(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-520942
(P2017-520942A)
(43)公表日　平成29年7月27日(2017.7.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621Z	2G017
H04L 9/08	(2006.01)	H04L	9/00	601E	5J104
G01R 33/02	(2006.01)	H04L	9/00	601C	
		G01R	33/02	Z	
		H04L	9/00	601A	

審査請求 有　予備審査請求 未請求　（全 22 頁）

(21)出願番号　特願2016-550251 (P2016-550251)
(86)(22)出願日　平成27年11月17日 (2015.11.17)
(11)特許番号　特許第6159893号 (P6159893)
(45)特許公報発行日　平成29年7月5日 (2017.7.5)
(85)翻訳文提出日　平成28年9月27日 (2016.9.27)
(86)国際出願番号　PCT/EP2015/076820
(87)国際公開番号　WO2016/142014
(87)国際公開日　平成28年9月15日 (2016.9.15)

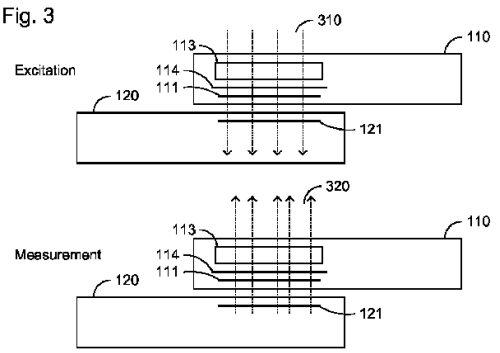
(71)出願人　598036300
テレフオンアクチーボラゲット　エルエム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】共有秘密鍵として用いるための鍵の生成

(57)【要約】
他の通信機器(120)との通信において共有秘密鍵として用いるための鍵を生成する通信機器(110)が提供される。通信機器(110，120)のそれぞれは、励起磁界を受けた際に、第１の電池(113)に含まれる金属粒子の第１の空間的に変化する密度によって発生する、空間的に変化する磁界(320)を測定するセンサアレイ(111，121)と、センサアレイ(111，121)から空間的に変化する磁界(320)を表す一式の値を取得し、一式の値から鍵を取得するように動作可能な処理手段と、を有する。励起磁界(310)は通信機器(110，120)の１つが有する磁界発生器(114)によって発生される。それにより、２つの通信機器(110，120)は、接近している際に、第１の電池(113)に含まれる金属粒子の空間的に変化する密度を調べることにより、同一の鍵を生成することができる。
【選択図】図３

Fig. 3



【特許請求の範囲】
【請求項１】
他の通信機器(120; 200)との通信において共有秘密鍵として用いるための鍵を生成する通信機器(110; 200)であって、
前記他の通信機器との通信を実現するための通信インタフェース(205)と、
励起磁界を受けた際に第１の電池(113)に含まれる金属粒子の第１の空間的に変化する密度によって発生する、空間的に変化する磁界(320)を測定するセンサアレイ(111, 121; 201)と、
処理手段(206; 600; 700)であって、
前記センサアレイから、前記空間的に変化する磁界を表す、一式の値を取得し、
前記一式の値から前記鍵を取得する、ように動作可能な処理手段と、
を有する通信機器。
【請求項２】
さらに、前記第１の電池(113; 203)を有する、請求項１に記載の通信機器。
【請求項３】
前記測定された磁界(420, 430)が、前記励起磁界(410)を受けた際に、金属粒子の前記第１の空間的に変化する密度および第２の電池(123; 203)に含まれる金属粒子の第２の空間的に変化する密度によって発生し、前記第２の電池が前記他の通信機器(120)に含まれる、請求項２に記載の通信機器。
【請求項４】
前記励起磁界を発生するための磁界発生器(114; 204)をさらに有する、請求項１から請求項３のいずれか１項に記載の通信機器。
【請求項５】
前記励起磁界が、前記他の通信機器の接近を検出したことに応じて発生される、請求項４に記載の通信機器。
【請求項６】
前記励起磁界が、前記通信機器のユーザから指示を受信したことに応じて発生される、請求項４に記載の通信機器。
【請求項７】
前記励起磁界が、前記他の通信機器の要求を受信したことに応じて発生される、請求項４に記載の通信機器。
【請求項８】
前記励起磁界が前記他の通信機器によって発生される、請求項１から請求項７のいずれか１項に記載の通信機器。
【請求項９】
前記一式の値が、前記他の通信機器によって発生された前記励起磁界を検出したことに応じて前記センサアレイから取得される、請求項８に記載の通信機器。
【請求項１０】
前記処理手段は、前記鍵を前記他の通信機器との通信において共有秘密鍵として用いるようにさらに動作可能である、請求項１から請求項９のいずれか１項に記載の通信機器。
【請求項１１】
前記処理手段は、基数変換を用いて前記一式の値から前記鍵を取得するように動作可能である、請求項１から請求項１０のいずれか１項に記載の通信機器。
【請求項１２】
前記一式の値の各値が、前記センサアレイの各センサによって測定された前記空間的に変化する磁界を表し、
前記処理手段は、
前記一式の値から１つ以上の値を選択し、
前記１つ以上の選択された値を測定したセンサの１つ以上のインデックス(510-540)に基づいて前記鍵を取得することによって、前記一式の値から前記鍵を取得する、

ように動作可能である、請求項１から請求項１０のいずれか１項に記載の通信機器。
【請求項１３】
前記センサアレイは、インダクタ、磁気抵抗センサ、ホール効果センサ、スピントランジスタ、フラックスゲート、磁気電気センサ、および磁気光学センサのいずれか１つまたは組み合わせに基づくセンサ(202)を有する、請求項１から請求項１２のいずれか１項に記載の通信機器。
【請求項１４】
モバイル端末、ユーザ機器、スマートフォン、ウェアラブルデバイス、タブレット、スマートウォッチ、キャッシュレジスタ、支払い端末、センサ、アクチュエータ、またはラップトップコンピュータのいずれか１つである、請求項１から請求項１３のいずれか１項に記載の通信機器。
【請求項１５】
請求項１から請求項１４のいずれか１項に記載の通信機器を有する車両。
【請求項１６】
他の通信機器(120)との通信において共有秘密鍵として用いるための鍵を生成する通信機器(110)の方法(800)であって、
励起磁界(310)を受けた際に第１の電池(113)に含まれる金属粒子の第１の空間的に変化する密度によって発生する、空間的に変化する磁界(320)を、センサアレイを用いて測定する(831)ことと、
前記センサアレイから、前記空間的に変化する磁界を表す、一式の値を取得する(832)ことと、
前記一式の値から前記鍵を取得する(833)ことと、を有する方法。
【請求項１７】
前記第１の電池(113)は前記通信機器(120)に含まれる、請求項１６に記載の方法。
【請求項１８】
前記測定された磁界(420，430)が、前記励起磁界(410)を受けた際に、金属粒子の前記第１の空間的に変化する密度および第２の電池(123)に含まれる金属粒子の第２の空間的に変化する密度によって発生し、前記第２の電池が前記他の通信機器(120)に含まれる、請求項１７に記載の方法。
【請求項１９】
前記励起磁界を発生させる(821)こと、をさらに有する請求項１６から請求項１８のいずれか１項に記載の方法。
【請求項２０】
前記励起磁界が、前記他の通信機器の接近を検出した(811)ことに応じて発生される(821)、請求項１９に記載の方法。
【請求項２１】
前記励起磁界が、前記通信機器のユーザから指示を受信した(812)ことに応じて発生される(821)、請求項１９に記載の方法。
【請求項２２】
前記励起磁界が、前記他の通信機器から要求を受信した(813)ことに応じて発生される(821)、請求項１９に記載の方法。
【請求項２３】
前記励起磁界が前記他の通信機器によって発生される、請求項１８または請求項１９に記載の方法。
【請求項２４】
前記一式の値が、前記他の通信機器によって発生された前記励起磁界を検出した(822)ことに応じて前記センサアレイから取得される(832)、請求項２３に記載の方法。
【請求項２５】
前記他の通信機器との通信において前記鍵を共通暗号鍵として用いる(835)ことをさらに有する、請求項１６から請求項２４のいずれか１項に記載の方法。

