(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113841114 B
(45)授权公告日 2025.02.25

(21)申请号 202080034386.1
(22)申请日 2020.05.11
(65)同一申请的已公布的文献号
申请公布号 CN 113841114 A
(43)申请公布日 2021.12.24
(30)优先权数据
19382359.8 2019.05.09 EP
(85)PCT国际申请进入国家阶段日
2021.11.08
(86)PCT国际申请的申请数据
PCT/EP2020/063068 2020.05.11
(87)PCT国际申请的公布数据
WO2020/225452 EN 2020.11.12

(73)专利权人 魁赛德科技有限公司
地址 西班牙巴塞罗那
(72)发明人 卡洛斯·阿贝兰
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
专利代理师 达小丽 夏凯

(51)Int.Cl.
G06F 7/58(2006.01)
(56)对比文件
US 2007214293 A1,2007.09.13
审查员 林浩

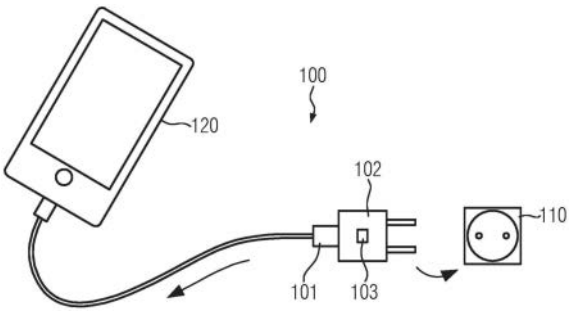
权利要求书2页 说明书12页 附图2页

(54)发明名称

传输功率和熵的设备

(57)摘要

一种用于从功率源向计算设备,优选移动计算设备传输功率的设备和一种用于向计算设备提供功率和/或熵的方法,其中该设备包括用于生成熵的熵生成器,并且其中当该设备被连接到计算设备时,该设备还适于将熵传输到计算设备,并且其中该设备适于利用从功率源接收的功率为所述熵生成器供应功率。



CN 113841114 B

1.一种用于从功率源向计算设备传输功率的设备,其中所述设备包括用于生成熵的熵生成器,以及其中当所述设备被连接到所述计算设备时,所述设备还适于将所述熵传输到所述计算设备,以及其中所述设备适于利用从所述功率源接收的功率为所述熵生成器供应功率,其中,所述设备适于将功率和熵相互独立地传输到所述计算设备。

2.根据权利要求1所述的设备,其中,所述熵生成器为随机数生成器或随机比特生成器。

3.根据权利要求1所述的设备,其中,所述设备包括存储设备,所述存储设备用于在随机数生成之后存储所述随机数,并且当所述设备被连接到所述计算设备时,将所述随机数提供给所述计算设备。

4.根据权利要求2所述的设备,其中,所述设备包括存储设备,所述存储设备用于在随机数生成之后存储所述随机数,并且当所述设备被连接到所述计算设备时,将所述随机数提供给所述计算设备。

5.根据权利要求1至4中的任一项所述的设备,其中,所述设备适于取决于条件向所述计算设备提供所述熵,所述条件包括已经在所述计算设备上的熵的量、在所述设备处接收到的来自所述计算设备的对熵的请求、所述计算设备的功率状态中的至少一个。

6.根据权利要求1至4中的任一项所述的设备,其中,所述设备包括用于将其与壁式插座直接连接的端口,或者其中所述设备包括用于将其与可直接与壁式插座连接的插头连接的端口,或其中所述设备是连接电缆,用于将所述设备与一侧上的功率连接器和另一侧上的所述计算设备连接。

7.根据权利要求1至4中的任一项所述的设备,其中,所述设备包括用于为所述计算设备供应功率的功率条,以及其中所述熵生成器能够利用来自所述功率条的功率被供应功率。

8.根据权利要求1至4中的任一项所述的设备,其中,所述熵生成器包括用于生成伪熵值的处理电路和用于使用物理随机过程生成真实熵值的熵芯片中的至少一个。

9.一种用于向计算设备提供功率和/或熵的方法,所述方法包括将所述计算设备与用于将功率从功率源传输到所述计算设备的设备连接,其中所述设备包括用于生成熵的熵生成器,以及其中所述方法包括利用从所述功率源接收的功率为所述熵生成器供应功率并且由所述熵生成器生成熵,并且在所述设备与所述计算设备连接时,将功率和熵中的至少一个传输到所述计算设备,其中,功率和熵彼此独立地从所述设备传输到所述计算设备。

10.根据权利要求9所述的方法,其中,所述熵生成器生成随机数或随机比特。

11.根据权利要求9所述的方法,其中,所述设备取决于条件向所述计算设备提供熵,所述条件包括已经在所述计算设备上的熵的量、在所述设备处接收到的来自所述计算设备的对熵的请求、所述计算设备的功率状态中的至少一个。

12.根据权利要求10所述的方法,其中,所述设备取决于条件向所述计算设备提供熵,所述条件包括已经在所述计算设备上的熵的量、在所述设备处接收到的来自所述计算设备的对熵的请求、所述计算设备的功率状态中的至少一个。

13.根据权利要求9至12中的任一项所述的方法,其中,所述熵生成器包括生成伪熵值的处理电路和使用物理随机过程生成真实熵值的熵芯片中的至少一个。

14.根据权利要求9至12中的任一项所述的方法,其中,当所述设备与功率源连接时,所

述熵生成器生成熵并且将所生成的熵存储在所述设备的存储设备中,以及其中当所述计算设备与所述设备连接时,所述熵从所述存储被传输到所述计算设备。

传输功率和熵的设备

技术领域

[0001] 本发明涉及一种用于从功率源向计算设备传输功率的设备。本发明还涉及一种用于向计算设备提供功率和/或熵的方法。

背景技术

[0002] 计算设备已成为日常生活中非常重要的一部分,具体地包括用户几乎整天随身携带的智能手机、平板电脑和膝上型计算机等移动设备,以及另一方面以更固定的方式通常在办公室或者在家里使用的个人计算机等计算设备。

[0003] 此外,由于这些设备在人与人之间的通信中发挥着重要作用,因此数据传输的安全性已成为越来越重要的主题。例如,可以通过使用随机数或任何其他形式的熵(比特的随机序列等)的加密消息来实现安全通信。然而,这种熵很难生成,并且高质量/高性能的熵生成器可能需要大量的功率和/或尺寸。

[0004] 对于计算设备,特别是对于移动计算设备,这种随机数生成将消耗大量的功率和/或空间,从而使制造商只能选择集成较低质量和/或较低性能的熵生成器。可替选地,用户可以携带的加密狗设备已被提议用于随机数生成。然而,提供用户必须亲自随身携带的附加设备以便向移动设备或其他计算设备提供熵是不舒服的并且因此会阻碍用户的采用,从而削弱他们的安全性。

