



US 20180338726A1

(19) **United States**

(12) **Patent Application Publication**  
**Yarger et al.**

(10) **Pub. No.: US 2018/0338726 A1**

(43) **Pub. Date: Nov. 29, 2018**

(54) **NEAR FIELD TELEMETRY LINK FOR  
PASSING A SHARED SECRET TO  
ESTABLISH A SECURE RADIO FREQUENCY  
COMMUNICATION LINK IN A  
PHYSIOLOGICAL CONDITION  
MANAGEMENT SYSTEM**

**Publication Classification**

(51) **Int. Cl.**  
*A61B 5/00* (2006.01)  
*G16H 50/20* (2018.01)  
*G06F 19/00* (2018.01)  
*A61B 5/145* (2006.01)  
*G08C 17/02* (2006.01)  
*G16H 15/00* (2018.01)  
*H04W 4/80* (2018.01)  
*G16H 20/10* (2018.01)  
*G16H 20/60* (2018.01)  
*A61B 5/024* (2006.01)

(52) **U.S. Cl.**  
 CPC ..... *A61B 5/72* (2013.01); *A61B 5/7275*  
 (2013.01); *G16H 50/20* (2018.01); *A61B*  
*5/742* (2013.01); *G06F 19/00* (2013.01); *A61B*  
*5/14532* (2013.01); *A61B 5/002* (2013.01);  
*G16H 15/00* (2018.01); *H04W 4/80* (2018.02);  
*Y02A 90/26* (2018.01); *G16H 20/10* (2018.01);  
*G16H 20/60* (2018.01); *A61B 5/02438*  
 (2013.01); *G08C 17/02* (2013.01)

(71) Applicant: **Becton, Dickinson and Company,**  
Franklin Lakes, NJ (US)

(72) Inventors: **Michael Yarger,** Chapel Hill, NC (US);  
**James Petisce,** Westford, MA (US);  
**Ellen DiResta,** Arlington, MA (US);  
**Deborah Burns,** Westford, MA (US);  
**David Mason,** Newburyport, MA (US)

(73) Assignee: **Becton, Dickinson and Company,**  
Franklin Lakes, NJ (US)

(21) Appl. No.: **16/036,184**

(22) Filed: **Jul. 16, 2018**

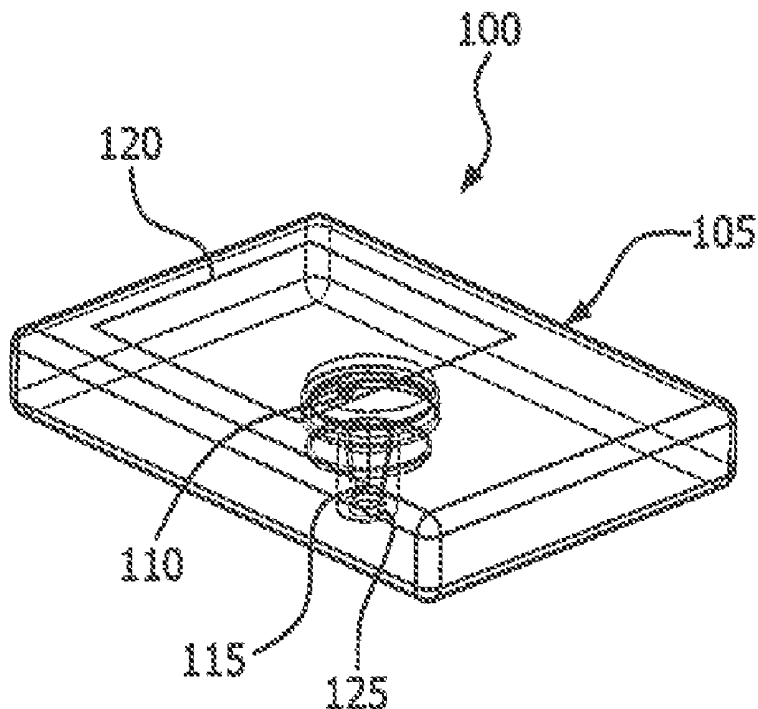
**Related U.S. Application Data**

(63) Continuation of application No. 14/364,597, filed on Jun. 11, 2014, now Pat. No. 10,039,496, filed as application No. PCT/US2012/069860 on Dec. 14, 2012.

(60) Provisional application No. 61/576,309, filed on Dec. 15, 2011.

(57) **ABSTRACT**

Pairing is provided between first and second wireless devices in a physiological condition management system. The first and second wireless devices are placed in proximity to initiate generation of a secret key via a random process at one of the devices and to exchange the secret key with the other device using a wireless near field communication (NFC) link. The shared secret key is then used to encrypt data for communication between the first and second wireless devices via a different secure radio frequency (RF) wireless channel.