【請求項２６】
前記鍵は、基数変換を用いて前記一式の値から取得される(833)、請求項１６から請求項２５のいずれか１項に記載の方法。
【請求項２７】
前記一式の値の各値が、前記センサアレイの各センサによって測定された前記空間的に変化する磁界を表し、
前記鍵が、
前記一式の値から１つ以上の値を選択し、
前記１つ以上の選択された値を測定したセンサの１つ以上のインデックスに基づいて前記鍵を取得する、ことによって前記一式の値から取得される(833)、
請求項１６から請求項２５のいずれか１項に記載の方法。
【請求項２８】
前記センサアレイは、インダクタ、磁気抵抗センサ、ホール効果センサ、スピントランジスタ、フラックスゲート、磁気電気センサ、および磁気光学センサのいずれか１つまたは組み合わせに基づくセンサを有する、請求項１６から請求項２７のいずれか１項に記載の方法。
【請求項２９】
前記通信機器は、モバイル端末、ＵＥ、スマートフォン、ウェアラブルデバイス、タブレット、スマートウォッチ、キャッシュレジスタ、支払い端末、またはラップトップコンピュータのいずれか１つである、請求項１６から請求項２８のいずれか１項に記載の方法。
【請求項３０】
コンピュータが実行可能な命令(603)を有するコンピュータプログラムであって、前記コンピュータが実行可能な命令は、機器が有する処理ユニット(601)で実行された際に、前記機器に請求項１６から請求項２９のいずれか１項に記載の方法を実行させる、コンピュータプログラム。
【請求項３１】
請求項３０に記載のコンピュータプログラムを格納したコンピュータ可読記憶媒体(602)。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、他の通信機器との通信において共有秘密鍵として用いるための鍵を生成するための通信機器、対応する方法、対応するコンピュータプログラム、および対応するコンピュータプログラム製品に関する。
【背景技術】
【０００２】
通信機器の多くの用途は、１つ以上の他の通信機器、または通信ネットワークとデータを交換するためにセキュアな通信を必要とする。この文脈において、通信機器は有線または無線技術を１つ以上の適切な通信プロトコルとともに用いて通信を実現可能な電子機器である。
【０００３】
第１の例は、携帯電話機、スマートフォン、ユーザ機器（ＵＥ）、タブレット、またはラップトップコンピュータといった第１のモバイル機器と、第２のモバイル機器との間で、ドキュメント、メッセージ、電子メール、または画像を交換することである。第２の例は、モバイル端末と、センサまたはアクチュエータとの間のマシンツーマシン（Ｍ２Ｍ）通信である。第３の例は、売り場(point-of-sale)の金融取引を達成するための、モバイル端末と支払い端末との間の通信である。
【０００４】
２つ以上の通信機器間、または通信機器と通信ネットワークとの間で送信されるデータ

およびメッセージに関してある程度のレベルのセキュリティを提供するために暗号化を用いることができる。いくつかの暗号化スキーム、特には対称スキームは、共有秘密鍵(shared secret)、すなわち、通信セッションに関与する通信機器間で共有され、かつそれらの機器だけが利用可能なビットストリングまたはシンボルのストリングといった情報、の利用可能性に基づいている。そのような共有秘密鍵は、１つの通信機器または別個のネットワークエンティティのソフトウェアまたはハードウェアで生成され、残りの通信機器に分配されてよい。鍵を共有する手順は単純でなく、攻撃にさらされている。例えば、共有秘密鍵は盗聴や中間者攻撃などの結果として暴れうる。

【発明の概要】

【０００５】

本発明の目的は上述した技術および従来技術の改良された代替物を提供することにある。

【０００６】

より具体的には、本発明の目的は、２つ以上の通信機器間、または通信機器と通信ネットワークとの間の通信における共有秘密鍵として用いるための鍵を生成するための改良された解決方法の提供にある。

【０００７】

本発明のこれらの目的および他の目的は、独立請求項に規定されるように、本発明のさまざまな態様によって達成される。本発明の実施形態は従属請求項によって特徴づけられる。

【０００８】

発明の第１の態様によれば、鍵を生成するための通信機器が提供される。通信機器は、例えばモバイル端末、ＵＥ、スマートフォン、タブレット、ラップトップコンピュータ、スマートウォッチのようなウェアラブルデバイス、センサ、アクチュエータ、または、キャッシュレジスターまたは支払い端末のような、売り場で金融取引を実現するための機器であってよい。鍵は、他の通信機器との通信において共有秘密鍵として用いられてよい。通信機器は、他の通信機器との通信を実現するための通信インタフェースと、励起磁界を受けた際に、第１の電池に含まれる金属粒子の第１の空間的に変化する密度によって発生する、空間的に変化する磁界を測定するためのセンサアレイと、処理手段とを有する。センサアレイは、例えば、インダクタ、磁気抵抗センサ、ホール効果センサ、スピントランジスタ、フラックスゲート、磁気電気センサ、および磁気光学センサのいずれか１つまたは組み合わせに基づくセンサを有しうる。処理手段はセンサアレイから値のセットを取得して、値のセットから鍵を得るように動作可能である。値のセットは空間的に変化する磁界を表している。

【０００９】

発明の第２の態様によれば、鍵を生成する通信機器の方法が提供される。鍵は、他の通信機器との通信において共有秘密鍵として用いられてよい。方法は、励起磁界を受けた際に、第１の電池に含まれる金属粒子の第１の空間的に変化する密度によって発生する、空間的に変化する磁界を測定することと、センサアレイから一式の値を取得することと、一式の値から鍵を得ることと、を有する。空間的に変化する磁界は、センサアレイを用いて測定される。一式の値は空間的に変化する磁界を表す。

【００１０】

発明の第３の態様によれば、コンピュータプログラムが提供される。コンピュータプログラムは、コンピュータが実行可能な命令であって、機器が有する処理ユニットで実行された際に、この機器に本発明の第２の態様の実施形態に従った方法を実行させる命令を有する。

【００１１】

本発明の第４の態様によれば、コンピュータプログラム製品が提供される。コンピュータプログラム製品は、本発明の第３の態様に従ったコンピュータプログラムを具現化したコンピュータ可読記憶媒体を有する。

【００１２】
本発明は、少なくとも２つの通信機器間の通信において共有秘密鍵として用いるための鍵が、天然の無作為さによって特徴付けられる物理的プロセスによって確立されうるとの知見を利用する。それによって、真の乱数が生成されるであろう。本発明の実施形態は、２つ以上の通信機器のそれぞれが鍵のコピーを生成することができるため、１つの通信機器で生成された鍵を他の通信機器と共有するための、複雑かつ攻撃を受けやすい手順を必要とせずに共有秘密鍵を確立する。
【００１３】
本発明は、物理的プロセスによって規定される出力値セットに至る入力値セットを有する関数として記述することのできる物理複製困難関数(PUF)の概念に基づいている。入力空間はやや大きくなり得、入力値を出力値に変換する関数を完全に特徴付けることは不可能と考えられている。ＰＵＦは、物理的システムを調べ、一式の物理量を応答として測定することによって実現することができる。
【００１４】
本発明の実施形態は、少なくとも１つの電池である第１の電池内の化学的プロセスの結果として生じる金属粒子をＰＵＦとして利用する。１つ以上の電池は例えばリチウムイオンまたはリチウムポリマータイプであってよく、金属粒子は、電池の充放電サイクルが繰り返される間にリチウム電極の表面で成長し、もう一方の電極に達するまで電池の電解質を横断して拡がることで知られているリチウムデンドライトであってよい（K. J. Harry, D. T. Hallinan, D. Y. Parkinson, A. A. MacDowell, および N. P. Balsara, ”Detection of subsurface structures underneath dendrites formed on cycled lithium metal electrodes”, Nature Materials, vol. 13, 69-73ページ, 2014）。電池内での金属粒子の局所的な密度、組成、または濃度、すなわち金属粒子の空間的分布は、確率過程の結果であるため、異なる電池を調べることによって得られる鍵は、非常に高い確率で相違する。それにより、共有秘密鍵は、鍵の生成に用いられる電池もしくは電池の組み合わせに固有なものとして確立することができる。
【００１５】
この目的を達成するため、通信機器の各々は、金属粒子から生じる空間的に変化する磁界を、アレイ内のセンサ数によって決定される空間解像度で測定することを可能にする磁界センサのアレイを用いて、同一電池内の金属粒子の空間的に変化する密度を測定する。鍵を得るために用いられる値は、測定された磁界の空間的変化を表している。
【００１６】
第１の電池から生じる空間的に変化する磁界は、第１の電池、従ってその中に含まれる金属粒子が受ける励起磁界に応じて発生する。励起磁界は、渦電流が金属粒子内で励起されるように電池を貫く。この励起場は例えば通信機器の１つによって生成されてよく、その後、通信機器のそれぞれが空間的に変化する磁界を他の通信機器とは独立して測定する。それに変わる方法として、通信機器のそれぞれが渦電流を金属粒子内で励起するための励起磁界を生成し、その後、得られた空間的に変化する磁界を、１回に１つの機器で測定する。
【００１７】
電池内の金属粒子の空間分布は時間とともに変化するため、鍵の同一コピーは、第１の通信機器が鍵を生成してから所定時間の間だけ再生成することができる。それにより、後の段階で鍵の同一コピーを生成する可能性が限定される。時間間隔は、電池がうける充放電サイクルの速度によって決定される金属粒子の成長速度、および、測定された空間的に変化する磁界を表す値から鍵を得るために用いられるアルゴリズムによって決定される。好適なことに、これは、２つの通信機器によって生成される共有秘密鍵が、限定された時間間隔の間だけ再生成可能であることの保証である。これにより、悪意のある機器が鍵の同一コピーを後の時点で生成することをより難しくする。
【００１８】
さらに、本発明の実施形態に従って共有秘密鍵を確立する少なくとも２つの通信機器は