发明内容

[0005] 技术问题

[0006] 从已知的现有技术出发,本发明要解决的问题是提供一种允许可靠地生成熵(如随机数)且不会过度消耗电池或其他功率源的潜在有限功率同时让用户感到舒适的设备和方法。

[0007] 技术方案

[0008] 该问题通过用于从功率源向计算设备传输功率的设备和用于向计算设备提供功率和/或熵的方法来解决。进一步的优选实施例由从属权利要求涵盖。

[0009] 根据该发明的用于从功率源向计算设备(优选地,移动计算设备)传输功率的设备包括用于生成熵的熵生成器,并且其中该设备进一步适用于在它连接到计算设备时将熵传输到计算设备,并且其中该设备适于利用从功率源接收的功率为熵生成器供应功率。

[0010] 功率源不需要在设备外部,而是也可以以例如以功率条(power bar)的形式集成到设备中。在任何情况下,该设备都具有传输功率和熵这二者的能力,因此能够类似地传输数据(熵)和功率。该发明并不限于同时传输功率和熵的情况,而是可以在不传输功率的情况下将熵传输到计算设备,或在某些情况下不向计算设备提供熵的同时传输功率。

[0011] 计算设备和设备之间的连接不需要是有线连接,而是也可以是无线连接,用于传输功率和/或传输熵。

[0012] 用户可以容易地使用根据该发明的设备来为计算设备(如智能电话)供应功率。同

时,几乎未被用户识别地,计算设备被提供有以例如随机数的形式的熵,以进一步用于例如加密通信或数据。因此,用户没有被提供他必须随身携带并且在他需要随机数的情况下使用的附加设备,而是以不需要用户的额外操作的方式来生成熵并将其提供给计算设备。

[0013] 熵生成器可以是随机数生成器或随机比特生成器。

[0014] 随机数在这里被认为是人类可读的随机数,例如1,234和1,000,067。与此相反,随机比特生成器可能会生成具有某种特定长度的0的序列和1的序列。例如,随机比特生成器可以生成20比特(或100比特或10000比特或10^7比特或任何其他比特数的序列),其中包含然后可由计算设备使用的0和1的随机序列。以同样的方式,由随机数生成器生成的随机数可以用于向计算设备提供随机数。提供随机数或随机比特序列可能更依赖于环境,但在使用随机数或随机比特的情况下可能具有优势,例如,在如加密通信或数据的进一步处理步骤中。

[0015] 术语"随机"包括伪随机值(数字或比特)和真实随机值(数字或比特)。伪随机值被认为是通过并非真正随机的方式获得的值,但是生成的伪随机值看起来是随机的。这适用于例如使用例如未预设的特定起始条件(如时间、日期等)的随机数生成算法。基于该起始条件,其他确定性算法计算一个值。该值是伪随机值,因为它取决于确定性算法和起始条件。如果两者都已知,则可以再现该值,因此该值不是真正随机的,而只是伪随机的。另一方面,真正的随机值被认为是真正随机的值,如例如从物理过程(如热过程或量子过程)获得的值。对于这样的过程,即使当准确地知道它们在某个时间点的状况,也不可能以确定性的方式确定系统的未来。例如,两束激光束的相位关系本质上是随机且无法预测,其中,一束源自始终在激光阈值上方驱动的激光器,另一束源自接近阈值驱动的激光器,因此它开始随机发射光子。同样,原子的衰变时刻或原子或分子的激发态与非激发态之间的跃迁无法预测,因此是真正随机的,并且将生成真正的随机值。

[0016] 在一个实施例中,该设备包括存储设备,该存储设备用于在随机数生成之后存储随机数,并且在将该存储设备连接到计算设备时,将随机数提供给该计算设备。

[0017] 可以以设备内部的闪速存储器或其他存储设备的形式提供存储设备。存储设备也可以是可与设备连接和断开连接的存储设备,但在任何情况下,存储设备都可以设置有由熵生成器生成的熵。因此,可以在允许在连接到计算设备后将熵快速传输到计算设备的情况下,将熵生成(这可能非常耗时)与和计算设备的连接分离,因为熵是"预先生成的"。

[0018] 此外,该设备可以适于取决于条件向计算设备提供熵,该条件包括计算设备上已有的熵量、在设备处接收到的来自计算设备的对熵的请求、计算设备的功率状态。

[0019] 由于计算设备并不总是需要随机数,因此一旦将计算设备连接到设备,根据特定条件向计算设备提供熵增加了对是否有以及有多少随机数被传输到计算设备的控制。

[0020] 此外,该设备可以适于将功率和熵相互独立地传输到计算设备。

[0021] 这意味着当该设备连接到计算设备时,该设备可以向计算设备传输功率或传输熵或传输功率和熵这两者。例如,这样允许仅在必要时传输功率。例如,如果智能手机的电池已经完全充满电,那么将大量功率传输到该计算设备就没有意义了。然而,可能仍然需要向计算设备提供以随机数等形式的熵,然后可以与此时未提供给计算设备的功率独立地促进该计算设备。另一方面,可能已经有足够的熵提供给计算设备,但是计算设备的电池还没有充满电。在这种情况下,一旦有足够的熵提供给计算设备,对随机数的提供可能根本不启动

或可能停止,但是提供功率以便为计算设备供应功率或用于加载计算设备的电池仍然可能一直持续直到充满电或不需要另外的功率为止。该实施例确保根据需要向相应的计算设备提供熵,从而避免不必要的数据传输和/或不必要的功率传输。

[0022] 根据一个实施例,该设备包括用于将其与壁式插座直接连接的端口,或者其中该设备包括用于将其与可直接与壁式插座连接的插头连接的端口,或者其中该设备是用于将其一侧与功率连接器连接而另一侧与计算设备连接的连接电缆。

[0023] 通过这样,可以提供设备的不同实现,这些实现取决于用户的环境和它们各自的使用是有利的。

[0024] 在可替选的实施例中,该设备包括用于为计算设备供应功率的功率条,并且其中熵生成器能够利用来自功率条的功率被供应功率。

[0025] 功率条被认为是包括其自身功率源的设备,例如以太阳能电池单体或电池的形式。该功率条不仅可以用于为计算设备供应功率,还可以用于将功率传输到熵生成器以使其生成熵。该设备通常由用户随身携带,例如当他想带着他的移动计算设备在户外度过更长的时间时。相应的熵生成器的集成不会对用户生成负面影响,因此允许以用户(几乎)不会注意到的方式向计算设备提供熵,从而不会提供任何不适。

[0026] 还可以规定,熵生成器包括用于生成伪熵值的处理电路和用于使用物理随机过程生成真实熵值的熵芯片中的至少一个。术语“芯片”可以指适用于生成真实熵值的(一个或多个)任何硬件部件(如电子的或光子的或它们的组合)。

