算する。すなわち、センサデータ取得部１１１が取得したセンサデータが、ステップＳ１０３での進捗率ｐの算出に有効なデータであればあるほど、情報処理装置１００は、ステップＳ１０３での進捗率ｐの算出の際に、進捗率ｐが上昇するように進捗率ｐを算出する。

【００４７】

情報処理装置１００は、ステップＳ１０３で進捗率ｐを算出すると、その算出した進捗率ｐに基づく情報を出力部１３０から出力しても良い。図５は、本開示の一実施形態に係る情報処理装置１００が出力部１３０に出力する画面の例を示す説明図である。図５に示したのは、ユーザが情報処理装置１００に対して鍵生成処理の開始を指示してから出力部１３０に出力される画面の一例である。図５には、進捗率ｐの増加に応じて状況が変化するプログレスバー１３１と、加速度データ１３２が出力部１３０に出力されている状態が示されている。情報処理装置１００は、図５に示したような画面を出力部１３０から出力することで、ユーザに対して鍵生成処理の進捗状況を分かりやすく提示することが出来る。なお、図５には進捗率ｐの値が出力部１３０に出力されている状態が示されているが、情報処理装置１００は、進捗率ｐは出力部１３０に出力せず、例えば進捗率ｐの増加に応じて状況が変化するプログレスバー１３１だけを出力部１３０に出力しても良い。

【００４８】

情報処理装置１００は、加速度データを出力部１３０へ表示する際に、Ｘ軸、Ｙ軸、Ｚ軸の３軸分を重ねて表示してもよい。ただし、すべてのデータを表示すると、鍵生成に利用するランダムネスが他者に露呈する可能性がある。そのため情報処理装置１００は、加速度データを表示する際に、一部のデータのみを表示したり、またはデータの精度を落として表示したりするなどして、鍵生成に利用するランダムネスが他者に露呈しないようにすることが望ましい。

【００４９】

もちろん、鍵生成処理の進捗状況を提示する画面は係る例に限定されるものではない。また情報処理装置１００は、画面へのプログレスバー１３１や進捗率の値の表示だけでなく、色の変化や音の変化等で鍵生成処理の進捗状況を出力部１３０から出力するようにしてもよい。例えば情報処理装置１００は、進捗率ｐが５％増加するごとに、Ｃ４、Ｄ４、Ｅ４、Ｆ４、Ｇ４、Ａ４、Ｂ４、Ｃ５、Ｄ５、Ｅ５、Ｆ５、Ｇ５、Ａ５、Ｂ５、…などと

段階的に高い音を出力部１３０から出力するようにしてもよい。また例えば情報処理装置１００は、進捗率の増加に伴って出力部１３０から出力する画面の色を変化させるような表示制御を実行してもよい。また例えば情報処理装置１００は、出力部１３０に対し、最初は複数の色からなる所定の図形が表示され、進捗率の増加に伴ってその複数の色が混ざっていくような表示制御を実行してもよい。

【００５０】

ステップＳ１０３で進捗率ｐを増加させる処理を実行すると、続いて情報処理装置１００は、その進捗率ｐの増加によって進捗率ｐが１００％に達したかどうかを判断する（ステップＳ１０４）。ステップＳ１０４の判断は、例えば進捗情報算出部１１３が実行し得る。

【００５１】

ステップＳ１０４の判断の結果、進捗率ｐが１００％に達していれば、続いて情報処理装置１００は、鍵生成処理を開始してから進捗率ｐが１００％に達するまでの加速度データを用いて、秘密鍵を生成する（ステップＳ１０５）。ステップＳ１０５の秘密鍵の生成処理は、例えば鍵生成部１１４が実行し得る。なお情報処理装置１００は、進捗率ｐが１００％に達すると、例えばバイブレータによる振動で、進捗率ｐが１００％に達したことをユーザに通知してもよい。情報処理装置１００は、進捗率ｐが１００％に達するまでの加速度データを用いて秘密鍵を生成するので、バイブレータによる振動によって生じたセンサデータは秘密鍵の生成には影響を与えない。

【００５２】

一方、ステップＳ１０４の判断の結果、進捗率ｐが１００％に達していれば、続いて情報処理装置１００は、ステップＳ１０２に戻って加速度データの取得処理を継続する。

【００５３】

情報処理装置１００は、進捗率ｐが１００％になり、加速度データを用いた秘密鍵の生成が完了すると、秘密鍵の生成が完了した旨の画面を出力部１３０から出力しても良い。図６は、本開示の一実施形態に係る情報処理装置１００が出力部１３０に出力する画面の例を示す説明図である。図６に示したのは、情報処理装置１００で秘密鍵の生成が完了した際に出力部１３０に出力される画面の一例である。図６に示した画面には、ＯＫボタン１２３が表示されている。ユーザがＯＫボタン１２３をタッチしたことを検出すると、情報処理装置１００は、秘密鍵を生成するアプリケーションを終了する。

【００５４】

本開示の一実施形態に係る情報処理装置１００は、上述した一連の処理を実行することで、ユーザが情報処理装置１００を振ったり、情報処理装置１００に振動を加えたりしたことに応じて得られるセンサデータを用いた秘密鍵の生成を可能にする。また本開示の一実施形態に係る情報処理装置１００は、上述した一連の処理を実行することで、ユーザに対してセンサデータの状態や、秘密鍵の作成処理の進捗状況を分かりやすく提示することができる。

【００５５】

続いて、進捗情報算出部１１３での進捗率ｐを算出するにあたって、進捗情報算出部１１３での進捗率の算出に有効なデータであるかどうか、すなわち、ユーザが情報処理装置１００を振ったことによる加速度データがセンサデータ取得部１１１で取得されたかどうかを判定部１１２で判定する際の判定処理例を説明する。

【００５６】

上述したように、判定部１１２は、３軸の加速度センサからセンサデータが出力される場合に、各軸について値の絶対値が所定の閾値を超えている場合、その時点でユーザが情報処理装置１００を振ったと判断してもよい。図７は、３軸の加速度センサからの出力データの一例をグラフで示す説明図である。図７には、ｘ軸方向のデータｘ１、ｙ軸方向のデータｙ１、ｚ軸方向のデータｚ１が、それぞれ示されている。また図７には、ユーザが情報処理装置１００を振った区間ｓ１、ｓ２も示されている。