、限定された時間間隔の間、通信機器のそれぞれが同一鍵のコピーを得る同一の電池に近接することを必要とするため、共有秘密鍵が確立される際に少なくとも２つの通信機器が近接していることを保証することができる。従って、悪意のある機器が共有秘密鍵のコピーを生成するリスクが低減される。

【００１９】

センサアレイから取得された一式の値は鍵またはセキュリティトークン、例えばバイナリビットストリングまたはビット以外のシンボルのストリングに変換され、セキュリティアプリケーション用のアルゴリズム、特には暗号化、暗号復号、署名、ハッシングなどに用いられてよい。多くの場合に一式の実数または複素数によって表現可能な測定された物理量から、ビットストリングまたはシンボルのストリングへの実際の変換は、ビット／シンボル抽出アルゴリズムによって実行されてよい。ＰＵＦの技術分野では、以下でさらに説明する周知のアルゴリズムがいくつか存在する。

【００２０】

測定値を鍵に変換するために用いられるアルゴリズムは、アルゴリズムの入力として用いられる値の小さな変化に実質的に影響されないことが好ましく、第１の電池の近くに存在する際に双方の通信機器がかなりの高確率で同一の鍵を生成することを可能にすべきである。例えば、鍵は基数変換(base conversion)を用いて、一式の値から得ることができる。測定ノイズなどに対する耐性(resilience)を向上させるため、必要に応じて最上位ビットだけを用いることができる。あるいは、空間的に変化する磁界を表す一式の値の各値がセンサアレイの別個のセンサで測定される場合、一式の値のうち、１つ以上の選択された値を測定したセンサの１つ以上のインデックスに基づいて、一式の値から鍵を得てもよい。一例として、一式の値の最小値、最大値、平均値、または中間値といった統計値の１つ以上を特定することができ、それらの値を測定したセンサの各インデックスを鍵の取得に用いることができる。別の例として、全ての値を、昇順、降順、または他の任意の順序で並べることができ、対応するセンサインデックスを鍵の取得に用いることができる。インデックスは、センサアレイ内のセンサの順序に従って割り当てられることが好ましい。

【００２１】

本発明の一実施形態によれば、第１の電池は通信機器に含まれる。すなわち、通信機器は自身の内蔵電池から鍵を取得する。同様に、通信機器が共有秘密鍵を確立しようとする他の通信機器は、第１の電池から発生する空間的に変化する磁界を、自身のセンサアレイを用いて測定することによって鍵のコピーを得ることができる。

【００２２】

本発明の一実施形態によれば、測定された磁界は、励起磁界を受けた際に、第１の電池に含まれる金属粒子の第１の空間的に変化する密度と、第２の電池に含まれる金属粒子の第２の空間的に変化する密度とから発生する。第２の電池は他の通信機器に含まれる。第１の電池と同様、第２の電池はリチウムイオンまたはリチウムポリマータイプであってよく、金属粒子はリチウムデンドライトであってよく、金属粒子の第２の空間的に変化する密度は経時変化してよい。本発明のこの実施形態は、共有秘密鍵が２つの電池もしくはこれらの電池を有する２つの通信機器の組み合わせに固有であるという点で有利である。これによって、悪意のある機器によって鍵のコピーが生成されるリスクがさらに軽減される。

【００２３】

本発明の一実施形態によれば、通信機器は、励起磁界を生成するための磁界発生器をさらに有する。磁界発生器は、例えばコイルと、このコイルを流れる電流を駆動するように構成された電源とであってよい。有利なことに、無線充電を目的として設けられているインダクタコイルを利用することができる。そのために、通信機器は第１の電池（必要に応じてさらに第２の電池）に含まれる金属粒子に渦電流を励起するための励起磁界を発生させる。必要に応じて、励起磁界は、通信機器の近くに他の通信機器が検出されたことに応じて発生されてもよい。あるいは、通信機器のユーザからの指示を受信したことに応じて励起磁界が発生されてもよい。例えば、ユーザは、共有秘密鍵の確立を開始するために、

ボタンを押下したり、アプリケーションを起動したり、機器を振ったり、ジェスチャを実行したりすることができる。さらに別の代替構成として、他の通信機器から要求を受信したことに応じて励起磁界が発生されてもよい。例えば、他の通信機器はセキュアな通信セッションの確立を要求することができる。これは、他の通信機器が磁気発生器を有しない場合、あるいは、通信機器のそれぞれが共有秘密鍵を確立するための自律的なプロセスを実行する場合に特に有利である。

【００２４】

本発明の別の実施形態によれば、他の通信機器によって励起磁界が発生されてよい。必要に応じて、他の通信機器で発生された励起磁界を検出したことに応じて、センサアレイから一式の値が取得されてよい。センサアレイは例えば、一式の値の要求を受信したことに応じて、または励起磁界が検出されたことに応じて、空間的に変化する磁界を測定することができる。あるいは、空間的に変化する磁界は、連続的もしくは周期的に測定されてもよい。

【００２５】

２つの通信機器が本発明の実施形態に従って共有秘密鍵を確立するために近づけられる場合、通信機器の少なくとも１つが、第１の電池（および、必要に応じて第２の電池）内に渦電流を励起するための磁気生成器を有し、その後、空間的に変化する磁界が両方の通信機器によって測定される。代替構成として、通信機器のそれぞれが、他の通信機器とは独立した処理において励起磁界を発生させ、その後、空間的に変化する磁界を測定することができる。

【００２６】

本発明の利点をいくつかのケースについて本発明の第１の態様の実施形態に関して説明してきたが、類似の考え方は本発明の他の態様の実施形態についても当てはまる。さらに、本発明の実施形態は、空間的に変化する磁界の測定中に同一の電池の近くに存在する２つ以上の通信機器によって共有秘密鍵として用いるための鍵を確立するために用いることができる。

【００２７】

本発明の他の目的、特報、および利点は、以下の詳細な説明、図面、および特許請求の範囲を精読することによって明らかになるであろう。本技術分野に属する当業者は、以下で説明する実施形態とは異なる実施形態を生み出すために本発明のさまざまな特徴を組み合わせることができることを理解する。

【００２８】

上述したものに加え、本発明のさらなる目的、特徴、および利点は、添付図面に関する以下の例示的かつ非限定的な詳細な説明を通じてよりよく理解されるであろう。

【図面の簡単な説明】

【００２９】

【図１】本発明の一実施形態に係る、近接する２つの通信機器の上面図および側面図である。

【図２】本発明の一実施形態に係る通信機器の上面図および側面図である。

【図３】本発明の一実施形態に係る、近接する２つの通信機器による鍵の生成を示す図である。

【図４】本発明の別の実施形態に係る、近接する２つの通信機器による鍵の生成を示す図である。

【図５】本発明の実施形態に係る、センサアレイ内のセンサにインデックスを割り当てるさまざまな方法を示す図である。

【図６】通信機器に含まれる処理手段の一実施形態を示す図である。

【図７】通信機器に含まれる処理手段の別の実施形態を示す図である。

【図８】本発明の一実施形態に係る、通信機器の方法を示すフローチャートである。

【００３０】

全ての図面は模式であり、必ずしも縮尺されておらず、さらに一般的には本発明を説明

するために必要な部分だけを示し、他の部分は省略されているか、示唆されるにすぎない。

【発明を説明するための形態】

【００３１】

以下、本発明の所定の実施形態を示す添付図面に関して本発明をより十分に説明する。しかしながら、本発明は多くの異なった形態で実施することができ、ここで説明する実施形態に限定されるように解すべきではない。むしろこれらの実施形態は、本開示が徹底的かつ完全となり、本発明の範囲を本技術分野の当業者に十分に伝えるように例として提供されている。