[0027] 用于生成伪熵值的处理电路优选地是硬件和/或利用程序代码生成随机数的软件部件的组合,例如基于一天中的时间作为初始化值。这些数字尽管可能近似于随机数,但并不是真正的随机数,因此与完全随机的真实熵值相比,它们只是“伪熵值”。

[0028] 用于使用物理随机过程生成真实熵值的熵芯片因此被理解为芯片或软件和/或硬件的其他组合,其利用优选地在该熵芯片上发生的物理过程生成随机值或熵值并且真正产出随机值。例如,这可以包括激光源的任意干涉值,其中所述源或至少一个所述源被供应功率到几乎达到并且仅偶尔超过激光阈值的值。因此,生成两个信号之间的随机相位关系,从而允许生成真实的随机熵值。在申请人拥有的EP19382318.4中描述了以光学部件形式的相应系统,其内容通过引用结合在此。

[0029] 从WO2019/086730A1还获知熵源或熵生成器,其内容通过引用并入本文。

[0030] 在该文献中,具体描述了随机数的物理生成的程序,其中该程序包括以下步骤:将垂直腔面发射激光器的增益周期性地从下阈值调制到上阈值并返回;保持往返增益为正的时间比腔往返时间更长;保持每次往返的净增益为负比腔往返时间更长,以生成随机振幅脉冲;检测光脉冲;将光脉冲转换为电模拟脉冲;将电模拟脉冲数字化为随机数。用于实现该过程的物理部件可以在本发明的上下文中用作熵源或熵生成器。

[0031] 在US9,218,160B2中描述了另一种随机数生成器或熵生成器,其内容通过引用并入本文。

[0032] 描述了一种通过量子随机数生成器生成随机数的过程,该过程包括以下步骤:a)借助于电脉冲驱动器以单模和高调制带宽操作激光器以生成相位随机化的光脉冲,b)将a)中产生的相位随机化光脉冲转换为具有随机振幅的光脉冲,以及c)借助于快速光电二极管检测所生成的随机振幅信号,从而仅基于随机振幅信号生成随机数。如此生成的随机数可

以用于本发明的上下文中。

[0033] 虽然生成伪熵值的处理电路的第一种替代方案可能消耗更少的能量,但是使用熵芯片生成的熵的随机性更准确,从而降低了破译相应熵的风险(例如以随机数的形式)并且防止恶意攻击。

[0034] 根据本发明的用于向计算设备提供功率和/或熵的方法包括将计算设备与用于将功率从功率源传输到计算设备的设备连接,其中该设备包括用于生成熵的熵生成器,并且其中该方法包括利用从功率源接收的功率为熵生成器供应功率并且由熵生成器生成熵,并且在该设备与计算设备连接时将功率和熵中的至少一个传输到计算设备。

[0035] 该方法允许在需要时以用户(几乎完全)不会注意到的方式为计算设备提供熵,从而不会引起任何不适或需要用户的任何进一步动作来提供所需的熵,例如,用于对他的通信加密。

[0036] 在一个实施例中,功率和熵彼此独立地从设备传输到计算设备。

[0037] 因此,功率和熵仅根据需要提供给计算设备。例如,在计算设备被充分供应功率的情况下,不向计算设备提供功率,但是只要没有在计算设备上提供足够的熵,仍然可以向计算设备提供熵。

[0038] 此外,熵生成器可以生成随机数或随机比特。

[0039] 例如在加密通信或求解随机算法中,随机数或随机比特(特别是给定长度的随机比特序列)可以根据需要有利地被另外的应用使用。

[0040] 此外,设备可以根据条件向计算设备提供熵,该条件包括计算设备上已有的熵量、在设备处接收到的来自计算设备的对熵的请求、计算设备的功率状态中的至少一个。

[0041] 从而,可以避免熵的无意的或不需要的生成和向计算设备的提供,从而节省计算设备处的内存并且节省将用于生成无意的或不需要的熵的功率。

[0042] 更进一步地,熵生成器可以包括生成伪熵值的处理电路和使用物理随机过程生成真实熵值的熵芯片中的至少一个。

[0043] 用于生成伪熵值的处理电路通常需要较少的功率,而生成真实熵值的熵芯片会导致更可靠的熵值(如完全任意的随机数),从而提高了例如通信加密或数据加密的安全性。取决于预期的熵的应用,可以将上述处理电路和熵芯片同时或彼此独立地使用。

[0044] 在进一步的实施例中,熵生成器在所述设备与功率源连接时生成熵,并且将所生成的熵存储在所述设备的存储设备中,并且其中当计算设备与所述设备连接时,熵从存储被传输到计算设备。

[0045] 因此,可以以预防方式生成熵,一旦实际上建立了连接,就使得向计算设备更快地传输熵。

[0046] 优选的熵生成器可以包括一个或多个物理部件和/或一个或多个软件部件。例如,熵生成器可以被实现为处理电路和如存储器的相关联的硬件部件,以及用于使用程序代码生成(伪)随机数(或通常的熵)的相应的软件。用于生成随机数的程序代码原则上是技术人员已知的。该程序代码可以在熵生成器中以其普通方式使用。这可以包括使用特定初始化条件生成随机数,所述特定初始化条件如当前时间、日期或程序代码或软件将生成熵所基于的任何其他适当的初始化值。由于使用该熵生成器生成的熵(例如,以随机数的形式)基于初始化条件以及使用定义明确的编程代码对从该初始化条件获得的数据进行进一步处

理,因此所生成的随机数并不是真正的随机数,因此是伪随机数。

[0047] 在另一个优选实施例中,熵生成器可以包括用于生成(真实)熵值的熵芯片。在这方面,术语“芯片”可能不被认为是指以通常在计算设备中实现的方式的处理芯片。相反,这可以被认为是指具有用于生成(真实)熵值或随机值的装置的集成部件。这可以包括利用物理过程的熵芯片,该物理过程本质上是随机的,如量子过程或热过程。这还可以包括使用噪声信号来生成(真实)熵值。在这点上,利用量子过程的系统可能是优选的,如从参考激光源和在激光阈值或稍高于激光阈值处驱动的激光源之间的相位关系获得的随机干涉信号。参考信号与其他激光源生成的信号之间的相位关系是完全随机的,因为它受量子力学定律支配,因此无法预测,从而生成真随机数。特别优选的熵生成器(或熵芯片)是申请人拥有的在EP19382318.4中描述的以光学部件形式的熵源,其内容通过引用结合在此。

[0048] 在该文献中,描述了一种用于生成随机数的系统(即,随机数生成器),该系统包括适于生成两个光信号的光学部件和连接到该光学部件的两个光电探测器,其中第一光电探测器适于接收第一光信号并且基于第一光信号生成第一电信号,而第二光电探测器适于接收第二光信号并且基于第二光信号生成第二电信号,其中光学部件适于生成随机生成第一电信号和第二电信号的第一光信号和第二光信号,其中第一电信号和第二电信号等于或大于另一个,其中光电探测器适于传输第一电信号和第二电信号到比较器,其中比较器适于基于第一电信号和第二电信号的比较来提供输出,从而提供随机数。如此输出的随机数可以是随机的比特序列。