【００５７】

例えば、Ｘ方向、Ｙ方向、Ｚ方向のそれぞれの加速度センサの、ｉ番目のデータでの値$Ｘ_{i}$、$Ｙ_{i}$、$Ｚ_{i}$のうち、いずれか１つの値の絶対値が所定の閾値$Ｃ_{1}$を超えた場合、すなわち、$|Ｘ_{i}|＞Ｃ_{1}$、または$|Ｙ_{i}|＞Ｃ_{1}$、または$|Ｚ_{i}|＞Ｃ_{1}$であった場合、判定部１１２は、そのｉ番目のデータの時点ではユーザが情報処理装置１００を振ったと判定する。

【００５８】

なお、単純に値の絶対値が所定の閾値を超えたことでユーザが情報処理装置１００を振ったと判定した場合、判定部１１２は、ユーザが情報処理装置１００を振っていなくても、乗り物に乗っている場合等に由来するノイズの影響で情報処理装置１００を振ったと判定する可能性がある。

【００５９】

そこで判定部１１２は、各軸について値の単位時間あたりの変化量の絶対値が所定の閾値を超えている場合、その時点でユーザが情報処理装置１００を振ったと判断してもよい。図８は、３軸の加速度センサからの出力データの、単位時間あたりの変化量の一例をグラフで示す説明図である。図８には、ｘ軸方向のデータｘ２、ｙ軸方向のデータｙ２、ｚ軸方向のデータｚ２が、それぞれ示されている。また図８には、ユーザが情報処理装置１００を振った区間ｓ１、ｓ２も示されている。

【００６０】

判定部１１２は、以下で定義する、ｉ番目のデータでの単位時間当たりの加速度変化量$ｄＸ_{i}$、$ｄＹ_{i}$、$ｄＺ_{i}$を利用して判定を行なう。なお、$Ｘ_{i}$、$Ｙ_{i}$、$Ｚ_{i}$はＸ方向、Ｙ方向、Ｚ方向のそれぞれの加速度センサの、ｉ番目のデータでの値である。また$ｔ_{i}$はｉ番目のデータが取得された時刻である。

$$ｄＸ_{i}＝（Ｘ_{i}－Ｘ_{i-1}）／（ｔ_{i}－ｔ_{i-1}）$$
$$ｄＹ_{i}＝（Ｙ_{i}－Ｙ_{i-1}）／（ｔ_{i}－ｔ_{i-1}）$$
$$ｄＺ_{i}＝（Ｚ_{i}－Ｚ_{i-1}）／（ｔ_{i}－ｔ_{i-1}）$$

【００６１】

そして判定部１１２は、例えば、$ｄＸ_{i}$、$ｄＹ_{i}$、$ｄＺ_{i}$のうち、いずれか１つについて絶対値が所定の閾値$Ｃ_{2}$を超えた場合、すなわち、$|ｄＸ_{i}|＞Ｃ_{2}$、または$|ｄＹ_{i}|＞Ｃ_{2}$、または$|ｄＺ_{i}|＞Ｃ_{2}$であった場合、判定部１１２は、そのｉ番目のデータの時点ではユーザが情報処理装置１００を振ったと判定する。また判定部１１２は、例えば、（$ｄＸ_{i}$、$ｄＹ_{i}$、$ｄＺ_{i}$）を３次元ベクトルと見なした場合のベクトル長が、ある閾値$Ｃ_{3}$を超えたとき、すなわち$（ｄＸ_{i}^{2}＋ｄＹ_{i}^{2}＋ｄＺ_{i}^{2}）^{1／2}＞Ｃ_{3}$であった場合、判定部１１２は、そのｉ番目のデータの時点ではユーザが情報処理装置１００を振ったと判定する。

【００６２】

判定部１１２は、このように各軸について値の単位時間あたりの変化量を用いて判定することで、ユーザが情報処理装置１００を振っていない場合における連続的な加速度の変化のノイズを除去して判定することが可能になる。

【００６３】

判定部１１２は、上述したような処理によって、ユーザが情報処理装置１００を振ったかどうかを判定することが出来る。ここで、加速度センサの値は、値に変化があった場合にのみ取得できることが多く、その場合には、加速度センサから一定間隔で値を取得することができない。また加速度センサから値を取得できる間隔は、加速度センサによって異なる。例えば、１秒間に２００回のデータを取得できる加速度センサもあれば、１秒間に最大でも５０回しか取得できない加速度センサもある。

【００６４】

加速度センサから値を取得できる間隔が異なると、判定部１１２が値の単位時間あたりの変化量を用いて判定する場合、間隔が長いほど、加速度変化量のピークを捉えにくくなる。従って、加速度センサから値を取得できる間隔が長い程、判定部１１２は情報処理装置１００を振ったと判定することが難しくなる。すなわち、情報処理装置１００を振った

と判定する頻度が異なると、同じように情報処理装置１００を振っても、ある装置では５秒振り続ければ進捗率が１００％に達するのに、ある装置では２０秒振り続けないと進捗率が１００％に達しない、ということが起こり得る。

【００６５】

しかし秘密鍵を生成するアプリケーションは広く配布されることが望ましく、従って、判定部１１２による判定アルゴリズムは、全ての装置で同じにすることが望ましい。

【００６６】

そこで、装置ごとのセンサの性能の違いを吸収するため、センサデータ取得部１１１は、前回にセンサ部１６０からセンサの値を取得した時刻から所定時間経過した後に、新たにセンサ部１６０からセンサの値を取得するようにしても良い。センサデータ取得部１１１は、この所定時間を任意の時間に設定することができるが、例えば値を取得できる間隔が長いセンサに合わせて所定時間を設定してもよい。このようにセンサデータ取得部１１１がセンサ部１６０からの値の取得間隔を調整することで、情報処理装置１００は、装置ごとのセンサの性能の違いを吸収し、判定部１１２による判定アルゴリズムを統一することが出来る。