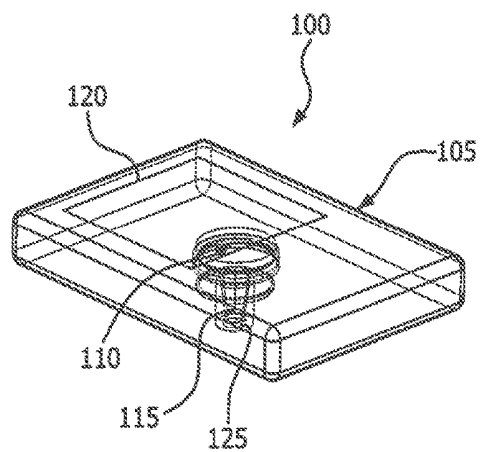


FIG. 1

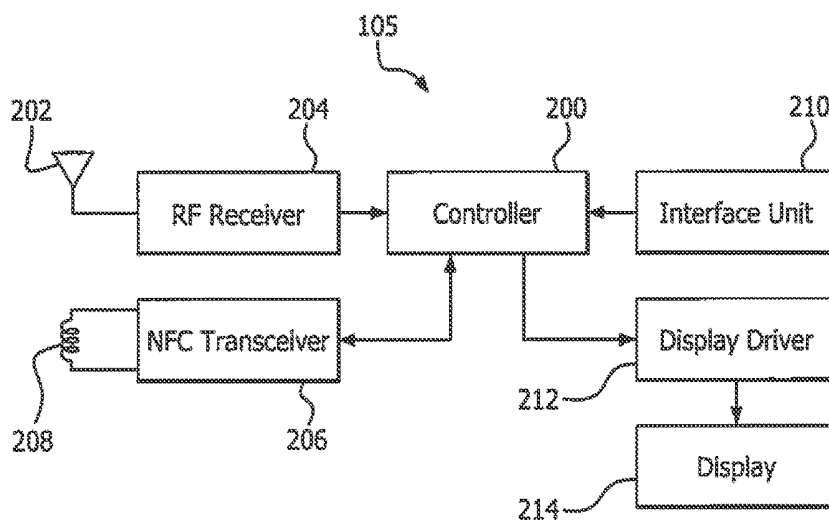


FIG. 2

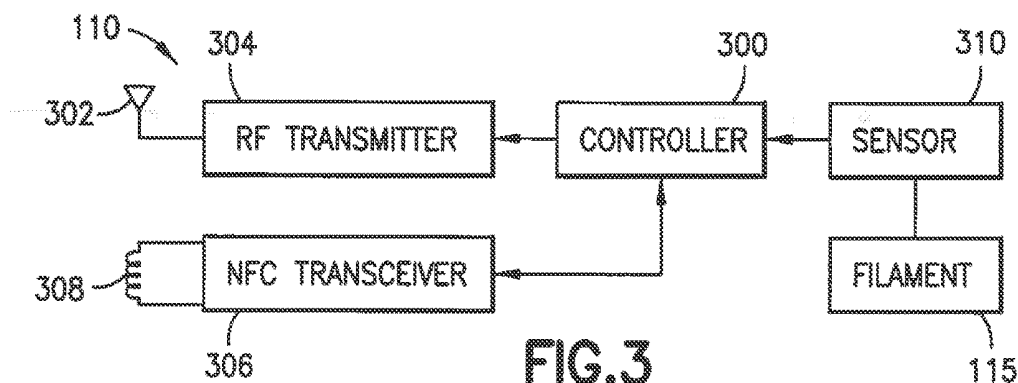


FIG.3

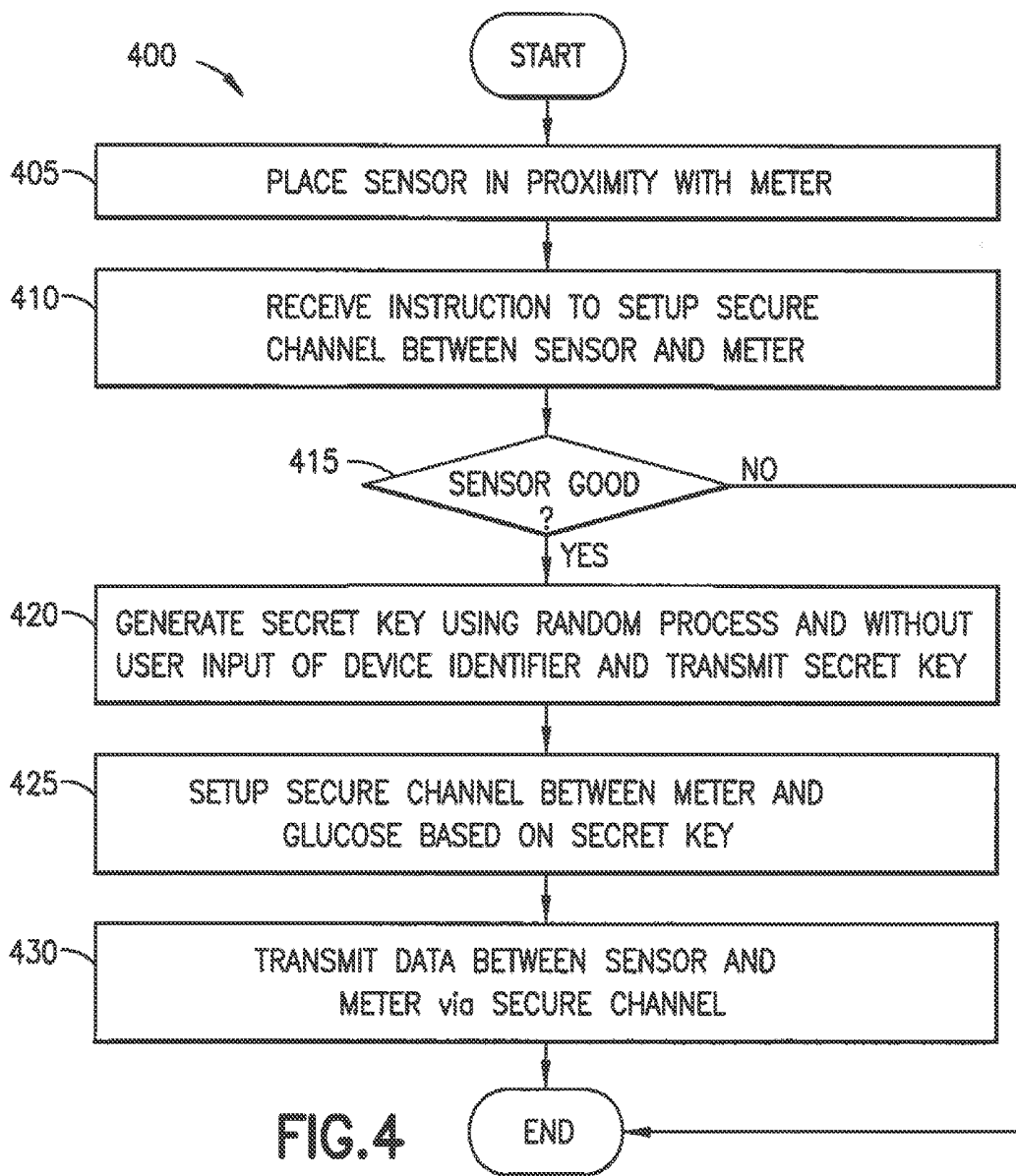


FIG.4

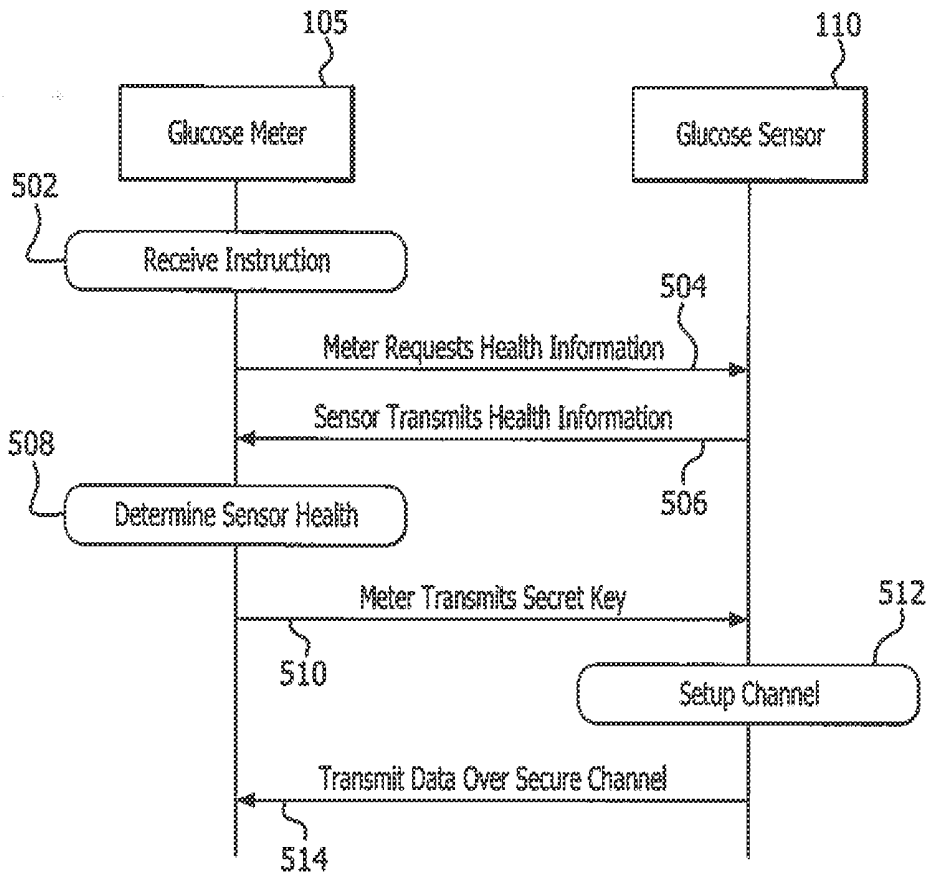


FIG. 5

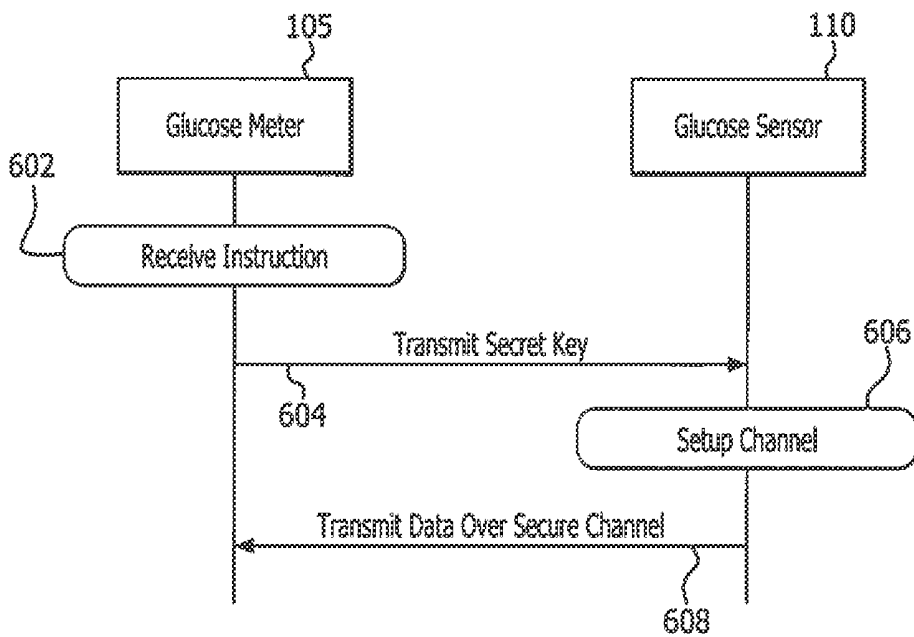


FIG. 6

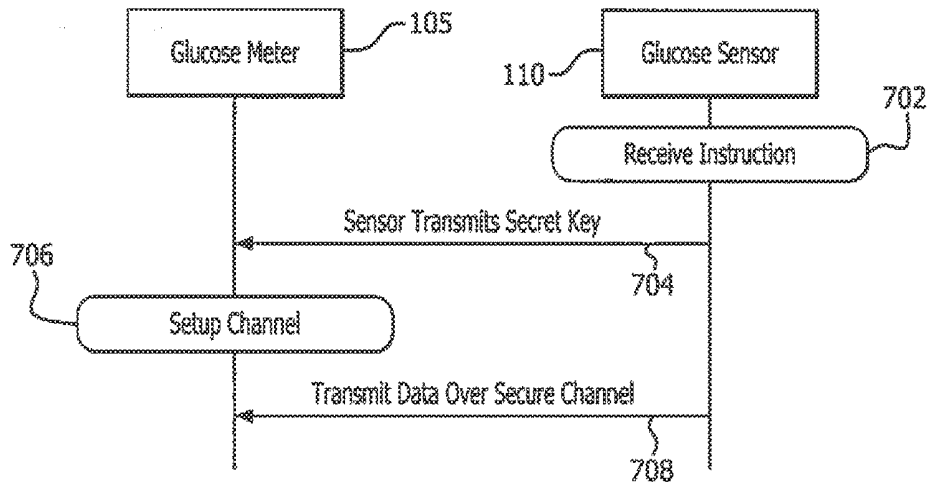


FIG. 7

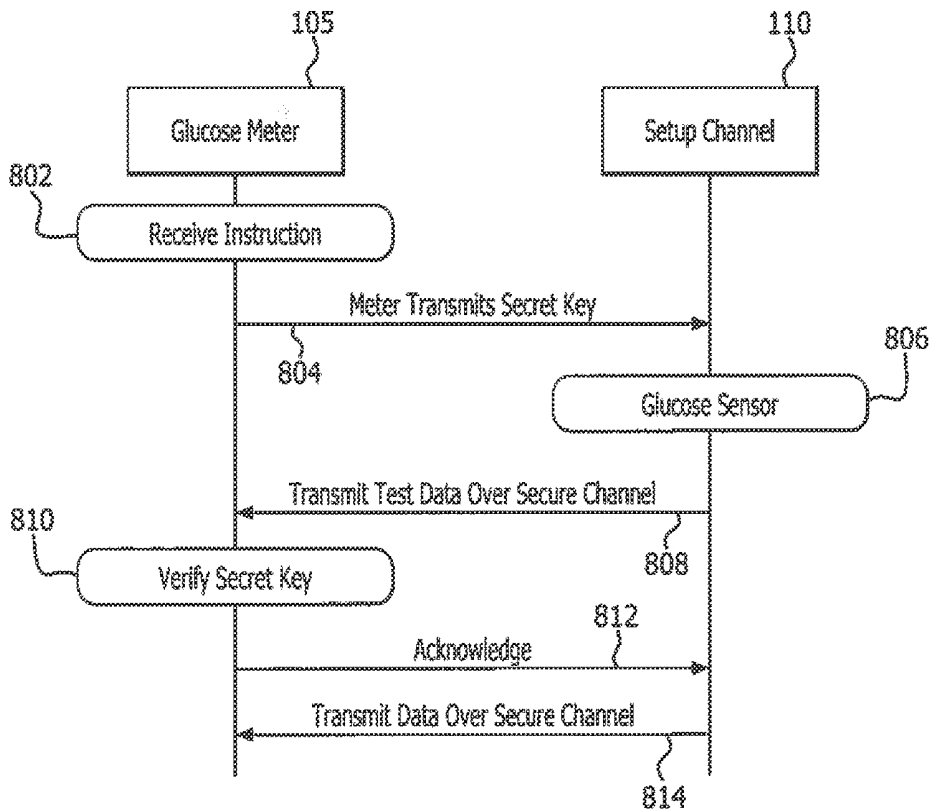


FIG. 8

**NEAR FIELD TELEMETRY LINK FOR  
PASSING A SHARED SECRET TO  
ESTABLISH A SECURE RADIO FREQUENCY  
COMMUNICATION LINK IN A  
PHYSIOLOGICAL CONDITION  
MANAGEMENT SYSTEM**

[0001] This application is a continuation of U.S. patent application Ser. No. 14/364,597, filed Jun. 11, 2014, which is a 35 U.S.C. § 371 national stage application of PCT/US12/69860, filed Dec. 14, 2012, which claims priority from U.S. provisional patent application Ser. No. 61/576,309, filed Dec. 15, 2011, the entirety of each application being incorporated by reference herein.