[0049] 在任何情况下,在用于以随机数的形式和/或以随机比特序列的形式生成熵的设备中提供熵生成器。后者指的是比特序列,即从熵生成器获得的0和1,而第一个,即随机数的生成,可以被认为是指人类可读的随机数。第一个或第二个的生成可以包括对原始信号的进一步处理,特别是在熵芯片用于生成真实随机值的情况下,因为这些值通常必须被数字化。因此,可以考虑熵生成器包括附加部件,如比较器和数字化器或允许将物理信号(例如,两个激光源的干涉信号)转换成数字值的任何其他装置。然后,这些数字值可以表示为实际上的随机数或任何包含0和1的比特序列。原始数字值的后处理也可能以随机性提取器的形式包括在内。这些随机性提取器的具体细节在此不提供,因为它们为本领域技术人员所熟知。

[0050] 可以“即时(on the fly)”生成熵,这意味着当包括熵生成器的设备被连接到功率源和计算设备时,只要建立了连接,熵生成器就生成熵并且将该熵提供给计算设备。

[0051] 可替选地,该设备可以包括存储设备,该存储设备可操作地连接到熵生成器,并且可以将所生成的熵(例如,以随机数或比特序列的形式)传输到该存储设备,并且可以将所述熵存储在该存储设备中。为此,存储设备可以被认为是非易失性存储设备,如USB存储设备。在这种情况下,可以在没有连接或独立于与计算设备的连接的情况下生成熵,并且可以将熵存储在存储设备中,例如用于稍后传输到计算设备。此外,可以提供附加部件,这些附加部件管理或监督或以任何其他方式控制将存储在存储设备中的熵提供给计算设备。该部件还可以连接到熵生成器,以便管理从熵生成器到存储设备或直接到计算设备的熵的提供。

[0052] 熵可以被提供给计算设备,例如提供给专门的专用存储或提供给在计算设备上运行的应用程序。如在金融预测中或在游戏中,在计算设备上,熵可以进一步用于例如加密数

据和/或通信的加密过程,或者用于解决随机化算法。

[0053] 就这点而言,应注意存在其中当设备被连接到功率源(例如,设备外部)时熵生成器生成熵的实施例。然后,可以将生成的熵提供给存储设备以供以后使用,特别是以后传输到计算设备。所生成的熵的量(例如,随机数的量)可以由部件控制以便适当地管理存储设备中的可用存储。例如,在达到存储设备的存储容量的情况下,可以不继续使用熵生成器的熵生成。部件可以将熵生成器生成熵的阈值设置为例如存储设备的存储容量的50%至90%或60%至85%,或者具体地80%。当达到该阈值时,熵生成可能会停止。

[0054] 此外,部件可以基于一个或多个条件来管理熵从熵生成器和/或存储设备到计算设备的传输。例如,熵是否从设备传输到计算设备可能取决于计算设备上已有的熵量。例如,在存在用于将熵传输到其的专用存储的情况下,一旦该专用存储已达到其存储容量,即使将计算设备连接到设备,熵也不能被传输到计算设备。

[0055] 可替选地或附加地,仅在设备处例如在部件处从计算设备接收到对熵的对应请求的情况下,才可以生成熵和/或将熵从设备传输到计算设备。响应于这样的请求,该部件可以使熵生成器和/或存储设备生成熵和/或将熵传输到计算设备。此外,可能存在向计算设备提供熵可以取决于的其他条件。例如,可以仅在超过计算设备处可用功率的特定阈值时才提供熵。例如,如果计算设备需要加载功率,则功率经由设备被传输到计算设备,但是熵的传输可以被暂停直到达到计算设备处可用功率的最小阈值为止。例如,如果连接到设备的计算设备的可用电池电量低于30%或低于20%或低于10%,则即使计算设备可能已请求熵,也不会向计算设备传输熵。如果超过该阈值,则可以将熵(例如,除了功率之外)传输到计算设备。

[0056] 该部件可以进一步控制熵在熵生成器处生成和/或(直接从熵生成器或从存储设备)传输到计算设备的速度。该控制还可以取决于上述条件并且可以导致每时间单位传输的熵量越大,计算设备上可用的功率实际上越高。

[0057] 该部件还可以包括允许监视熵生成器和/或存储设备的硬件部件和/或软件部件(以编程等的形式)。该监视可以包括检查由熵生成器生成的熵的结果的随机性。例如,如果该部件检测到由熵生成器生成的熵的概率分布的偏移,则可以执行健康诊断以便例如检测并且潜在地纠正缺陷。此外,可以提供该部件以便在生成熵或当已经将熵存储在存储设备中的同时或紧接着进一步处理由熵生成器生成的熵。这种后处理可以包括,例如,确定所生成的随机数的原始信号的概率分布,并且还可以包括对于每个所生成的随机值(例如,对于每个所生成的随机数)决定是否要将其传输到计算设备。例如,计算设备可能只使用超过特定阈值的随机数。例如,该阈值可以与随机数的对应最小值相关联,如例如大于10亿的随机数。对于熵生成器生成的任何随机数,该部件可以检查是否超过了该阈值,如果没有,则可以通过例如从存储设备中将相应的随机数删除来丢弃它。

[0058] 此外,该部件可以通过例如控制熵生成器是否被激活来控制熵生成器的工作。这可能取决于例如在设备内部的功率源处可用的功率量或者取决于从计算设备接收到的对熵的请求。如果在内部功率源处剩余的功率太少(例如,小于50%或小于30%或小于25%或小于20%或小于10%),则熵生成器可能不会被激活或可能被停用。此外,如果从连接的计算设备接收到相应的请求,则熵可以仅由熵生成器生成。

附图说明

[0059] 图1示出了根据一个实施例的用于从功率源向计算设备传输功率的设备；

[0060] 图2示出了根据第二实施例的用于向计算设备传输功率的设备；

[0061] 图3示出了根据第三实施例的用于从功率源向计算设备传输功率的设备，其中该设备包括功率条；

[0062] 图4示出了设备的部件的示意图。

具体实施方式

[0063] 图1示出了用于从功率源(在图1中示出为壁式插座110)向计算设备120传输功率的设备100。

[0064] 壁式插座110形式的功率源不应被理解为是限制性的。也可能有其他功率源(固定的和/或移动的/可移动的)能够用于提供功率，该功率然后经由设备100传输到计算设备120。这例如适用于电池或功率条或其他设备的形式，仅提供可以用于为计算设备提供功率的功率量。设备100因此被理解为包括功率源的设备或在功率源外部的设备，并且参与从功率源到计算设备120的功率传输。