【００６７】

またセンサデータ取得部１１１は、装置ごとのセンサの性能の違いを吸収するため、所定の時間における、例えば鍵生成アプリケーションを起動してから所定の時間における、自装置でのセンサ部１６０からの値を取得可能な平均の間隔Ｓを実測しても良い。例えばセンサデータ取得部１１１は、センサ部１６０から値をＴ秒間取得し、そのＴ秒間でＮ個の値がセンサ部１６０から取得できたとすると、平均の間隔ＳはＳ＝Ｔ／Ｎとなる。そして判定部１１２は、センサデータ取得部１１１が算出した平均間隔Ｓに応じ、上記所定の閾値C_1の値を変化させてもよい。つまり判定部１１２は、C_1をＳの関数C_1（Ｓ）とする。具体的には、平均間隔Ｓが広いほど、判定部１１２は情報処理装置１００を振ったと判定しにくくなるので、関数C_1（Ｓ）はＳが増加すると減少するような関数にすることが望ましい。

【００６８】

このように、センサデータ取得部１１１は、鍵生成アプリケーションを起動してから、鍵生成のランダムネスとして利用するセンサ部１６０の値の取得が開始されるまでの間の時間を利用することで、ユーザからの見た目には特に影響を与えずに、装置ごとのセンサの性能の違いを吸収することが出来る。

【００６９】

センサによっては、ＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）により、値を取得可能な間隔の情報が得られるものがある。しかし、センサによっては、正しい値ではなく、例えば０のような異常値を、値を取得可能な間隔として返すものもある。値を取得可能な間隔として異常値が返されてしまうと、正しい間隔の情報を得ることが出来ない。そこで、ＡＰＩによる値ではなく、センサデータ取得部１１１が値を取得可能な間隔を実測することで、本実施形態に係る情報処理装置１００は、異常値に影響されなくなるという効果を奏する。

【００７０】

そして判定部１１２は、上述したようにセンサデータ取得部１１１が算出した平均間隔Ｓに応じ、上記所定の閾値C_1の値を変化させることで、端末間のセンサの性能の差異を吸収することが可能になる。

【００７１】

続いて、図３のステップＳ１０５における秘密鍵の生成処理について例示する。図９は、本開示の一実施形態に係る情報処理装置１００の動作例を示す流れ図である。図９に示したのは、図３のステップＳ１０５における秘密鍵の生成処理の一例を詳細に示したものである。以下、図９を用いて本開示の一実施形態に係る情報処理装置１００の動作例について説明する。なお、以下の処理は鍵生成部１１４が実行するものとする。また鍵生成部１１４が生成する秘密鍵のビット長をＫビットとし、鍵生成部１１４が使用する関数Ｈは

、データをＬビットに圧縮する関数であるとする。なおデータを圧縮する関数には、例えばＳＨＡ２５６があり、ＳＨＡ２５６の場合、Ｌ＝２５６となる。

【００７２】

鍵生成部１１４は、進捗率ｐが１００％に達すると、鍵生成処理を開始してから進捗率ｐが１００％に達するまでのｎ個の加速度データx_1，…，x_nをセンサデータ取得部１１１から取得する（ステップＳ１１１）。加速度データx_1，…，x_nをセンサデータ取得部１１１から取得すると、続いて鍵生成部１１４は、変数ｉを１にセットし（ステップＳ１１２）、続いてＫ≦ｉＬかどうかを判断する（ステップＳ１１３）。

【００７３】

ステップＳ１１３の判断の結果、Ｋ≦ｉＬとなった場合は（ステップＳ１１３、Ｙｅｓ）、続いて鍵生成部１１４は、ｉ＝１，…，Ｎについて、ｉ，端末固有の情報（例えばＭＡＣアドレス）ｐ＿ｓｔｒ，x_1，…，x_nを連結したビット列（ｉ｜｜ｐ＿ｓｔｒ｜｜x_1｜｜…｜｜x_n）を関数Ｈに適用することにより、Ｌビット（例えば２５６ｂｉｔ）の長さのデータｈ１，…，ｈｎを得る。すなわち鍵生成部１１４は、h_i＝Ｈ（ｉ｜｜ｐ＿ｓｔｒ｜｜x_1｜｜…｜｜x_n）を計算する（ステップＳ１１４）。ステップＳ１１４でh_iを計算すると、続いて鍵生成部１１４は、ｉにｉ＋１を代入し（ステップＳ１１５）、上記ステップＳ１１３の判定処理を再度実行する。

【００７４】

一方、上記ステップＳ１１３の判断の結果、Ｋ＞ｉＬとなった場合は（ステップＳ１１３、Ｎｏ）、続いて鍵生成部１１４は、Ｌ×Ｎビットのデータｈ１｜｜…｜｜ｈｎの内のＫビットを秘密鍵として出力する（ステップＳ１１６）。

【００７５】

図３のステップＳ１０５における秘密鍵の生成処理の別の方法について例示する。図１０は、本開示の一実施形態に係る情報処理装置１００の動作例である。図１０に示したのは、図３のステップＳ１０５における秘密鍵の生成処理の一例を詳細に示したものであり、擬似乱数生成アルゴリズムを適用して生成した乱数を秘密鍵とする場合の動作例である。なお、擬似乱数生成アルゴリズムの例としては、ＮＩＳＴ　ＳＰ８００－９０Ａ等のＤＲＢＧ（決定性乱数生成器）がある。以下、図１０を用いて本開示の一実施形態に係る情報処理装置１００の動作例について説明する。なお、以下の処理は鍵生成部１１４が実行するものとする。また鍵生成部１１４が生成する秘密鍵のビット長をＫビットとする。

【００７６】

鍵生成部１１４は、進捗率ｐが１００％に達すると、鍵生成処理を開始してから進捗率ｐが１００％に達するまでのｎ個の加速度データx_1，…，x_nをセンサデータ取得部１１１から取得する（ステップＳ１２１）。加速度データx_1，…，x_nをセンサデータ取得部１１１から取得すると、続いて鍵生成部１１４は、ビット列x_1｜｜…｜｜x_nをエントロピー、またはエントロピーの一部、端末固有の情報（例えばＭＡＣアドレス）ｐ＿ｓｔｒをｐｅｒｓｏｎａｌｉｚａｔｉｏｎ　ｉｎｐｕｔとして利用し、乱数シードｓを初期化する（ステップＳ１２２）。