**FIELD OF THE INVENTION**

[0002] The present invention disclosed and claimed herein generally relates to a physiological condition monitor (e.g., a continuous glucose monitor) and, more particularly, to methods and apparatuses to establish a near field telemetry link for passing a shared secret to establish a secure radio frequency communication link in a physiological condition monitoring system.

**BACKGROUND OF THE INVENTION**

[0003] Diabetes is a disease in which a person has high blood sugar either because the body does not produce enough insulin or because the person's cells are insensitive to the produced insulin. Accordingly, it is beneficial to monitor the person's glucose levels to identify trends in glucose levels, identify factors that affect glucose levels, evaluate foods and medications on glucose levels, and identify changes in a treatment plan.

[0004] A continuous glucose monitor (CGM) is an electronic system that measures and displays glucose level in a user's body. A CGM includes a sensor that is attached to a user's skin and held securely in place by a fastener. To measure glucose levels of the user, the sensor generally includes a metal filament that penetrates and rests in the fatty layer of the user's skin. The sensor communicates with a handheld meter that displays the glucose measurements from the sensor. A CGM is helpful to avoid potentially dangerous hyperglycemia or hypoglycemia and to help the user lower their average blood sugar levels over time.

[0005] Because the sensor is attached to the user's skin and the meter is a handheld device, wires would make the CGM difficult to use. Accordingly, CGM systems are preferably implemented with a wireless communication link between the sensor and the monitor. Accordingly, a separate transmitter may be incorporated into the sensor to transmit data to the handheld meter. Unique information must be exchanged between the transmitter and meter to create a secure communication link. Generally, for the user's convenience, the transmitter is implemented in a small form factor and includes a fixed battery that cannot be easily replaced. As such, the transmitter must be replaced when the battery is exhausted. Current CGM systems require the user to input information into the meter that identifies the transmitter, thereby allowing the meter to receive information from the sensor. This information is typically printed on the transmitter and, therefore, available for any person to read the information.