【００３２】

暗号技術は機器間のセキュアな通信のために広く用いられている。暗号化方法の１種は、大きな整数の因数分解や離散対数といった、現在利用可能な計算能力のレベルでは解くのが困難であろうと考えられる基本的な数学的問題に基づく対称暗号化方法である。公開鍵および秘密鍵に基づく実用的なしくみは今日広く用いられているが、必要とされる計算能力が、例えばＭ２Ｍ機器のように電池容量または処理能力に制限のある、制約された機器においては利用可能でないかもしれないという欠点がある。

【００３３】

暗号化方法の別の一種は対称暗号化に基づく。一例は、好ましくはランダムなビットストリングがメッセージを安全に交換することを望む２つの機器間の共有秘密鍵として用いられるワンタイムパッド法である。第１の機器は符号化メッセージを形成するため、メッセージとランダムビットストリングとの排他的論理和を実行することができる。そして符号化メッセージは第２の機器に送信され、第２の機器は受信メッセージとランダムビットストリングとの排他的論理和を実行することによって受信メッセージを復号する。ワンタイムパッド法は公開鍵暗号化といった非対称法よりも強いセキュリティの概念を提供する。さらに、必要とされる計算の程度は比較的低く、そのためこの方法は制約された機器での実施に好適である。この方法の主な欠点は、通信セッションに関与する全ての機器の間で共有秘密鍵として用いられるランダムビットストリングを、悪意のある機器に明かすことなく配信する必要があることである。

【００３４】

以下では、他の通信機器との通信において共有秘密鍵として用いるための鍵を生成するための通信機器の実施形態を説明する。

【００３５】

図１において、本発明の実施形態に係る、近づけられた２つの通信機器１１０および１２０が上面図（最上部）および側面図で示されている。通信機器１１０および１２０のそれぞれは、以下でさらに詳細に説明する図２に示す通信機器２００の一実施形態であり、例えば移動端末、ＵＥ、スマートフォン、ウェアラブルデバイス、タブレット、スマートウォッチ、ＰＯＳでのキャッシュレジスタまたは支払い端末、センサまたはアクチュエータ、またはラップトップコンピュータといったＭ２Ｍ機器であってよい。通信機器１１０および１２０の１つは、例えば自動車、トラック、バス、船、鉄道、飛行機、またはドローンといった車両、あるいは例えば白物家電、ドアロック、監視および警報機器、または自律掃除機および芝刈り機である家電製品に含まれてよい。

【００３６】

本発明の実施形態は、通信機器１１０および１２０のような２つの通信機器の間のセキュアな通信で共有秘密鍵として用いることのできる鍵を生成するために、空間的に変化する、第１の電池（および必要に応じて第２の電池）内の金属粒子の密度を利用する。第１の電池および第２の電池は例えば、経時的にリチウムデンドライトを成長させることで知られているリチウムポリマーまたはリチウムイオン電池であってよい。特に、第１の電池および必要に応じて第２の電池は、通信機器１１０および１２０にそれぞれ含まれることが好ましい。つまり、第１の電池および第２の電池は図１に示される電池１１３および１２３に対応する。あるいは、対応関係が逆であってもよい。

【００３７】
第１の電池に含まれる金属粒子の、第１の空間的に変化する密度（さらに、必要に応じて第２の電池に含まれる金属粒子の、第２の空間的に変化する密度）は、好ましくは通信機器１１０および１２０の少なくとも１つが有する磁界生成器１１４／１２４によって発生される、例えば磁界パルスまたは交流(ac)磁界である励起磁界を用い、金属粒子に渦電流を励起することによって調べることができる。渦電流は、第１および第２の電池内の金属粒子の空間的に変化する密度に起因する、空間的に変化する磁界を引き起こす。空間的に変化する磁界を測定することにより、第１の電池内の金属粒子の空間的に変化する密度、あるいは金属粒子の第１の空間的に変化する密度および金属粒子の第２の空間的に変化する密度の組み合わせ、を表す一式の値を取得することができる。リチウムデンドライトの場合のように、金属粒子が確率過程の結果であれば、電池内における金属粒子それぞれの空間的に変化する密度、または空間的な分布は唯一無二である。従って、測定値はＰＵＦからの応答であり、その値から、共有秘密鍵として用いるための無作為な鍵または秘密トークンを得ることができる。

【００３８】
磁界に基づく金属検知技術の基本的な概念は１９３０年代にさかのぼるが、デジタル信号処理の登場とともに進化している。金属探知器は一般に２つのコイルまたはインダクタを有し、第１のインダクタには磁界、すなわち励起磁界が発生するように電流が流される。生成される磁界は、励起磁界を受けるすべての金属粒子に渦電流を誘導する。そして渦電流は磁界を発生させ、この磁界は第２のインダクタで傍受され、測定されてよい。得られた信号は、異なる金属粒子を検出ならびに区別するために用いることのできる特徴的な構成を有する。

【００３９】
金属探知器に関して２つの基本的な動作モードを区別することができる。第１の動作モードはパルス誘導検知モードである。このモードでは、励起磁界強度が有限期間の（おそらく周期的な）パルス形状を有する。測定される磁界強度は、励起磁界強度の後に、パルスのほぼ終わりまで続く。その時点で、測定される磁界強度は特徴的な減衰を示す。減衰形状および減衰時間は、存在する金属粒子の量およびタイプに依存する。第２の動作モードは連続波検知モードであり、周期的に変化する励起磁界が用いられる。このモードでは、励起磁界と測定された磁界との振幅および位相の差が、存在する金属粒子の量およびタイプを反映する。

【００４０】
図１に示すように、通信機器１１０および１２０は、本発明の実施形態に従って、両者間の通信における共有秘密鍵として用いるための鍵を生成するために互いに近づけられている電池１１３および１２３の１つまたは両方の中の金属粒子から発生する空間的に変化する磁界を測定できるようにするため、通信機器の一方が有するセンサアレイ１１１／１２１が、通信機器のもう一方が有する電池１２３／１１３から発生する空間的に変化する磁界を測定できるように通信機器１１０および１２０を互いに配置する必要がある。さらに、第１の通信機器１１０が励起磁界を発生させるための磁界発生器１１４をさらに有する場合、測定可能な強度の磁界を引き起こす渦電流を励起するように、通信機器１１０および１２０は、発生された励起場が第２の通信機器の有する電池１２３を貫くように相対配置されるべきである。図１において、これは領域１３０によって図示されており、この領域は、本発明の実施形態に従って鍵を生成することを容易にするように、通信機器１１０および１２０の位置合わせにおいてユーザを誘導するために、通信機器１１０および１２０の表面に示されてもよいし、通信機器１１０および１２０のディスプレイまたはタッチスクリーン（図２には示していない）に表示されてもよい。実際には、領域１３０は、通信機器１１０または１２０の中で、センサアレイ１１１／１２１（さらに必要に応じて電池１１３／１２３および／または磁界発生器１１４／１２４）がそれぞれ配置されている場所を示している。センサアレイ１１１／１２１（および必要に応じて電池１１３／１２３および／または磁界発生器１１４／１２４）は、通信機器１１０／１２０の外表面に

、あるいは外表面の近くに設けられるのが好ましいことが理解されるであろう。通信機器１１０／１２０の一実施形態が自動車などの車両に含まれる場合、センサアレイ１１１／１２１（および必要に応じて磁界発生器１１４／１２４）は例えばダッシュボードに設けられてよい。あるいは、通信機器１１０／１２０の実施形態が白物家電のような家電製品に含まれる場合、センサアレイ１１１／１２１（および必要に応じて電池１１３／１２３および／または磁界発生器１１４／１２４）は白物家電のコントロールパネルに設けられてよい。

【００４１】

発明をさらに説明するために、近づけられた通信機器１１０および１２０を図３および図４に再び示す。ここでは、第１の電池（および必要に応じて第２の電池）内の金属粒子の空間的な分布を調べることに基づいて鍵を生成する過程を示す（側面図のみ）。