【００７７】

上記ステップＳ１２２で乱数シードｓを初期化すると、続いて鍵生成部１１４は、初期化した乱数シードｓを基にＫビットの乱数ｒを生成し、その乱数ｒを鍵とする（ステップＳ１２３）。鍵生成部１１４は、図１０に示した一連の処理を実行することで、鍵生成処理を開始してから進捗率ｐが１００％に達するまでのｎ個の加速度データx_1，…，x_nを用いた秘密鍵の生成が可能となる。

【００７８】

図３のステップＳ１０５における秘密鍵の生成処理のさらに別の方法について例示する。図１１は、本開示の一実施形態に係る情報処理装置１００の動作例である。図１１に示したのは、図３のステップＳ１０５における秘密鍵の生成処理の一例を詳細に示したものであり、擬似乱数生成アルゴリズムを適用して生成した乱数を秘密鍵とする場合の動作例である。

【００７９】
鍵生成部１１４は、進捗率ｐが１００％に達すると、鍵生成処理を開始してから進捗率ｐが１００％に達するまでのｎ個の加速度データx_1，…，x_nをセンサデータ取得部１１１から取得する（ステップＳ１３１）。加速度データx_1，…，x_nをセンサデータ取得部１１１から取得すると、続いて鍵生成部１１４は、ビット列$x_1||\cdots||x_n$をエントロピー、またはエントロピーの一部として利用し、乱数シードｓをリシードする（ステップＳ１３２）。
【００８０】
上記ステップＳ１２２で乱数シードｓをリシードすると、続いて鍵生成部１１４は、初期化した乱数シードｓを基にＫビットの乱数ｒを生成し、その乱数ｒを鍵とする（ステップＳ１３３）。
【００８１】
鍵生成部１１４は、上述したような処理を実行することにより、加速度データx_1，…，x_nを用いて鍵を生成することが出来る。また鍵生成部１１４は、鍵を生成する際にセンサ部１６０から送られる加速度データをそのまま使用するので、加速度データが少しでも違うと、全く違う値の鍵を生成することが出来る。従って本開示の一実施形態に係る情報処理装置１００は、同じ鍵を二度生成することを困難にさせて、秘密鍵の安全性を担保することが出来る。
【００８２】
上述した実施形態では、秘密にすることが求められる鍵（秘密鍵）を生成するものである。このような鍵には、共通鍵暗号技術に利用する共通鍵や、公開鍵暗号技術に利用する秘密鍵などがある。さらに、上述した実施形態において生成した秘密鍵を基に、公開鍵暗号技術に利用する公開鍵を生成することも可能である。
【００８３】
例えば、生成したのがＲＳＡの秘密鍵（素数ｐ，ｑ）であれば、鍵生成部１１４は、その秘密鍵から公開鍵（合成数Ｎ＝ｐｑ）を生成することが出来る。また例えば、生成したのがＥＣＤＳＡ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ；楕円曲線ＤＳＡ）の秘密鍵（スカラーｘ）であれば、鍵生成部１１４は、その秘密鍵から公開鍵ｙ（Ｇをベースポイントとして、Ｇのスカラー倍ｙ＝ｘＧ）を生成することが出来る。
【００８４】
例えば、生成したのが、特開２０１２－９８６９０号公報等で開示されている、多次多変数連立方程式に対する求解問題の困難性に安全性の根拠をおく公開鍵認証方式で用いられる秘密鍵（ベクトルｘ）であれば、鍵生成部１１４は、その秘密鍵から公開鍵ｙ（Ｆを２次多変数多項式から構成される写像として、ｙ＝Ｆ（ｘ））を生成することが出来る。
【００８５】
情報処理装置１００は、上述したように鍵生成部１１４が生成した公開鍵をユーザが視覚的に理解できるように出力部１３０から出力してもよい。例えば鍵生成部１１４は、生成した公開鍵をｂａｓｅ６４などでエンコードすることにより、視覚的に理解できるような情報に変換し、出力制御部１１５は、鍵生成部１１４が生成した当該情報を出力部１３０から出力する制御を実行してもよい
【００８６】
上述したように鍵生成部１１４が生成した公開鍵は、例えばｂｌｕｅｔｏｏｔｈ（登録商標）、Ｗｉ－Ｆｉ、ＮＦＣ（Ｎｅａｒ　ｆｉｅｌｄ　ｃｏｍｍｕｎｉｃａｔｉｏｎ）などの無線通信や、ＵＳＢケーブルなどの有線通信、テキスト入力による手作業でのコピー等により、情報処理装置１００から他の機器に転送されて、転送先の当該他の機器に登録されるようにしてもよい。
【００８７】
上述の実施形態で述べたように、鍵生成部１１４で生成された鍵（秘密鍵及び公開鍵）は、情報処理装置１００の内部に格納されてもよく、情報処理装置１００と別の装置、例

えばスマートフォン、タブレット端末、ＵＳＢメモリなどのポータブルデバイスを含む何らかの装置に格納され得る。そして鍵生成部１１４で生成された鍵は、その後、常に利用可能な状態にしてもよく、鍵が格納される装置に設けられるボタンまたはスイッチなどの機構により、利用可能状態と利用不可状態とを切替可能としてもよい。具体的には、切替の機構として、鍵をスマートフォンに格納している場合、装置にインストールされているアプリケーションが提供する機能、例えばウィジェットと呼ばれる、ホーム画面に貼り付けられてユーザの操作を受け付けることが可能な機能であってもよい。

【００８８】

そして、秘密鍵を格納した装置は、秘密鍵が利用可能状態であればその秘密鍵を利用した公開鍵認証の要求に自動で応答するが、秘密鍵が利用不可状態であればその秘密鍵を利用した公開鍵認証の要求に応答しないように動作を制御してもよい。

【００８９】

＜２．ハードウェア構成例＞

上記の各アルゴリズムは、例えば、図１２に示す情報処理装置のハードウェア構成を用いて実行することが可能である。つまり、当該各アルゴリズムの処理は、コンピュータプログラムを用いて図１２に示すハードウェアを制御することにより実現される。なお、このハードウェアの形態は任意であり、例えば、パーソナルコンピュータ、携帯電話、ＰＨＳ、ＰＤＡ等の携帯情報端末、ゲーム機、接触式又は非接触式のＩＣチップ、接触式又は非接触式のＩＣカード、又は種々の情報家電がこれに含まれる。但し、上記のＰＨＳは、Ｐｅｒｓｏｎａｌ Ｈａｎｄｙ－ｐｈｏｎｅ Ｓｙｓｔｅｍの略である。また、上記のＰＤＡは、Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔの略である。