[0006] As such, the unique information can be easily obtained by observing unique information disposed on the

transmitter or intercepting the communications with the unique information. Due to the importance of wireless medical devices, regulators have become interested in the security of such wireless medical devices. Further, because the user has to manually enter the unique information, replacing the transmitter is inconvenient. Moreover, battery life is an important factor in CGM sensors, and similar devices, where the battery is not designed to be replaced. Accordingly, there is a need for a method to exchange information for encrypting data in wireless medical devices that is convenient for users, and minimize battery usage.

**SUMMARY OF THE INVENTION**

[0007] A system and method for pairing first and second wireless devices in a physiological condition management system by exchanging a secret key is provided.

[0008] In accordance with an illustrative embodiment, a method for pairing first and second wireless devices in a physiological condition management system comprises: placing a first wireless device in proximity with a second wireless device; generating an indication that the first and second wireless devices are in proximity with each other to establish communication via a near field communication (NFC) link; generating a secret key at the first wireless device using a random process and sharing the secret key with the second wireless device in response to the indication that the first and second wireless devices are in proximity with each other to establish communication via the NFC link; and transmitting signals between the first and second wireless devices via a secure radio frequency (RF) link that is different from the NFC link and on which the signals are encrypted using the secret key. The secret key is not generated until after the first and second wireless devices are placed proximally to each other to establish the NFC link. Generating the secret key does not employ user input of an identifier of the second wireless device.

[0009] An illustrative wireless physiological condition monitoring system is disclosed that comprises first and second wireless devices configured to perform physiological condition management operations. At least one of the first and second wireless devices is configured to generate an indication when the first and second wireless devices are in proximity with each other and have established communication via a near field communication (NFC) link. The first wireless device is configured to generate a secret key using a random process and share the secret key with the second wireless device in response to the indication that the first and second wireless devices are in proximity with each other to establish communication via the NFC link. The first and second wireless devices are configured to transfer data via a secure radio frequency (RF) link that is different from the NFC link and on which the data is encrypted using the secret key by at least one of the first and second wireless devices, and at least the other one of the first and second wireless devices is configured to decrypt the data using the secret key. The secret key is not generated until after the first and second wireless devices are placed proximally to each other to establish the NFC link.

[0010] In accordance with an illustrative embodiment, a first wireless device is securely paired with a second wireless device in a physiological condition management system. The first wireless device comprises: a controller configured to perform a physiological condition management operation; and at least one wireless communication interface

for transmitting physiological condition management signals to and from the second wireless device. The controller is configured to generate a secret key using a random process and share the secret key with the second wireless device via the at least one wireless communication interface in response to an indication that the first and second wireless devices are in proximity with each other to establish communication via the near field communication (NFC) link and to transmit physiological condition management signals to the second wireless device using a secure radio frequency (RF) link that is different from the NFC link based on the secret key, the first wireless device encrypting the physiological condition management signals using the secret key. The secret key is not generated until after the physiological condition meter and the physiological condition sensor are placed proximally to each other.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 depicts a CGM system in accordance with an illustrative embodiment of the present invention;

[0012] FIG. 2 depicts a block diagram of an example glucose meter for use in the CGM system of FIG. 1;

[0013] FIG. 3 depicts a block diagram of an example glucose sensor for use in the CGM system of FIG. 1;

[0014] FIG. 4 is a flow chart of an illustrative process that the CGM system of FIG. 1 may implement to pair the glucose meter and the glucose sensor; and

[0015] FIGS. 5-8 illustrate examples of communication sequences between the glucose meter and the glucose sensor according to the example process of FIG. 4.

#### DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0016] A near field telemetry link for passing a shared secret to establish a secure radio frequency communication link in a physiological condition monitoring system (e.g., continuous glucose monitoring system) is generally described herein. As will be described in detail below, an example glucose meter and an example glucose sensor of the CGM system are placed in proximity to exchange a secret key using a near field wireless link, which is used to pair the devices and encrypt data to secure a radio frequency (RF) wireless channel between the sensor and the monitor. As will be appreciated by one skilled in the art, there are numerous ways of carrying out the examples, improvements and arrangements of the methods disclosed herein. Although reference is made to the illustrative embodiments depicted in the drawings and the following descriptions, the embodiments disclosed herein are not meant to be exhaustive of the various alternative designs and embodiments that are encompassed by the disclosed invention.

[0017] Reference is now made in detail to the illustrative embodiments of the invention, which, together with the drawings and the following examples serve to explain the principles of the invention. These embodiments are described to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized without departing from the spirit and scope of the present invention. Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. Although any methods and materials similar or equivalent to those described herein can

be used in the practice or testing of the present invention, the example methods, devices and materials are now described.