【００４２】

図３において、第１の通信機器１１０は、センサアレイ１１１、第１の電池１１３、および磁界発生器１１４を有し、第２の通信機器１２０はセンサアレイ１２１を有するものとして示されている。第１の通信機器１１０は、例えばスマートフォンであってよく、第２の通信機器１２０は販売場所(point-of-sale)での支払い端末である。支払い端末は電池を持たず、電源によって給電されてもよい。通信機器１２０が車両や家電製品で実施される場合も同様である。従って、スマートフォン１１０および支払い端末１２０のそれぞれは、第１の電池１１３内の金属粒子の第１の空間的に変化する密度を調べることによって鍵を生成することができる。そのために、図３の上側に示す励起フェーズの間、磁界発生器１１４は第１の電池１１３を貫く励起磁界３１０を発生させる。励起磁界３１０は例えば磁界パルスまたは交流磁界であってよい。励起磁界３１０に応じて、第１の電池１１３に含まれる金属粒子に渦電流が励起され、渦電流は、図３の下側に示す、空間的に変化する磁界３２０を引き起こす。空間的に変化する磁界３２０は、第１の電池１１３内の金属粒子の空間的に変化する密度を表す。空間的に変化する磁界３２０は第１の通信機器１１０に含まれるセンサアレイ１１１によって、さらに、実質的に同時に、第２の通信機器１２０に含まれるセンサアレイ１２１によって、測定されてよい。あるいは、センサアレイ１１１および１２１の一方が、第１の励起磁界３１０に引き続いて、空間的に変化する磁界３２０を測定し、もう一方のセンサが、第２の励起磁界３１０に引き続いて、空間的に変化する磁界３２０ををを測定してもよい。

【００４３】

図４は、第２の通信機器１２０が電池、すなわち第２の電池１２３を有するように図示されていることをのぞき、図３と同様である。図４に示した構成は、例えば通信機器１１０および１２０の両方がスマートフォンである場合に当てはまる。従って、第１および第２のスマートフォン１１０および１２０はそれぞれ、第１の電池１１３に含まれる金属粒子の第１の空間的に変化する密度と、第２の電池１２３に含まれる金属粒子の第２の空間的に変化する密度との組み合わせを調べることによって鍵を生成することができる。センサアレイ１１１および１２１は、電池１１３および１２３からの寄与を分離することができず、総磁界だけを測定できるからである。そのため、図４の上側に示した励起フェーズの間、磁界発生器１１４は第１の電池１１３および第２の電池１２３を貫く励起磁界４１０を発生させる励起磁界４１０は例えば、磁界パルスまたは交流磁界であってよい。励起磁界４１０に応じて、第１の電池１１３および第２の電池１２３に含まれる金属粒子に渦電流が励起され、渦電流は、図４に下側に示す、空間的に変化する磁界４２０および４３０をそれぞれ引き起こす。空間的に変化する磁界４２０および４３０は、第１の電池１１３内の金属粒子の空間的に変化する密度および第２の電池１２３内の金属粒子の空間的に変化する密度をそれぞれ表す。空間的に変化する磁界４２０および４３０の組み合わせは、第１の通信機器１１０に含まれるセンサアレイ１１１によって、さらに、実質的に同時に、第２の通信機器１２０に含まれるセンサアレイ１２１によって、測定されてよい。あるいは、センサアレイ１１１および１２１の一方が、第１の励起磁界４１０に引き続いて、空間的に変化する磁界４２０および４３０を測定し、もう一方のセンサアレイが、第２

の励起磁界４１０に引き続いて、空間的に変化する磁界４２０および４３０を測定してもよい。

【００４４】

第１の電池１１３（および必要に応じて第２の電池）から発生する、空間的に変化する磁界の測定につづき、通信機器１１０および１２０のそれぞれは、自身のセンサアレイ１１１／１２１から取得した一式の値から鍵を取得する。第１の電池１１３および第２の電池１２３に関する、磁界発生器１１４のような励起磁界源の相対配置が異なることに加え、第１の電池１１３および第２の電池１２３に関するセンサアレイ１１１および１２１の相対配置が異なることにより、センサアレイ１１１および１２１によって測定される磁界は同一でない。しかし、最新の通信機器、特にスマートフォン、タブレット、ラップトップコンピュータには平坦な形状を有するタイプの電池が一般に設けられていること、また、励起磁界３１０／４１０が近接場において実質的に均一であるように磁界発生器を設計可能であることから、第１の電池１１３内の金属粒子が受ける励起磁界の強度と、第２の電池１２３内の金属粒子が受ける励起磁界の強度との差は無視できる。同様に、外部電池１２３／１１３と比較して、内蔵電池１１３／１２３に対するセンサアレイ１１１／１２１の適切な配置により、センサアレイ１１１およびセンサアレイ１２１によって実行される測定間の差は十分に小さい。

【００４５】

さらに図３および図４に関して、第２の通信機器１２０が有する磁界発生器１２４は、第１の通信機器１１０が有する磁界発生器１１４の代わりに、あるいはそれに加えて用いられてよい。例えば、第１の通信機器１１０によって発生された励起磁界を用いるのではなく、本発明の実施形態は第２の通信機器１２０によって発生された励起磁界を用いることができる。特に、センサアレイ１１１および１２１が空間的に変化する磁界３２０または，４２０および４３０を同時に測定しない場合、通信機器１１０および１２０のそれぞれは別個の処理によって鍵を生成することができる。より具体的には、第１の通信機器１１０は磁界発生器１１４を用いて励起磁界３１０または４１０を発生させ、その結果得られる、空間的に変化する磁界３２０または、４２０および４３０を測定することができ、この磁界に基づいて第１の通信機器１１０は鍵を取得する。その後、第２の通信機器１２０は自身の磁界発生器１２４（図３および図４には不図示）を用いて励起磁界を発生させ、その結果得られる空間的に変化する磁界を測定することができる。この磁界に基づいて第２の通信機器１２０は鍵を取得する。

【００４６】

図２に関して、通信機器１１０および１２０のような他の通信機器との通信で共有秘密鍵として用いるための鍵を生成するための通信機器の実施形態２００をより詳細に説明する。

【００４７】

通信機器２００は、他の通信機器との通信を達成する通信インタフェース２０５と、第１の電池から発生する空間的に変化する磁界を測定するためのセンサアレイ２０１と、処理手段２０６とを有する。

【００４８】

通信インタフェース２０５は例えば、イーサネットカードのようなネットワークインタフェース、ユニバーサルシリアルバス(USB)、FireWire、ライトニングのようなシリアルまたはパラレルポート、または、ＧＳＭ(Global System for Mobile Communications)、ＵＭＴＳ(Universal Mobile Telecommunications System)、またはＬＴＥ(Long Term Evolution)、無線ローカルエリアネットワーク(WLA)/ WiFi、ブルートゥース、近距離無線通信(NFC)技術、ZigBeeなどのようなセルラモバイルネットワークを通じた通信をサポートする無線インタフェースであってよい。

【００４９】

センサアレイ２０１は、インダクタ、磁気抵抗センサ、ホール効果センサ、スピントランジスタ、フラックスゲート、磁気電気センサ、および磁気光学センサのいずれか１つ、

または組み合わせに基づく複数のセンサ２０２を有する。センサアレイ２０１でのセンサ２０２の空間配置に起因して、空間的に変化する磁界を、アレイ２０１内のセンサ２０２の数および／または各センサ２０２の領域によって決定される空間解像度で測定することができる。より具体的には、各センサ２０２は、包含する磁力線に対応する、空間的に変化する磁界を測定してよい。磁界の変化の大きさはリチウムデンドライトの密度に依存するため、各センサ２０２の出力は局所的なリチウムデンドライトの密度を表す。センサアレイ２０１は、通信機器に含まれる電池２０３および、通信機器の近くにある他の通信機器に含まれる電池（すなわち、図１に示した電池１１３および１２３の一方または両方）の１つまたは両方から発生する空間的に変化する磁界への寄与を測定することができるように配置される。

【００５０】

第１の電池は、第１の電池を貫く励起磁界を受けた際に空間的に変化する磁界を引き起こす、金属粒子の第１の空間的に変化する密度を有する。第１の電池は、電池２０３のように通信機器２００に含まれてもよいし、他の通信機器に含まれてもよい。必要なら、測定される磁界は、金属粒子の第１の空間的に変化する密度および、他の通信機器に含まれる第２の電池に含まれる金属粒子の第２の空間的に変化する密度から発生するものであってよい。第２の電池は第１の電池と同じタイプであっても、違うタイプであってもよい。

【００５１】

通信機器２００は、金属粒子の第１の空間的に変化する密度（および必要に応じて金属粒子の第２の空間的に変化する密度）に渦電流を励起するために用いられる励起磁界を生成するための磁界発生器２０４をさらに有してよい。励起磁界は例えば磁界パルスまたは交流磁界であってよい。磁界発生器２０４は例えばインダクタコイルおよびコイルと流れる電流を駆動するために構成された電源とを有してよい。磁界発生器２０４は、発生された励起磁界が通信機器２００に含まれる電池２０３と、通信機器２００の近くにある他の通信機器が有する電池との少なくとも一方を貫く励起磁界を生成するように配置される。有利なことに、無線充電用に設けられているインダクションコイルを、励起磁界を発生させるために用いることができる。