[0065] 参与意味着功率可以经由该设备100传输到所连接的计算设备120，但不一定要求设备100提供功率。这意味着可以经由设备100提供功率，但在某些情况下，设备实际上不提供功率，而在其他情况下，设备向所连接的计算设备120提供功率。例如，如果计算设备已经充满电，则没有必要传输功率，并且在这种情况下，在一些实施例中，没有功率经由设备100传输到计算设备。也不一定要求在使用中，设备100永久地将功率从功率源传输到计算设备120，而是根据本发明的设备100仅旨在至少具有将功率从功率源110传输到计算设备120的能力。

[0066] 计算设备120在图中被示出为以智能电话形式的移动计算设备。然而，这并不旨在是限制性的。计算设备可以是用户通常与之交互的任何计算设备。这不仅适用于移动计算设备形式的计算设备，而且还可以被认为适用于如个人计算机这样的固定计算设备。如果计算设备是移动计算设备，则这可以指智能手机、膝上型电脑、平板计算机或用户可以随身携带的任何其他移动计算设备。此外，在本发明的意义上，如耳机和/或麦克风(特别是无线耳机和/或麦克风)的设备可以被视为“计算设备”，只要它们包括用于处理数据(如语音数据)的装置即可。因此，可以确保耳机和/或麦克风到其他设备(如膝上型电脑)之间的局部传输。

[0067] 可替选地，根据本发明的实施例，整辆车可被视为“计算设备”。具体而言，根据本发明，具有计算部件的电动汽车可以被视为“计算设备”。这些可以如下面描述的其他计算设备一样被加载有电功率，同时被加载有随机数。这样，可以提高电动汽车的安全性。例如，由此可以使用加载的随机数保护与外部计算设备的通信或自动驾驶仪的功能。

[0068] 同样，提供了实施例，根据这些实施例，汽车充当用于将功率和熵传输到另一计算设备的设备。在这种情况下，计算设备可以是使用例如汽车提供的USB连接器被供应功率的智能手机。同时，经由连接器，可以向计算设备提供熵，该熵可以用于确保计算设备与汽车(例如，经由蓝牙)的无线通信。

[0069] 与固定计算设备相比，移动计算设备可以被视为使得它们自己的功率源以例如适

于为计算设备充分供应功率的电池的形式集成的任何计算设备。

[0070] 根据本发明,设备100不仅包括用于将功率从功率源传输到计算设备120的装置,而且还包括能够生成熵的熵生成器103。在本发明的上下文中,熵被认为是指随机的任何事物,具体地是随机数或随机比特序列。随机数和随机比特序列可以具有任意长度并且可以由熵生成器以任何认为合适的方式生成,包括通过例如利用特定硬件部件和软件部件来生成伪随机数,所述特定硬件部件和软件部件使用程序代码例如基于初始值(如一天的日期或时间)生成随机数。熵生成器的其他实现可以利用实际上或至少几乎随机的物理过程,如干涉、晶体管中的亚稳定性(meta stability)、电子或热噪声或混沌耦合振荡器中的随机振荡。更一般地,可以使用随机量子物理过程或随机统计(宏观)物理过程,如热力学过程。

[0071] 在任何情况下,熵生成器不必限于一种特定的实现方式,而是可以想到熵生成器的多种实施方式。

[0072] 根据本发明,在任何情况下,熵生成器103由在设备100处从功率源110接收的功率和/或在设备100处可用的功率被供应功率。如果功率源被集成到设备中(以具有相应熵生成器的功率条形式实现设备,这将在后面解释),这意味着设备本身及其集成功率源为熵生成器供应功率以生成熵。在功率源在设备100外部的情况下,从该功率源接收的功率可以传输到计算设备120并且该功率中的一些可以用于为熵生成器供应功率。这可以包括没有计算设备与设备100连接但来自功率源的功率仍然用于为熵生成器供应功率并且生成熵的情况。

[0073] 在图1的描绘中,设备100被提供为包括两个部件的设备。第一部件是插头102,该插头102在此处被描绘为包括熵生成器103并且其被进一步描绘为可连接到壁式插座或更一般地,可连接到设备外部的功率源。在图1中,示出了实施例,其中熵生成器被提供作为耦合到外部功率源(此处为壁式插座的形式)110的设备的一部分。这可能是有利的,因为那些插头102通常具有显著的尺寸并且因此可以提供足够的空间用于包括熵生成器103和潜在地相关联的其他硬件和/或软件部件。与外部功率源的耦合可以被直接(即,没有其他中间设备)或间接提供,例如通过将包括熵生成器的设备与电缆耦合,电缆然后也与外部功率源耦合。

[0074] 旨在设备100不需要被实现为插头和电缆的组合。相反,设备100也可以仅通过具有熵生成器的插头或仅通过设置有熵生成器的电缆来实现。

[0075] 本发明的另一个实施例包括熵生成器103,并且所有相应部件没有集成在插头中,而是集成在将插头与计算设备120连接的电缆101中。电缆101可以包括可连接到插头(如插头102)或可以在一侧上提供或传输功率的任何其他设备的第一端口以及可以在另一侧上可连接到计算设备的端口。在该实施例的情况下,电缆101适于向计算设备传输功率。此外,它适于将以熵形式的数据传输到计算设备,其中熵由包括在电缆中的熵生成器生成。特别优选的熵生成器是申请人拥有的EP19382318.4中描述的以光学部件形式的熵源,该专利申请的内容通过引用结合在此。

[0076] 因此,为熵生成器供应功率所需的硬件部件的任何电路都可以设置在可直接连接到外部功率源(如壁式插座)的设备中,或者它可以包含在不直接连接到功率源的设备(以电缆101的形式)中。电缆101的端口可以是USB端口、迷你USB端口或任何其他被认为合适的实现。也可以使用闪电连接器。此外,在设备以电缆101的形式提供的实施例中,可以提供不

同于第二端口的第一端口。例如,电缆101的一个端口可以以USB连接器的形式实施,而另一个端口以迷你USB连接器的形式提供。

[0077] 熵生成器和任何相应的软件和/或硬件可以被包含在具有更大物理尺寸的端口中,并且还具有足够的可用空间来包括那些部件。然而,在其他实施例中,相应的熵生成器和相关联的部件可以被设置在具有较小物理尺寸的端口中和/或可以被设置为电缆101的柔性部分的一部分。这可以通过集成和/或印刷电路来实现。

[0078] 关于图1中给出的熵生成器的解释适用于进一步描述中描述的其他实现。

[0079] 图2示出了另一实施例,其中设备200是用于至少向计算设备120无线传输功率的设备。这可以使用公知的感应充电技术来提供,例如使用包括电感率的板201,当将计算设备靠近板201定位或定位在板201之上或在板201处时,经由该板201(即,使用电磁场),可以以无线方式将功率传输到计算设备。不言而喻,除了板201,也可以使用任何其他形状的设备。