[0018] FIG. 1 depicts an illustrative embodiment of a CGM system 100. Generally, the CGM system 100 comprises a glucose meter 105 and a glucose sensor 110. In operation, the glucose meter 105 and the glucose sensor 110 communicate by a radio frequency (RF) wireless link. To establish the RF wireless link, the glucose meter 105 and the glucose sensor 110 must be linked together (paired) so that the glucose meter 105 only receives information from the paired glucose sensor 110 and not another nearby sensor or other unauthorized device. In the example of FIG. 1, the glucose sensor 110 and the glucose meter 105 securely exchange a secret key that is used to encrypt information transmitted on a different wireless link. That is, for example, the glucose sensor 110 uses the secret key to encrypt data that is transmitted to the glucose meter 105, which uses an identical secret key to decrypt the encrypted data. The glucose meter 105 may also preferably include an error check field in the decrypted data to verify successful reception and decryption of the received data.

[0019] The glucose sensor 110 typically includes a filament 115 that is inserted into the user's skin and rests in the fatty layer beneath the user's skin. Other methods of sensor deployment (e.g., subcutaneous, intravenous, and so on) can be used as described below. In other examples, the glucose sensor 110 may be implemented by an optical sensor, a chemical sensor, or any device suitable for detecting a body characteristic or analyte such as glucose. As such, the user generally does not feel the filament 115 piercing the user's skin. To secure the position of the sensor, a suitable fastener such as an adhesive patch fixes the sensor in place. In the CGM system 100, the glucose meter 105 includes any suitable display 120 to provide graphical and/or textual information to the user, such as the user's current glucose level. However, the display 120 may provide the information in any suitable form, such as a line graph illustrating the glucose level over time. In such an example, the user is able to monitor their glucose level based on food and beverage consumption or other relevant events occurring throughout the day.

[0020] In the example of FIG. 1, the glucose meter 105 and the glucose sensor 110 preferably include a low power radio link by using inductive coupling of inductors in each device, which is also known as near field communication (NFC). When such inductors are placed in close proximity (e.g., 10 cm), the magnetic field generated by a current in a transmitting inductor will induce a voltage in a receiving inductor, thereby enabling a very short range wireless communication link. In the example of FIG. 1, after an instruction from a user or another indication that the glucose meter 105 and the glucose sensor 110 are close in proximity, the glucose meter 105 and/or glucose sensor 110 exchange a shared key using the NFC wireless link. As will be described below, the shared key is randomly generated data for encrypting communications between the glucose meter 105 and the glucose 110 using a different low power wireless link.

[0021] Because the glucose meter 105 and the glucose sensor 110 must be close in proximity due to the NFC wireless channel, security of the shared key is transmitted in confidence that another sensor is not nearby and can intercept the shared key. Further, the user is not required to enter information to manually pair the glucose meter 105 and the

glucose sensor 110, thereby facilitating the operation of the CGM system 100 due to replacing a glucose sensor 110, for example. In another example, the glucose sensor must be placed in electrical and/or optical contact with the glucose meter and a secret key may be transmitted via the electrical and/or optical contact.

[0022] In the CGM system 100, the example glucose sensor 110 is a low power device that is typically replaced every 5-7 days. As such, the glucose sensor 110 is initially in a low power state or a powerless state to preserve its power source before being actuated to communicate with the glucose meter 105. Accordingly, to activate the CGM system 100, the glucose sensor 110 must be actuated (i.e., turned on) and the glucose meter 105 and the glucose sensor 110 must exchange information to enable wireless communication to enable the CGM system 100.

[0023] To preserve power, the power source of the glucose sensor 110 may not be electrically coupled to the other electric devices in the glucose sensor 110 using, for example, any suitable latch or a switch. An operation by a user may cause the latch to close, thereby electrically coupling the power source to the electrical devices in the glucose sensor 110 to turn it on. For example, the glucose meter 105 in FIG. 1 includes a receptacle 125 configured to receive the glucose sensor 110. The receptacle 125 may also include a mechanical contact that biases a latch in the glucose sensor 110 to couple the power source to the electrical devices therein, thereby actuating the glucose sensor 110. The receptacle 125 may also include a switch (e.g., optical, mechanical, electrical, etc.) that detects the presence of the glucose sensor 110 when disposed therein.

[0024] In this example, when the glucose sensor 110 is disposed in the receptacle 125, the glucose sensor 110 is actuated and the glucose meter 105 is informed that the glucose sensor 110 is disposed in the receptacle 125 in a single step. In other examples, the user may initiate that the glucose sensor is proximate to the glucose meter by depressing a button disposed on the glucose meter 105 and/or the glucose sensor 110, for example. To enable communication, unique information must be exchanged to indicate that the transmitted data is provided from the glucose meter 105 and/or glucose sensor 110. As noted above, prior devices used a number unique on the device itself that identified it. However, the example glucose meter and/or the example sensor generate a secret key using a random process and exchange the secret key using the NFC wireless link. Using the secret key, the glucose meter 105 and glucose sensor 110 encrypt and decrypt data based on the secret key.