【００９０】

図１２に示すように、このハードウェアは、主に、ＣＰＵ９０２と、ＲＯＭ９０４と、ＲＡＭ９０６と、ホストバス９０８と、ブリッジ９１０と、を有する。さらに、このハードウェアは、外部バス９１２と、インターフェース９１４と、入力部９１６と、出力部９１８と、記憶部９２０と、ドライブ９２２と、接続ポート９２４と、通信部９２６と、を有する。但し、上記のＣＰＵは、Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略である。また、上記のＲＯＭは、Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙの略である。そして、上記のＲＡＭは、Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙの略である。

【００９１】

ＣＰＵ９０２は、例えば、演算処理装置又は制御装置として機能し、ＲＯＭ９０４、ＲＡＭ９０６、記憶部９２０、又はリムーバブル記録媒体９２８に記録された各種プログラムに基づいて各構成要素の動作全般又はその一部を制御する。ＲＯＭ９０４は、ＣＰＵ９０２に読み込まれるプログラムや演算に用いるデータ等を格納する手段である。ＲＡＭ９０６には、例えば、ＣＰＵ９０２に読み込まれるプログラムや、そのプログラムを実行する際に適宜変化する各種パラメータ等が一時的又は永続的に格納される。

【００９２】

これらの構成要素は、例えば、高速なデータ伝送が可能なホストバス９０８を介して相互に接続される。一方、ホストバス９０８は、例えば、ブリッジ９１０を介して比較的データ伝送速度が低速な外部バス９１２に接続される。また、入力部９１６としては、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチ、及びレバー等が用いられる。さらに、入力部９１６としては、赤外線やその他の電波を利用して制御信号を送信することが可能なリモートコントローラ（以下、リモコン）が用いられることもある。さらに、入力部９１６としては、各種センサ、例えば地磁気センサ、加速度センサ等のセンサやＧＰＳ等の現在地を取得するものが用いられることもある。

【００９３】

出力部９１８としては、例えば、ＣＲＴ、ＬＣＤ、ＰＤＰ、又はＥＬＤ等のディスプレイ装置、スピーカ、ヘッドホン等のオーディオ出力装置、プリンタ、携帯電話、又はファクシミリ等、取得した情報を利用者に対して視覚的又は聴覚的に通知することが可能な装置である。但し、上記のＣＲＴは、Ｃａｔｈｏｄｅ Ｒａｙ Ｔｕｂｅの略である。また

、上記のＬＣＤは、Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙの略である。そして、上記のＰＤＰは、Ｐｌａｓｍａ　ＤｉｓｐｌａｙＰａｎｅｌの略である。さらに、上記のＥＬＤは、Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ　Ｄｉｓｐｌａｙの略である。

【００９４】

記憶部９２０は、各種のデータを格納するための装置である。記憶部９２０としては、例えば、ハードディスクドライブ（ＨＤＤ）等の磁気記憶デバイス、半導体記憶デバイス、光記憶デバイス、又は光磁気記憶デバイス等が用いられる。但し、上記のＨＤＤは、Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅの略である。

【００９５】

ドライブ９２２は、例えば、磁気ディスク、光ディスク、光磁気ディスク、又は半導体メモリ等のリムーバブル記録媒体９２８に記録された情報を読み出し、又はリムーバブル記録媒体９２８に情報を書き込む装置である。リムーバブル記録媒体９２８は、例えば、ＤＶＤメディア、Ｂｌｕ－ｒａｙメディア、ＨＤ　ＤＶＤメディア、各種の半導体記憶メディア等である。もちろん、リムーバブル記録媒体９２８は、例えば、非接触型ＩＣチップを搭載したＩＣカード、又は電子機器等であってもよい。但し、上記のＩＣは、Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔの略である。

【００９６】

接続ポート９２４は、例えば、ＵＳＢポート、ＩＥＥＥ１３９４ポート、ＳＣＳＩ、ＲＳ－２３２Ｃポート、又は光オーディオ端子等のような外部接続機器９３０を接続するためのポートである。外部接続機器９３０は、例えば、プリンタ、携帯音楽プレーヤ、デジタルカメラ、デジタルビデオカメラ、又はＩＣレコーダ等である。但し、上記のＵＳＢは、Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓの略である。また、上記のＳＣＳＩは、Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅの略である。

【００９７】

通信部９２６は、ネットワーク９３２に接続するための通信デバイスであり、例えば、有線又は無線ＬＡＮ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、又はＷＵＳＢ用の通信カード、光通信用のルータ、ＡＤＳＬ用のルータ、又は接触又は非接触通信用のデバイス等である。また、通信部９２６に接続されるネットワーク９３２は、有線又は無線により接続されたネットワークにより構成され、例えば、インターネット、家庭内ＬＡＮ、赤外線通信、可視光通信、放送、又は衛星通信等である。但し、上記のＬＡＮは、Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋの略である。また、上記のＷＵＳＢは、Ｗｉｒｅｌｅｓｓ　ＵＳＢの略である。そして、上記のＡＤＳＬは、Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅの略である。

【００９８】

例えば、情報処理装置１００がこのようなハードウェア構成を有する場合、例えば制御部１１０の機能はＣＰＵ９０２が担い得る。また例えば入力部１２０の機能は入力部９１６が担い得る。また例えば、出力部１３０の機能は出力部９１８が担い得る。また例えば、通信部１４０の機能は通信部９２６が担い得る。また例えば記憶部１４０の機能はＲＯＭ９０４、ＲＡＭ９０６、記憶部９２０、又はリムーバブル記録媒体９２８が担い得る。また例えばセンサ部１６０の機能は入力部９１６が担い得る。

【００９９】

＜３．まとめ＞

以上説明したように本開示の一実施形態によれば、ユーザに特別な操作を強いることなく、情報処理装置１００の動きを検出するセンサ部１６０が出力した情報を用いて鍵情報、特に秘密鍵を生成する情報処理装置１００が提供される。本開示の一実施形態に係る情報処理装置１００は、所定の期間内、例えば、ユーザが鍵情報の生成開始を情報処理装置１００に指示してから、センサ部１６０からの情報が充分得られるまで（例えば進捗率ｐが１００％になるまで）の期間内でセンサ部１６０が出力した情報を用いて鍵情報を生成する。