【００５２】

磁界パルスまたはパルス列が励起磁界として用いられる場合、通常、各パルスの期間は数十ミリ秒のオーダであり、一方でパルス列の繰り返し周波数は数百ヘルツのオーダであってよい。金属粒子に励起される渦電流から発生する空間的に変化する磁界の全般的な振る舞いは、励起磁界と非常によく似ている。しかし、励起磁界が消滅した後、測定される、空間的に変化する磁界の減衰は、金属粒子の密度およびタイプに依存する。測定される減衰している磁界の減衰時間は、例えば測定される磁界強度が最大値の９０％から１０％に減衰するのに要する時間として規定することができる。パルスの減衰時間は第１の電池（必要に応じてさらに第２の電池）内のリチウムデンドライトのような金属粒子の局所的な密度に比例する。

【００５３】

別の方法は連続波検知の利用である。その場合、磁界発生器２０４は正弦曲線的な強度を有する励起磁界を発生させる。その結果、測定される、空間的に変化する磁界もまた、１つ以上の正弦曲線成分を含む。しかし、正弦曲線成分のそれぞれの位相および振幅は金属粒子の密度に依存するため、センサ２０２で測定される磁界の振幅および位相、すなわち複素数値は、鍵の取得に用いることができる。

【００５４】

必要に応じて、他の通信機器の接近を検出したことに応じて励起磁界を発生させるようにしてもよい。例えば、図３および図４に関し、第１の通信機器１１０に含まれる磁界発生器１１４は第２の通信機器１２０の接近を検出したことに応じて励起磁界３１０または４１０を発生させてもよい。これは例えば、第２の通信機器１２０によって送信され、第１の通信機器１１０によって受信される無線信号またはビーコンの信号強度が、閾値を超えたことの判定によって実現することができる。あるいは、励起磁界の発生を周期的に、

またはタイマが満了した際に開始するようにしてもよい。励起磁界の発生だけでなく、鍵の生成またはセキュアな通信の確立の全体的な手順が、他の通信機器の接近の検知、周期的、あるいはタイマの満了に応じて開始されてよいことは理解されるであろう。

【００５５】

磁界発生器２０４は、必要に応じて、通信機器２００のユーザからの指示を受信したことに応じて励起磁界を発生させてもよい。例えば、ユーザはボタンを押下したり、スマートフォン２００でアプリケーションを開始したり、通信機器２００を振ったり、またはジェスチャを行ったりすることができる。同様に、鍵の生成またはセキュアな通信の確立の全体的な手順が、そのようなユーザ指示の受信に応じて開始されてもよい。さらに必要に応じて、磁界発生器２０４は、他の通信機器からの要求の受信に応じて励起磁界を発生させてもよい。例えば、図３および図４に関して、第１の通信機器１１０に含まれる磁界発生器１１４は、第２の通信機器１２０からの要求を通信インタフェース２０５を通じて受信したことに応じて励起磁界３１０または４１０を発生させてもよい。この要求は例えば、通信機器１１０および１２０の間のセキュアな通信セッションの確立に関するものであってもよいし、共有秘密鍵を確立することの要求に関するものであってもよい。

【００５６】

本発明の別の実施形態によれば、励起磁界は他の通信機器が発生する。例えば、第１の通信機器１１０が有する磁界発生器１１４によって発生された励起磁界３１０または４１０に応じてそれぞれ生じる、空間的に変化する磁界３２０または、４２０および４３０を測定する、図３および図４に示す第２の通信機器１２０について当てはまる。

【００５７】

通信機器２００が有する処理手段２０６は、センサアレイ２０１から一式の値を取得し、一式の値から鍵を取得するように動作可能である。値は、空間的に変化する磁界、特には測定された磁界の空間的な変化を表す。通信機器２００または他の通信機器によって発生される励起磁界の検出に応じて、あるいは処理手段２０６による要求に応じて、センサアレイ２０１は空間的に変化する磁界を測定することができ、処理手段２０６はセンサアレイ２０１から一式の値を継続的または周期的に取得することができる。すなわち、処理手段２０６は、励起磁界を発生するために磁界発生器２０４を制御するようにも動作可能である。

【００５８】

加えて、処理手段２０６は共有秘密鍵として生成された鍵を、他の通信機器との通信に用いるようにも動作可能である。例えば、通信機器１１０および１２０のような２つの通信機器は、互いに同一の鍵を生成していることを確認するためにセキュアな通信セッションの確立を試みることができる。セキュアな通信セッションは２つの通信機器間で直接確立されてもよいし、売り場での金融取引を実現するためのサーバまたはブローカのようなサードバーティを通じて確立されてもよい。

【００５９】

処理手段２０６は、複数の選択肢を用いて一式の値から鍵を取得するように動作可能であってよい。この文脈において、鍵（セキュリティトークンと呼ばれることもある）はビット、文字、または他の種類のシンボルのストリング、ベクトル、シーケンス、またはアレイであり、暗号化、暗号復号、署名、ハッシングなどのセキュリティ用途に用いることができる。

【００６０】

例えば、鍵は基数変換によって一式の値から取得することができる。ここでは、センサアレイ２０１から取得された一式の値がＮ個の値を有するものとする。値のそれぞれは、例えばセンサアレイ２０１のＮ個のセンサ２０２の１つに対応してよい。鍵を生成するため、Ｎ個の値のそれぞれはｋビットの二進数として表されてよく、結果として、一式の値からは合計Ｋ＝ｋＮビットが抽出されてよい。測定ノイズなどへの耐性を強化するために、最上位ビットだけを用いてもよい。

【００６１】

特に向きなどが微妙に変化する状況下で２つの通信機器で鍵の同一のコピーを生成する、より信頼できる方法を提供するため、一式の値から鍵を取得するためにより洗練された方法を用いることができる。例えば、Ｎ個の値を直接バイナリ形式に変換する代わりに、ノイズおよび他の測定アーチファクトに対してより強い耐性を提供する、一式の値の特性に基づいて鍵を取得してもよい。そのような特定は例えば最小値、最大値、平均値など、一式の値の統計的な特性、または一式の値に課された順序であってよい。そして、センサアレイ２０１内のセンサ２０２のそれぞれのインデックスまたは位置に基づいて鍵を取得することができる。

【００６２】

より具体的には、一式の値の各値が、センサアレイ２０１の各センサ２０２によって測定された空間的に変化する磁界を表し、センサアレイ２０１の各センサ２０２には、センサアレイ２０１内の位置に関するインデックス識別子が関連付けられているものとする。センサアレイ２０１内のセンサ２０２にインデックスを割り当てる別の方法を図５に示す。第１の例５１０として、センサ２０２は列優先(row-major)順に従って最小インデックス（例えば１）から最大インデックス（例えばセンサアレイ２０１内のセンサ２０２の最大数で、図５では１２としている）までインデックス付けされてよい。第２の例５２０として、センサ２０２は最小インデックスから最大インデックスまで行優先(column-major)順でインデックス付けされてよい。第３の例５３０として、センサ２０２はアレイまたは行列スタイル表記「ｎ，ｍ」に基づいて特定されてもよい。ここでｎは所定のセンサの行のインデックス、ｍはセンサアレイ２０１のそのセンサの列のインデックスである。最後に、第４の例５４０として、インデックスｎおよびｍの順序を反転してもよい。すなわち、センサ２０２は「ｍ，ｎ」として特定される。

【００６３】

このようにするため、処理手段２０６は、一式の値から１つ以上の値を選択し、１つ以上の選択した値を測定したセンサ２０２の１つ以上のインデックスに基づいて鍵を取得することにより、一式の値から鍵を取得するように動作可能である。

【００６４】

例えば、センサアレイ２０１から取得された一式の値の最小値および最大値を選択してもよい。その後、それらの値を測定したセンサ２０２のインデックスが調べられる。一例として、センサ２０２が順序５１０に従ってインデックス付けされており、（塗りつぶされた四角でマークした）インデックス「３」を有するセンサが最小値を、（塗りつぶされた円でマークした）インデックス「１０」を有するセンサが最大値を測定したものとする。そして、これら２つのインデックスから鍵が、例えば最小値に対するインデックスのバイナリ表記「００１１」（最大１６のセンサまでを考慮した４ビット表記を仮定し、0・8+0・4+1・2+1・1=3である）と、最大値に対するインデックスのバイナリ表記「１０１０」との連続、すなわち「００１１１０１０」として得られる。別の例として、センサが順序５４０に従ってインデックス付けされている場合、上述した２つのセンサはそれぞれインデックス「３，１」および「２，３」で特定される。この場合、行および列インデックスのそれぞれに関する（最大４つの行および列を考慮した）２ビット表現を用いて、最小値に関するインデックスはバイナリ表記で「１１０１」である（行インデックスのバイナリ表記1・2+1・1=3と、列インデックスのバイナリ表記0・2+1・1=1の連続）。また、最大値に関するインデックスはバイナリ表記で「１０１１」であり、それらは例えば連結されて鍵「１１０１１０１１」になる。センサアレイ２０１内のセンサ２０２の順序を反映するインデックスを用いる、センサ位置に基づく鍵の取得は、測定ノイズおよび機器の向きなどによる変動などに対する感受性が低いという点で鍵の生成において有利である。