[0080] 设备200还包括熵生成器204,例如集成到板中或附接到板或以任何其他方式提供给板。也可以通过提供相应的调制信号并且例如经由蓝牙连接传输所述信号,以无线方式将利用熵生成器生成的熵传输到计算设备。可替选地,可以使用有线连接将熵提供给计算设备120。在这种情况下,熵生成器实际上可以如相对于图1所解释的那样被集成到电缆中,或者它可以被集成在设备200中,并且该电缆可以仅用于传输数据。

[0081] 在根据图2的实施例中进一步示出了功率源202和将设备200与功率源连接的连接电缆203。这只是出于解释性原因提供的,因为图2的实施例中的设备200当然也需要与功率源(或内部功率源)的某种连接,通过该功率源可以为设备200供应功率并且可以将设备200的功率传输到计算设备。

[0082] 图3示出了设备300的第三实施例,其中设备300以包括功率条301和熵生成器303的设备的形式实施。功率条301可以被视为集成到设备300中的功率源,并且可以是原本众所周知的功率条或移动功率源。与该功率条相关联或附接到它或通过适当手段连接到它的是熵生成器303,该熵生成器303可以生成熵以便被传输(例如经由电缆302)到计算设备120。功率条301的功率可以以无线方式或经由电缆302以有线方式传输到计算设备。同样地,熵生成器303所生成的熵可以经由电缆302或者任何其他适当的连接传输到计算设备120,或者可以使用例如蓝牙连接以无线方式传输熵。在这点上,需要注意的是,与图2一样,用于将熵生成器生成的熵传输到计算设备的手段不需要与用于将功率传输到计算设备的手段相同。例如,虽然可以使用电缆连接来传输功率,但是可以使用如红外端口、蓝牙连接、WLAN连接或任何其他合适的无线连接之类的无线连接将熵从设备传输到计算设备。另一方面,可以以无线方式传输功率而使用例如设备和计算设备之间的连接电缆以有线方式传输熵。

[0083] 图3的实施例基本上包括设备,该设备具有自己的功率源,因此不永久地连接到外部功率源,或者原则上不需要连接到外部功率源以将功率传输到计算设备。在这点上,设备300可以被认为是独立的,因为它可以独立于外部功率源向计算设备120提供功率和熵。虽然在图3所示的实施例中,设备300包括功率条301,也可以有其他合理的实施例。例如,代替功率条,可以提供多个收集太阳能的太阳能电池单体来生成功率,然后可以将该功率传输到计算设备并且可以将该功率用于为熵生成器供应功率。同样的组合也可能是合理的,其

中提供多个太阳能电池单体,将收集到的功率馈送到功率条,功率条又将功率传输到计算设备和/或熵生成器和/或存储它以备稍后将其用于此类传输。

[0084] 图4描绘了示意性地示出根据本发明的一个实施例的设备的部件的实施例。图4的描述意在与已经提到的实施例相结合。具体地,如下文所见,涉及如何生成熵以及如何进一步使用熵的特征同样可以在上文已经提及的其他实施例中实施。

[0085] 图4的描绘大体描绘了设备400,其中在一侧提供了用于将设备400连接到功率源的连接装置405。在另一侧,提供了用于将设备400连接到计算设备120的连接装置404。

[0086] 用于将设备400连接到功率源110的连接装置405将仅被理解为示例性的。在功率源设置在设备400内部的实施例的情况下,该连接装置405可以被视为至少将熵生成器与相应功率源连接的内部连接装置。

[0087] 此外,连接装置404可以构成提供无线或有线连接以传输功率和/或熵的连接装置。如上所述,可能存在与用于传输熵的装置相比使用不同的用于传输功率的装置的实施例。因此,连接装置404可以被认为是用于以被认为合适的任何方式传输功率和/或熵的一般装置的更一般的描述。这还包括其中经由与如上所述用于传输熵的传输机制不同的传输机制来传输功率的实现。

[0088] 设备400可以进一步包括负责传输或管理功率传输的内部电路。然而,这里没有进一步详细描述这些部件,因为它们可以以本领域技术人员公知的方式实现。

[0089] 然而,设备400还包括熵生成器和用于促进熵向计算设备的传输的对应部件。

[0090] 熵生成器在此大体被描绘为元件401并且可以包括一个或多个物理部件和/或一个或多个软件部件。例如,熵生成器可以被实现为处理电路和如存储器的相关联的硬件部件以及用于使用程序代码生成(伪)随机数(或通常的熵)的相应的软件。用于生成随机数的程序代码原则上是技术人员已知的。该程序代码可以在设备400中提供的熵生成器401中以其通常的方式使用。这可以包括使用特定初始化条件生成随机数,所述特定初始化条件如当前时间、日期或程序代码或软件将生成熵所基于的任何其他适当的初始化值。由于使用该熵生成器生成的熵(例如,以随机数的形式)基于初始化条件,并且使用定义明确的编程代码对从该初始化条件获得的数据进行进一步处理,因此所生成的随机数并不是真正的随机数,因此是伪随机数。

[0091] 可替选地,元件401可以包括用于生成(真实)熵值的熵芯片。在这方面,术语“芯片”可能不被认为是指以通常在计算设备中实现的方式的处理芯片。相反,这可以被认为是指具有用于生成(真实)熵值或随机值的装置的集成部件。这可以包括利用物理过程的熵芯片,该物理过程本质上是随机的,如量子过程或热过程。这还可以包括使用噪声信号来生成(真实)熵值。在这点上,利用量子过程的系统可能是优选的,如从参考激光源和在激光阈值或稍高于激光阈值处驱动的激光源之间的相位关系获得的随机干涉信号。参考信号与其他激光源生成的信号之间的相位关系是完全随机的,因为它受量子力学定律支配,因此无法预测,从而生成真正的随机数。特别优选的熵发生器(或熵芯片)是申请人拥有的在EP19382318.4中描述的以光学部件形式的熵源,其内容通过引用结合在此。

[0092] 在任何情况下,在用于以随机数的形式和/或以随机比特序列的形式生成熵的设备中提供熵生成器。后者指的是比特序列,即从熵生成器获得的0和1,而第一个,即随机数的生成,可以被认为是指人类可读的随机数。第一个或第二个的生成可以包括对原始信号

的进一步处理,特别是在熵芯片用于生成真实随机值的情况下,因为这些值通常必须被数字化。因此,可以考虑元件401包括附加部件,如比较器和数字化器或允许将物理信号(例如,两个激光源的干涉信号)转换成数字值的任何其他装置。然后,这些数字值可以表示为实际上的随机数或任何包含0和1的比特序列。原始数字值的后处理也可能以随机性提取器的形式包括在内。因为这些随机性提取器的具体细节为本领域技术人员所熟知,所以在此不提供。