【０１００】

本開示の一実施形態に係る情報処理装置１００は、所定の期間内でセンサ部１６０が出力した情報を用いて鍵情報を生成することで、秘密情報の生成の際のランダムネスとしてセンサ部１６０が出力した情報を用いる際に、ユーザの負担が少なく、かつ手軽に充分なランダムネスを得ることを可能にする。

【０１０１】

また本開示の一実施形態に係る情報処理装置１００は、装置間でセンサの性能が異なる場合を考慮し、センサ部１６０から出力されるセンサデータの取得間隔を調整する。本開示の一実施形態に係る情報処理装置１００は、センサ部１６０から出力されるセンサデータの取得間隔を調整することで、センサの性能が装置で異なる場合であっても同じような操作感を提供することが可能となる。

【０１０２】

本明細書の各装置が実行する処理における各ステップは、必ずしもシーケンス図またはフローチャートとして記載された順序に沿って時系列に処理する必要はない。例えば、各装置が実行する処理における各ステップは、フローチャートとして記載した順序と異なる順序で処理されても、並列的に処理されてもよい。

【０１０３】

また、各装置に内蔵されるＣＰＵ、ＲＯＭおよびＲＡＭなどのハードウェアを、上述した各装置の構成と同等の機能を発揮させるためのコンピュータプログラムも作成可能である。また、該コンピュータプログラムを記憶させた記憶媒体も提供されることが可能である。また、機能ブロック図で示したそれぞれの機能ブロックをハードウェアで構成することで、一連の処理をハードウェアで実現することもできる。また、当該コンピュータプログラムはスマートフォンやタブレット等種々の情報処理端末向けアプリケーション・プログラムとして、インターネット等のネットワーク上に存在する所定のアプリケーション配信サイトから配信することが可能である。このようなアプリケーション配信サイトは、プログラムを記憶する記憶装置と、クライアント（スマートフォンやタブレット等種々の情報処理端末）からのダウンロード要求に応じ、そのアプリケーション・プログラムを送信する通信装置とを備えるサーバ装置が提供し得る。

【０１０４】

以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

【０１０５】

例えば上記実施形態では、進捗情報として進捗率を算出していたが、本開示はかかる例に限定されるものではない。情報処理装置１００が所定の回数振られたら秘密鍵の生成に用いるセンサデータの取得を完了するとした場合、進捗情報算出部１１３は進捗情報として、例えば情報処理装置１００が振られた回数を計数しても良い。例えば情報処理装置１００が１００回振られたら秘密鍵の生成に用いるセンサデータの取得を完了するとした場合、進捗情報算出部１１３は情報処理装置１００が振られた回数を計数することで、進捗情報として、情報処理装置１００が何回振られているかについてや、鍵の生成のためには後何回振れば良いかについて算出することが出来る。

【０１０６】

また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

【０１０７】

なお、以下のような構成も本開示の技術的範囲に属する。

（１）

所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得するセン

サデータ取得部と、
前記センサデータ取得部が所定の期間において取得した前記情報に基づいて、認証処理に用いられる鍵情報を生成する鍵生成部と、
を備える、情報処理装置。
（２）
前記センサからの前記情報の取得が完了するまでの進捗情報に基づく情報を出力する進捗情報算出部をさらに備える、前記（１）に記載の情報処理装置。
（３）
前記進捗情報算出部は、前記鍵生成部での鍵情報の生成に用いられる前記情報の取得が完了するまでの進捗情報を算出する、前記（２）に記載の情報処理装置。
（４）
前記進捗情報算出部が算出した進捗情報を出力する出力部をさらに備える、前記（２）または（３）に記載の情報処理装置。
（５）
前記鍵生成部での鍵情報の生成に用いられる前記情報の取得が完了するまでの進捗情報を算出する進捗情報算出部をさらに備える、前記（１）～（４）のいずれかに記載の情報処理装置。
（６）
前記センサデータ取得部が取得した前記情報は前記鍵生成部での鍵情報の生成に有効な情報か否かを判定する判定部をさらに備える、前記（１）～（５）のいずれかに記載の情報処理装置。
（７）
前記判定部は、前記センサデータ取得部が取得した前記情報の単位時間あたりの変化量を用いて判定する、前記（６）に記載の情報処理装置。
（８）
前記判定部は、前記センサデータ取得部が取得した前記情報の絶対値を用いて判定する、前記（６）に記載の情報処理装置。
（９）
前記センサデータ取得部は、前記情報を取得してから所定時間が経過した後に新たな前記加速度情報を取得する、前記（１）～（８）のいずれかに記載の情報処理装置。
（１０）
前記センサデータ取得部は、前記所定の期間の前に前記センサからの情報の平均取得間隔を用いて前記所定時間を決定する、前記（９）に記載の情報処理装置。
（１１）
前記センサデータ取得部が取得する前記情報は、加速度情報である、前記（１）～（１０）のいずれかに記載の情報処理装置。
（１２）
前記鍵生成部は、前記センサデータ取得部が取得した前記情報と、自装置固有の情報を用いて鍵情報を生成する、前記（１）～（１１）のいずれかに記載の情報処理装置。
（１３）
前記鍵生成部が生成する鍵情報は秘密鍵である、前記（１）～（１２）のいずれかに記載の情報処理装置。
（１４）
所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得することと、
所定の期間において取得された前記情報をに基づいて、認証処理に用いられる鍵情報を生成することと、
を含む、情報処理方法。
（１５）
コンピュータに、