【００６５】

鍵取得アルゴリズムは最小値および最大値だけでなく、一式の値の順序に従った他の値を含むように拡張されうることもまた理解されよう。例えば、Ｎ個の値全てを昇順または降順に並び替えることができ、対応するセンサインデックス列を鍵の取得に用いることができる。例えば、昇順または降順で並び替えされた測定値に関連付けられたインデックス

を連結して鍵にすることができる。図５に示したセンサアレイに関して、Ｎ＝１２のセンサインデックスを表すには４ビットが必要であるため、この方法ではＫ＝４Ｎビット、すなわち４８ビットの鍵が得られるであろう。

【００６６】

必要に応じて、センサアレイ２０１から取得された全測定値を、最大値、最小値、平均値、移動平均値などを用いてスケーリングしてもよい。一式の値から鍵を取得するために用いられるアルゴリズムは小さな変動に鈍感であるべきであり、それによって両方の通信機器において非常に高い確率で同じ鍵が生成されることを可能にする。

【００６７】

さらなる改良として、第２の通信機器１２０に含まれる電池１２３を調べるために、第１の通信機器１１０に含まれるセンサアレイ１１１が用いられる場合、通信機器１１０および１２０の相対的な平行移動に対して所定レベルの不変性をもって鍵を取得できることが望ましい。これは、電池より表面積が大きなセンサアレイ１１１を用い、鍵を取得するためにセンサアレイ１１１のセンサのサブセットだけを選択することによって実現することができる。例えば、センサのサブセットは、電池１２３の外周に対応する外周に含まれるものを選択することができる。

【００６８】

ＰＵＦの技術分野において、測定状況におけるノイズおよび変動にとって信頼できるビット抽出アルゴリズムが知られている。そのようなアルゴリズムの１つはＬＩＳＡアルゴリズムである（ C.-E. D. Yin and G. Qu, ”LISA: Maximizing RO PUF's secret extraction”, in 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 100-105ページ, 2010）。このアルゴリズムは、測定のセットの個々の値はそれほど安定していないかもしれないという知見に基づく。実施形態でいえば、例えば通信機器１１０および１２０の相対的な向きによって個々の値が変化しうるということであってよい。個々の値を考慮するよりも、アルゴリズムは、より離れたセンサ２０２によって測定された値の組を用いる。そして、１組の値の差の符号を、１つのビットを抽出するために用いることができる。同じ組に属する値は遠く離れた位置で測定されているため、測定状況におけるノイズや変動に対する耐性が実現される。信頼できかつ安定した方法でビットを抽出するために用いることのできる代替アルゴリズムはＫＳＣ(Kendall Syndrome Coding)アルゴリズム(C.-E. Yin and G. Qu, ”Kendall Syndrome Coding (KSC) for Group-Based Ring-Oscillator Physical Unclonable Functions”, Technical report, University of Maryland, 2011)である。

【００６９】

さらに図２に関して、通信機器２００は、ディスプレイ、タッチスクリーン、１つ以上のキーまたはキーボード、カメラなどの追加構成要素を有することができる。

【００７０】

以下、処理手段２０６の実施形態６００を、図６に関して説明する。処理手段６００は、汎用プロセッサのような処理ユニット６０１と、ランダムアクセスメモリ(RAM)、フラッシュメモリなどのようなコンピュータ読み取り可能な記憶媒体６０２とを有する。さらに、処理手段６００は、センサアレイ２０１、磁界発生器２０４、通信インタフェース２０５、および必要に応じて１つ以上のキー、キーパッドまたはキーボードおよび、ディスプレイまたはタッチスクリーンといった追加の構成要素を制御したり、および／またはそれらから情報を受信したりするための１つ以上のインタフェース６０４（図６では「Ｉ／Ｏ」）を有する。メモリ６０２は、モバイル端末、ＵＥ、スマートフォン、ウェアラブル機器、タブレット、スマートウォッチ、キャッシュレジスタ、支払い端末、センサ、アクチュエータ、またはラップトップコンピュータなどの通信機器を、処理ユニット６０１でコンピュータ実行可能な命令６０３が実行された際に、ここで説明する本発明の実施形態に従って動作させるためのコンピュータ実行可能な命令６０３、すなわちコンピュータプログラムを含む。

【００７１】

図７は、通信機器２００が有する処理手段２０６の代替実施形態７００を示す。処理手段７００は、センサアレイ２０１から、センサアレイ２０１によって測定された空間的に変化する磁界を表す一式の値を取得するための取得モジュール７０２と、一式の値から鍵を取得するための鍵取得モジュール７０３と、センサアレイ２０１、磁界発生器２０、通信インタフェース２０５、および必要に応じて１つ以上のキー、キーパッドまたはキーボードおよび、ディスプレイまたはタッチスクリーンといった追加の構成要素を制御したり、および／またはそれらから情報を受信したりするための１つ以上のインタフェースモジュール７０４（図７では「Ｉ／Ｏ」）を有する。必要に応じて、処理手段７００は、他の通信機器の接近を検出するための近接モジュール７０１を有してもよい。近接モジュール７０１，取得モジュール７０２、および鍵取得モジュール７０３、さらには処理手段７００が有しうる追加モジュールは、ここで説明したような本発明の実施形態に従って動作するように構成される。

【００７２】

処理手段７００が有するモジュール７０１～７０４および任意の追加モジュールは、いかなる種類の電気回路、例えば、アナログ電気回路、デジタル電気回路、および適切なコンピュータプログラムを実行する処理手段のいずれか１つまたは組み合わせによって実施されてもよい。

【００７３】

以下、他の通信機器との通信において共有秘密鍵として用いるための鍵を生成するための、通信機器の方法の実施形態８００を、図８に関して説明する。

【００７４】

方法８００は、励起磁界を受けた際に、第１の電池に含まれる金属粒子の第１の空間的に変化する密度から発生する空間的に変化する磁界を測定すること８３１を有する。第１の電池は例えば通信機器が有することができる。空間的に変化する磁界は８３１でセンサアレイを用いて測定される。方法８００はさらに、センサアレイから一式の値を取得すること８３２を有し、この一式の値は、空間的に変化する磁界を表す。方法８００はさらに、一式の値から鍵を取得すること８３３を有する。

必要に応じて、測定される磁界は、励起磁界を受けた際に、金属粒子の第１の空間的に変化する密度および第２の電池に含まれる金属粒子の第２の空間的に変化する密度から発生する。第２の電池は第２の通信機器に含まれる。

【００７５】

方法８００は、励起磁界を生成すること８２１をさらに有してよい。必要に応じて、励起磁界は他の通信機器の近接を検出すること８１１に応じて発生８２１される。あるいは、励起磁界は通信機器のユーザからの指示を受信したこと８１２に応じて、あるいは他の通信機器から要求を受信したこと８１３に応じて生成８２１されてもよい。

【００７６】

方法８００の一実施形態によれば、励起磁界は他の通信機器によって発生されてもよい。必要に応じて、他の通信機器が発生した励起磁界を検出したこと８２２に応じてセンサアレイから一式の値が取得８３２される。

【００７７】

方法８００の一実施形態によれば、方法８００はさらに、他の通信機器との通信に鍵を共通暗号鍵として用いること８３５を有してもよい。必要に応じて、共通暗号鍵は検証されてもよい。すなわち、通信機器および他の通信機器が同一の鍵を生成していることが検証されてもよい。