[0093] 可以“即时(on the fly)”生成熵,这意味着当设备400被连接到功率源和计算设备时,只要建立了连接,熵生成器就生成熵并且将该熵提供给计算设备。

[0094] 可替选地,该设备400可以包括存储设备402,该存储设备可操作地连接到熵生成器401,并且可以将所生成的熵(例如,以随机数或比特序列的形式)传输到该存储设备,并且可以将所述熵存储在该存储设备中。为此,存储设备402可以被认为是如USB存储设备那样的非易失性存储器。在这种情况下,可以在没有连接或独立于与计算设备的连接的情况下生成熵,并且可以将熵存储在存储设备中,例如用于稍后传输到计算设备。此外,可以提供附加部件403,这些附加部件管理或监督或以任何其他方式控制将存储在存储设备402中的熵提供给计算设备。部件403还可以连接到熵生成器以管理从熵生成器到存储设备402或直接到计算设备120的熵的提供。

[0095] 熵可以被提供给计算设备,例如提供给专门的专用存储或提供给在计算设备上运行的应用程序。如在金融预测中或在游戏中,在计算设备上,熵可以进一步用于例如加密数据和/或通信的加密过程,或者用于解决随机化算法。

[0096] 就这点而言,应注意存在其中当设备400被连接到功率源110(例如,在设备400外部)时熵生成器401生成由部件403控制的熵的实施例。然后,可以将生成的熵提供给存储设备402以供稍后使用,特别是稍后传输到计算设备。所生成的熵的量(例如,随机数的量)可以由部件403控制以便适当地管理存储设备中的可用存储。例如,在达到存储设备的存储容量的情况下,可以不继续使用熵生成器的熵生成。部件403可以将熵生成器生成熵的阈值设置为例如存储设备402的存储容量的50%至90%或60%至85%,或者具体地80%。当达到该阈值时,熵生成可能会停止。

[0097] 此外,部件403可以基于一个或多个条件来管理熵从熵生成器401和/或存储设备402到计算设备120的传输。例如,熵是否从设备400传输到计算设备120可能取决于计算设备上已有的熵量。例如,存在用于将熵传输到的专用存储,在该专用存储已达到其存储容量的情况下,即使将计算设备连接到设备400,熵也不能被传输到计算设备。

[0098] 可替选地或附加地,仅在设备400处例如在部件403处从计算设备420接收到对熵的对应请求的情况下,才可以生成熵和/或将熵从设备传输到计算设备120。响应于这样的请求,部件403可以使熵生成器401和/或存储设备402生成熵和/或将熵传输到计算设备。此外,可能存在向计算设备提供熵可以取决于的其他条件。例如,可以仅在超过计算设备处可用功率的特定阈值时才提供熵。例如,如果计算设备需要加载功率,则功率经由设备400被传输到计算设备120,但是熵的传输可以被暂停,直至达到计算设备120处可用的功率的最小阈值。例如,如果连接到设备400的计算设备的可用电池电量低于30%或低于20%或低于10%,则即使计算设备可能已经请求熵,也不会向计算设备传输熵。如果超过该阈值,则可以将熵(例如,除了功率之外)传输到计算设备。

[0099] 部件403可以进一步控制熵在熵生成器401处生成和/或(直接从熵生成器或从存储设备402)传输到计算设备120的速度。该控制还可以取决于上述条件并且可以导致每时间单位传输的熵量越大,计算设备上可用的功率实际上越高。

[0100] 部件403还可以包括允许监视熵生成器401和/或存储设备402的硬件部件和/或软件部件(以编程等的形式)。该监视可以包括检查由熵生成器生成的熵的结果的随机性。例如,如果部件403检测到由熵生成器生成的熵的概率分布的偏移,则可以执行健康诊断以便例如检测和潜在地纠正缺陷。此外,可以提供部件403,以便在生成熵或当已经将熵存储在存储设备402中的同时或紧接着进一步处理由熵生成器生成的熵。这种后处理可以包括,例如,确定所生成的随机数的原始信号的概率分布,并且还可以包括对于每个所生成的随机值(例如,对于每个所生成的随机数)决定是否要将其传输到计算设备。例如,计算设备可能只使用超过特定阈值的随机数。例如,该阈值可以与随机数的对应最小值相关联,如例如大于10亿的随机数。对于熵生成器生成的任何随机数,该部件403可以检查是否超过了该阈值,如果没有,则可以通过例如从存储设备402中将相应的随机数删除来丢弃它。

[0101] 此外,该部件可以通过例如控制熵生成器是否完全被激活来控制熵生成器401的工作。这可以例如取决于设备内部功率源处可用的电量(如图3中所解释的)或取决于从计算设备接收到的对熵请求。如果在内部功率源处剩余的功率太少(例如,小于50%或小于30%或小于25%或小于20%或小于10%),则熵生成器可能不会被激活或可能被停用。此外,如果从连接的计算设备接收到相应的请求,则熵可以仅由熵生成器生成。