所定の情報をセンシングするセンサが取得した前記情報を前記センサから取得することと、

所定の期間において取得された前記情報に基づいて、認証処理に用いられる鍵情報を生成することと、

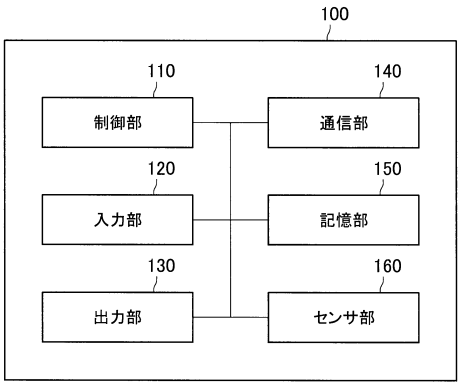
を実行させる、コンピュータプログラム。

【符号の説明】

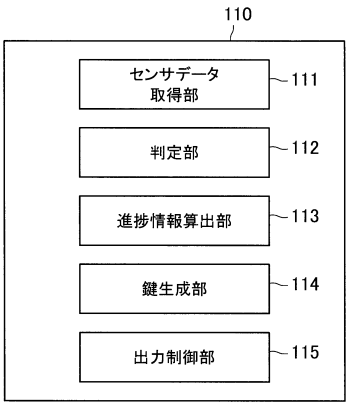
【０１０８】

１００　情報処理装置
１１０　制御部
１１１　センサデータ取得部
１１２　判定部
１１３　進捗情報算出部
１１４　鍵生成部
１１５　出力制御部
１２０　入力部
１３０　出力部
１４０　通信部
１５０　記憶部
１６０　センサ部