【００７８】

方法８００の一実施形態によれば、鍵は基数変換を用いて一式の値から取得８３３される。

【００７９】

方法８００の別の実施形態によれば、一式の値の各値は、センサアレイの対応する１つのセンサによって測定された、空間的に変化する磁界を表し、鍵は、一式の値から１つ以

上の値を選択し、１つ以上の選択された値を測定したセンサの１つ以上のインデックスに基づいて鍵を取得することにより、一式の値から鍵を取得する８３３。

【００８０】

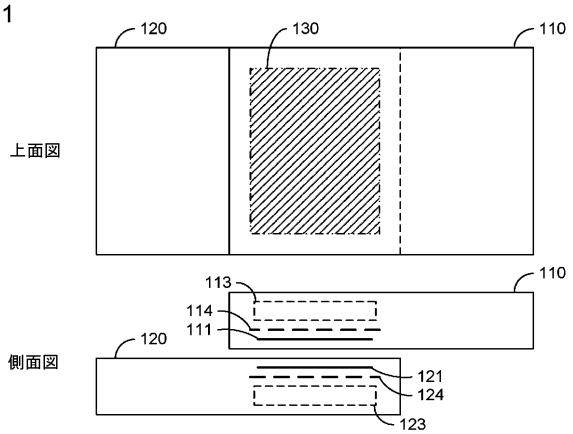
本開示を通じて記述されたことに従って、方法８００が追加の、あるいは変更されたステップを有しうることが理解されよう。方法８００は、モバイル端末、ＵＥ、スマートフォン、ウェアラブルデバイス、タブレット、スマートウォッチ、キャッシュレジスタ、支払い端末、またはラップトップコンピュータといった通信機器によって実行されてよい。方法８００の一実施形態は、通信機器２００が有する処理ユニット６０１によって実行されるコンピュータプログラム６０３のようなソフトウェアとして実施されてよく、それによって通信機器２００はここで説明した本発明の実施形態に従って動作することが可能である。

【００８１】

本技術分野に属する当業者には、本発明がここで説明した実施形態に決して限定されないことが明らかである。それどころか、添付した特許請求の範囲の範囲内で多くの変更や変化が可能である。

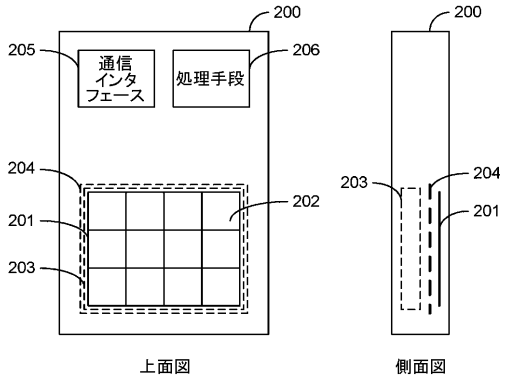
【図１】

Fig. 1



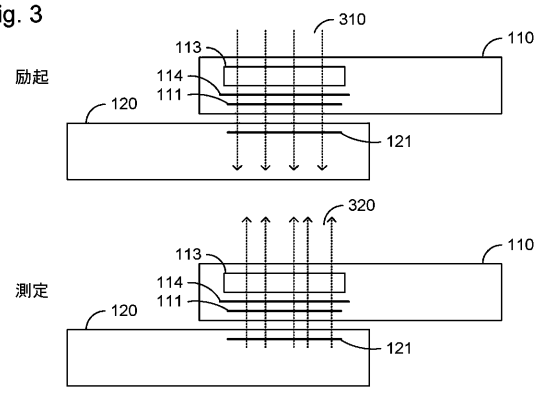
【図２】

Fig. 2



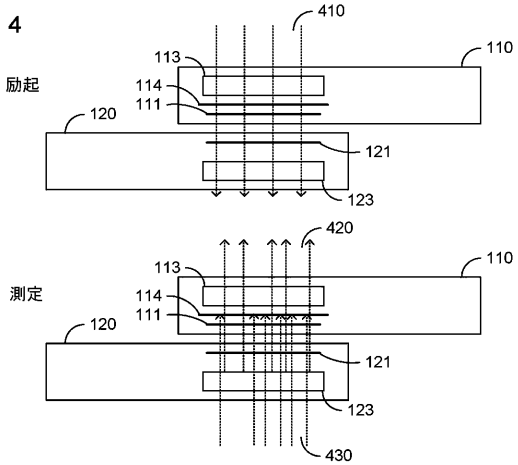
【図３】

Fig. 3

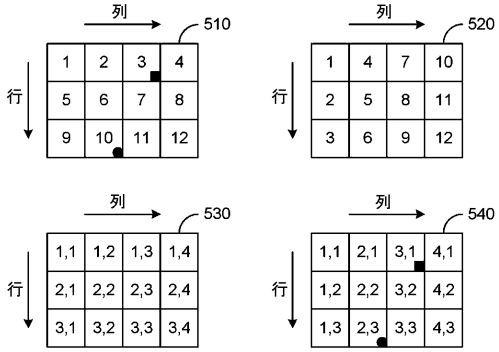


【図４】

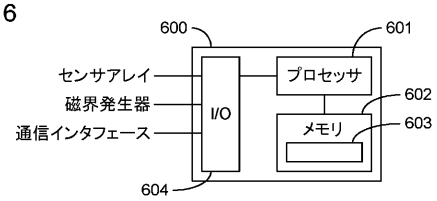
Fig. 4



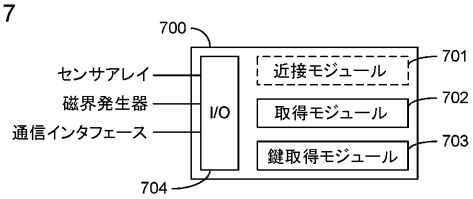
【図５】
Fig. 5



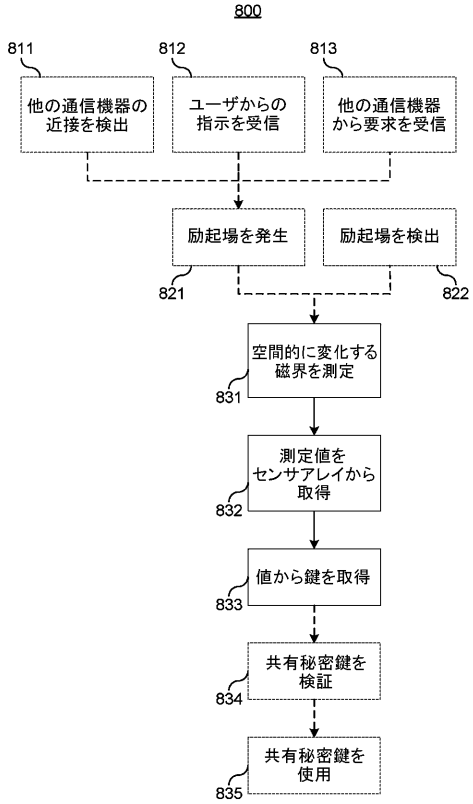
【図６】
Fig. 6



【図７】
Fig. 7



【図８】
Fig. 8



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/076820

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD. H04L9/32

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015/071431 A1 (ZHU XIAOCHUN [US] ET AL) 12 March 2015 (2015-03-12) abstract paragraphs [0011], [0012] -----	1-31
A	KATHERINE J. HARRY ET AL: "Detection of subsurface structures underneath dendrites formed on cycled lithium metal electrodes", NATURE MATERIALS, vol. 13, no. 1, 24 November 2013 (2013-11-24), pages 69-73, XP055286880, GB ISSN: 1476-1122, DOI: 10.1038/nmat3793 cited in the application the whole document -----	1-31

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 2016	18/07/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/076820

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015071431 A1	12-03-2015	CN 105493190 A	13-04-2016
		EP 3044792 A1	20-07-2016
		US 2015071431 A1	12-03-2015
		WO 2015035049 A1	12-03-2015

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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

（特許庁注：以下のものは登録商標）
１．ＦＩＲＥＷＩＲＥ
２．ブルートゥース
３．ＺＩＧＢＥＥ

(72)発明者 ローレンソン， マシュー ジョン
スイス国 ビュシニー １０３０， ル デ ローザンヌ ２０ エー
(72)発明者 アンダーソン， ラーシュ
スウェーデン国 ソルナ １６９４０， エドヴィンアドルフソンズ ヴィ．９
(72)発明者 ビュルケルト， ティル
スウェーデン国 フッディンゲ １４１３７， ヴィトヴィンゲヴェーゲン ５３
(72)発明者 クロニー， ハーム ステファン
スイス国 エシャラン １０４０， シェミン デ ラ ヴィレール ４９
(72)発明者 ノーラン， ジュリアン チャールズ
スイス国 ピュリー １００９， シェミン デ ダルゲロル ５
(72)発明者 ストレム， ジェイコブ
スウェーデン国 ストックホルム エスイー－１１７ ３２， ヘレネボルグスガタン ６シー，２ ティーアー－ル

Ｆターム(参考) 2G017 AA01 AB07 AC09 AD01 AD11 AD53 AD55 BA05 BA15 BA18
CB01 CB20 CC02
5J104 AA16 EA18 EA20 EA23 NA02 NA37 PA02