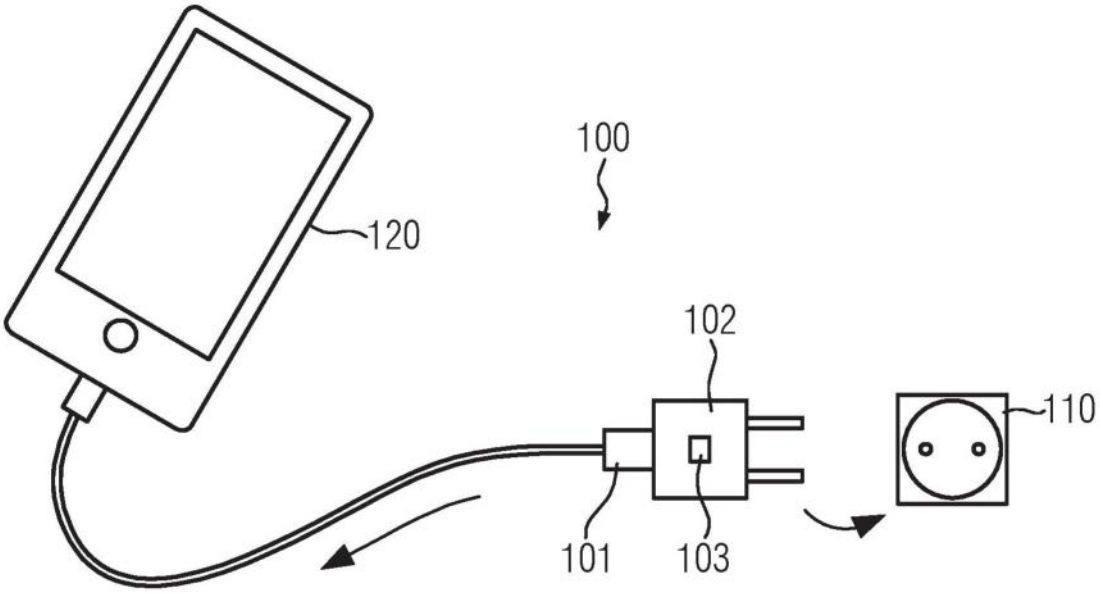


图1

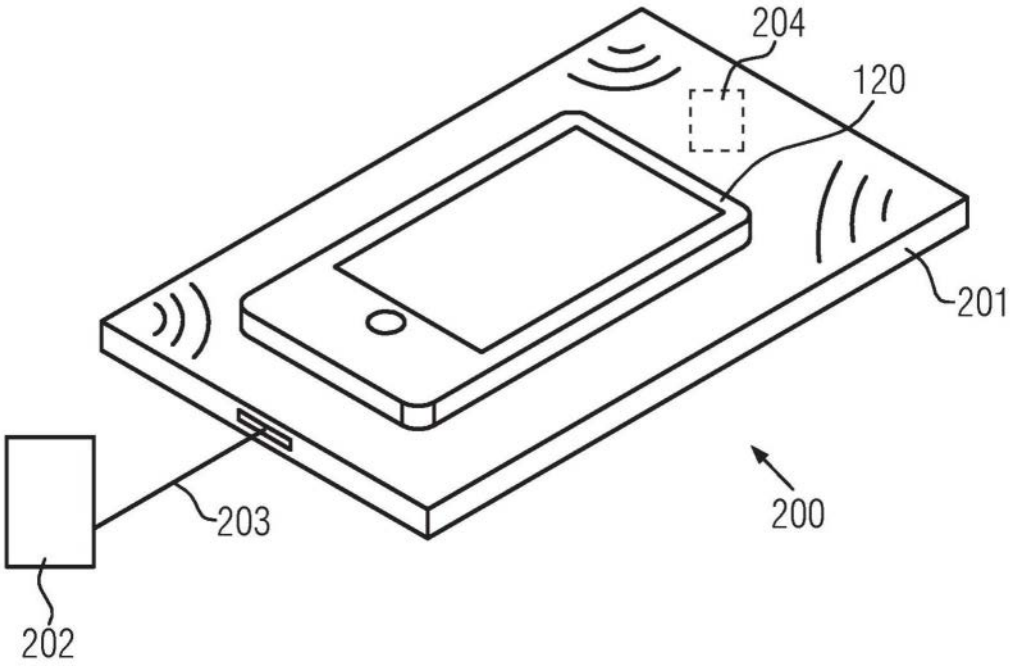


图2

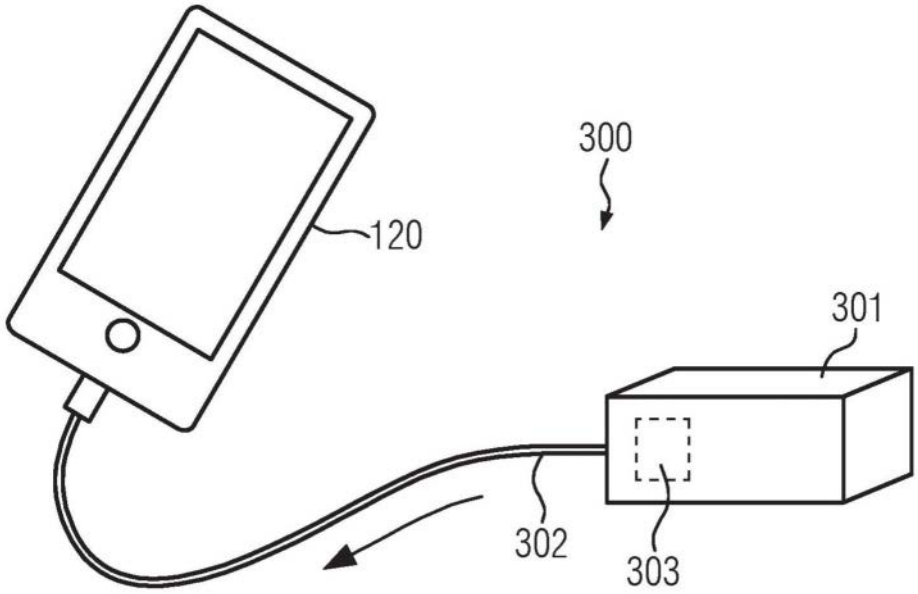


图3

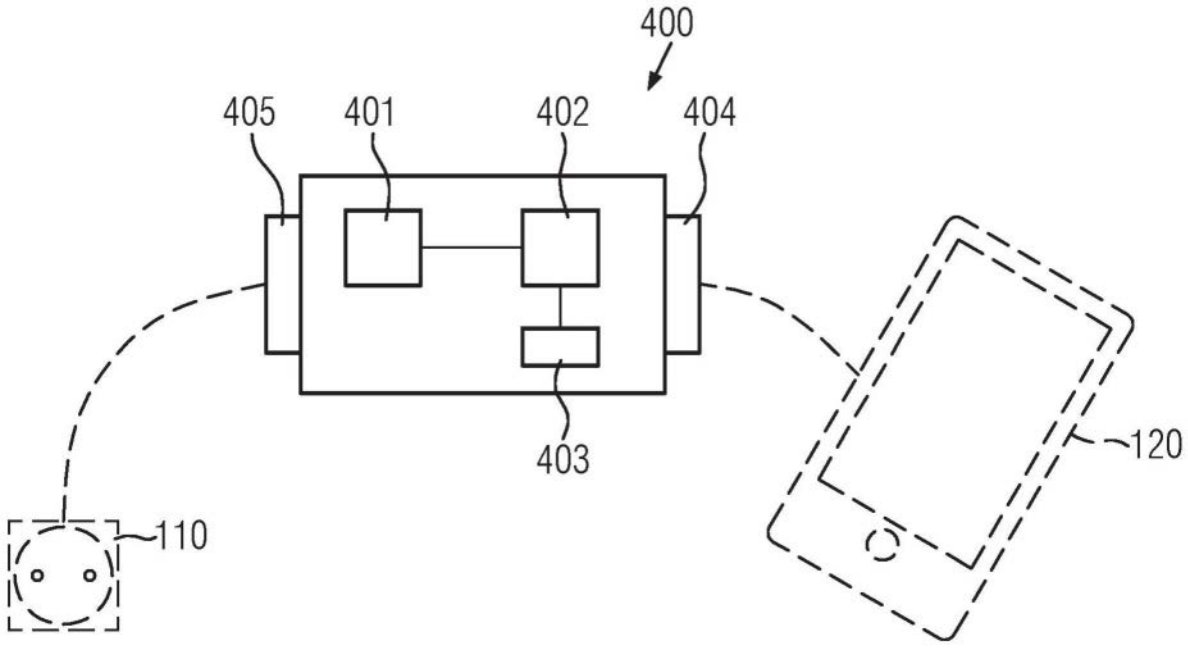


图4