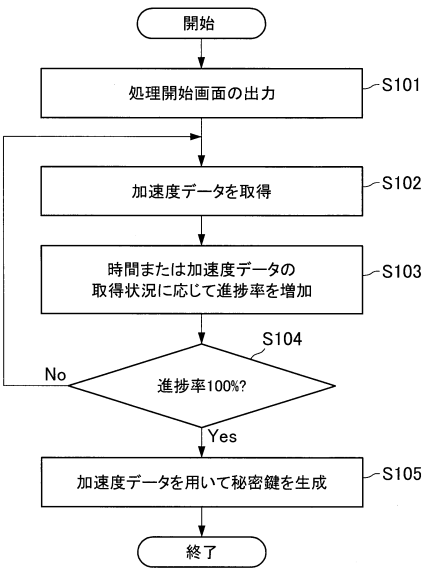
【図１】



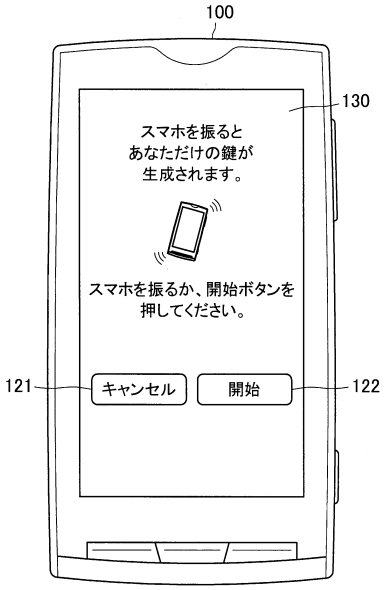
【図２】



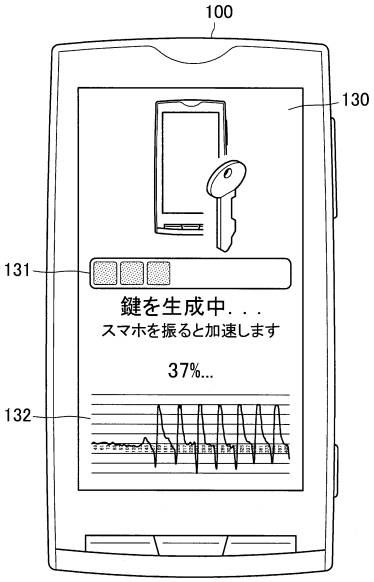
【図３】



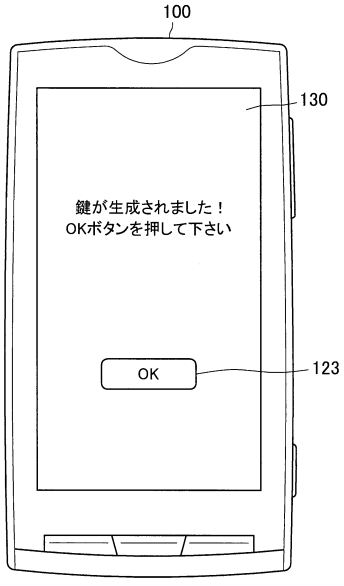
【図４】


100
130
スマホを振ると
あなただけの鍵が
生成されます。
スマホを振るか、開始ボタンを
押してください。
121
キャンセル
開始
122

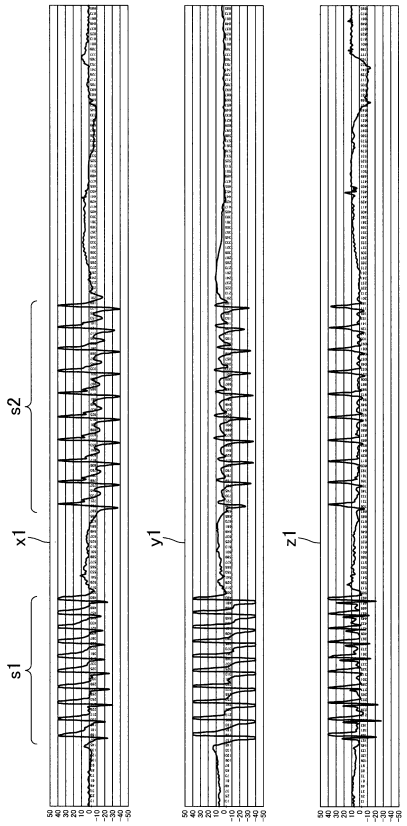
【図５】


100
130
131
鍵を生成中．．．
スマホを振ると加速します
37%...
132

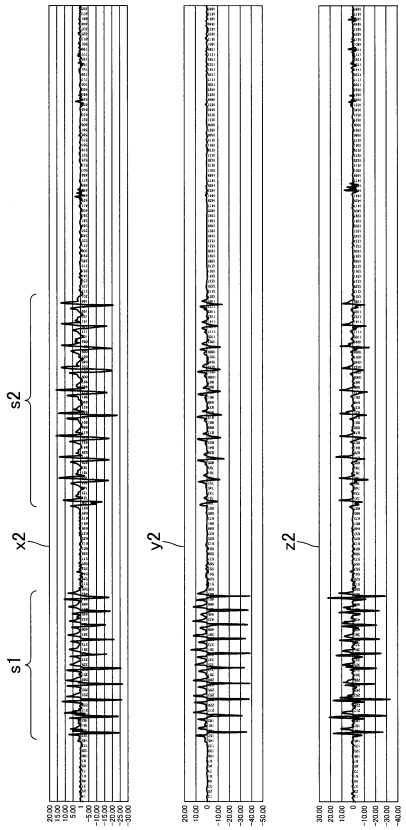
【図６】


100
130
鍵が生成されました！
OKボタンを押して下さい
OK
123

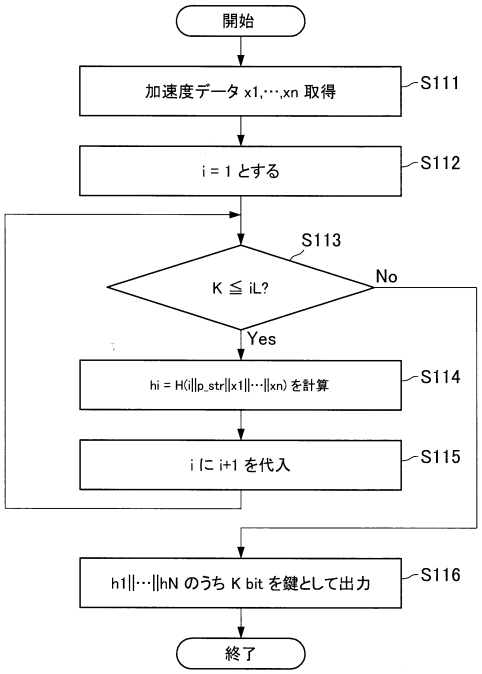
【図７】


s2
x1
s1
y1
z1

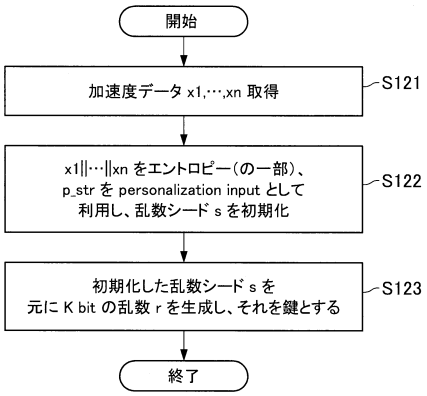
【図８】


s2
x2
s1
y2
z2

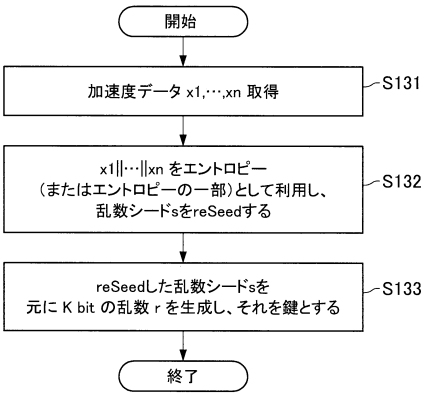
【図９】


開始
加速度データ x1,…,xn 取得
S111
i = 1 とする
S112
S113
K ≦ iL?
No
Yes
hi = H(i||p_str||x1||…||xn) を計算
S114
i に i+1 を代入
S115
h1||…||hN のうち K bit を鍵として出力
S116
終了

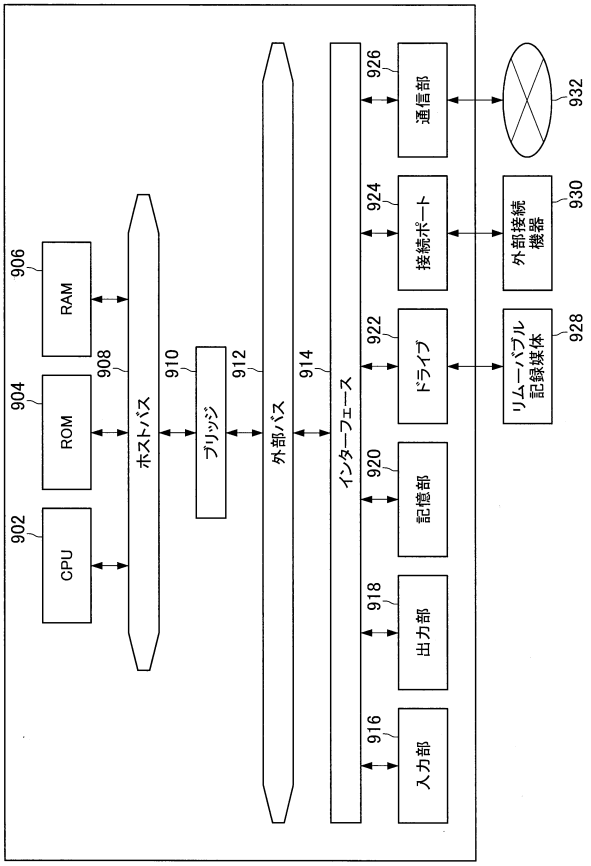
【図１０】


開始
加速度データ x1,…,xn 取得
S121
x1||…||xn をエントロピー（の一部）、
p_str を personalization input として
利用し、乱数シード s を初期化
S122
初期化した乱数シード s を
元に K bit の乱数 r を生成し、それを鍵とする
S123
終了

【図１１】


開始
加速度データ x1,…,xn 取得
S131
x1||…||xn をエントロピー
（またはエントロピーの一部）として利用し、
乱数シードsをreSeedする
S132
reSeedした乱数シードsを
元に K bit の乱数 r を生成し、それを鍵とする
S133
終了

【図１２】


902
CPU
904
ROM
906
RAM
908
ホストバス
910
ブリッジ
912
外部バス
914
インターフェース
916
入力部
918
出力部
920
記憶部
922
ドライブ
924
接続ポート
926
通信部
928
リムーバブル記録媒体
930
外部接続機器
932

フロントページの続き

(72)発明者　市川　美和
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　白井　太三
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　一司　豊秀
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　井手　裕二
東京都港区港南１丁目８番１５号　ソニーモバイルコミュニケーションズ株式会社内

審査官　平井　誠

(56)参考文献　特開２０１１－１３０２２４（ＪＰ，Ａ）
特開平０４－２４７７３７（ＪＰ，Ａ）
特開２０１３－１４０４１５（ＪＰ，Ａ）
米国特許出願公開第２０１０／０１９９０９２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８