[0025] In a preferred embodiment, the glucose sensor 110 remains idle in a low or zero power state until the glucose meter 105 is brought into close proximity to the sensor. In this example, it will be understood that the roles of the sensor and meter may be exchanged, and only the example of the sensor remaining in a low power state until activated is provided herein. Both the sensor 110 and the meter 105 include an inductive element 208/308 for NFC communication. Preferably, the meter 105 is brought into close proximity to the sensor 110, and then the meter's inductive element 208 is energized. The energized inductive element 208 produces a magnetic field that induces a current in the sensor 105 inductive element 308 due to their close proximity. The sensor is preferably programmed to begin the pairing process when the appropriate current is induced in the inductive element 308 by the energized meter inductive

element 208. Advantageously, this method avoids unnecessary battery drain that results from conventional methods of pairing including periodic polling. Moreover, the inductive nature of the pairing permits energy to be delivered to the sensor from the energized meter inductive element 308 due to the inductive link, further reducing battery drain, and even charging the battery of the sensor.

[0026] Further, the glucose meter 105 and the glucose sensor 110 may also exchange information relating to the health of the glucose sensor 110 (e.g., spoilage information, battery status, expiration date, etc.) to determine if the glucose sensor 110 is suitable for use. For instance, the glucose sensor 110 may transmit a preprogrammed expiration date to the glucose meter 105, which determines if the glucose sensor 110 is safe to use. In another example, the glucose sensor 110 may determine that it has spoiled by being exposed to a predetermined temperature for a particular period of time. As such, the glucose sensor 110 may transmit an indication of the duration it was exposed to the predetermined temperature to the glucose meter 105, which determines if the glucose sensor 110 is safe to use. In the event that the glucose meter 105 determines the glucose sensor 110 is not safe to use, the shared key is not exchanged to prevent use of the glucose sensor 110 with the glucose meter 105.

[0027] FIG. 2 illustrates a block diagram of an example glucose meter 105. Generally, the glucose meter 105 includes a controller 200 that is implemented by any suitable device to control the operation of the glucose meter 105 (e.g., a microcontroller, a microprocessor, an application specific integrated circuit, a functional programmable gate array, etc.). The controller 200 in the example of FIG. 2 includes an antenna 202 configured for receiving wireless communication signals and transmitting the received signals to an RF receiver 204, which converts (e.g., amplifies, demodulates, decodes, etc.) the received signal into data for the controller 200. In some examples, the controller 200 may need to process (e.g., decode, error check etc.) the received data before use.

[0028] As described above, the glucose meter 105 also includes an NFC transceiver 206 for sending and receiving data over the NFC wireless link. In such an example, the NFC transceiver 206 receives data from the controller 200 to transmit the data via an inductor 208. As described above, a current flowing through the inductor 208 creates an electric field that induces a voltage in a corresponding inductor. Similarly, a voltage can be induced on the inductor 208 that is received by the NFC transceiver 206, thereby receiving a signal from a transmitting device. The NFC transceiver 206 receives the transmitted signal, converts it into the transmitted signal into data, which is then provided to the controller 200.

[0029] The controller 200 is coupled to receive data from an interface unit 210. The interface unit 210 is any suitable interface to operate the glucose meter. For example, the interface unit 210 may include a one or more buttons that allow the user to control the glucose meter 105. The controller 200 is further coupled to the display driver 212 to provide instructions thereto to control a display 214. That is, the controller 200 provides instructions to the display driver 212 to display information for the user's consumption. In some examples, the display driver 212 may be integral with the controller 200.

[0030] FIG. 3 illustrates a block diagram of an example glucose sensor 110. Although the glucose sensor 110 is illustrated as a single device, it can be implemented by detachable modules that are fastened together. Generally, the glucose sensor 110 includes a controller 300 that is implemented by any suitable device to control the operation of the glucose sensor 110 (e.g., a microcontroller, a microprocessor, an application specific integrated circuit, a functional programmable gate array, etc.). The controller 300 is the example of FIG. 3 includes an antenna 302 configured for transmitting wireless communication signals and received signals from an RF transmitter 304, which converts (e.g., amplifies, demodulates, decodes, interleaves, etc.) data received from the controller 300 for transmission to a receiving device such as the glucose meter 105, for example. In some examples, the controller 300 may need to process (e.g., encode, generate error check data, etc.) the data before transmission.

[0031] As described above, the glucose sensor 110 also includes an NFC transceiver 306 for sending and receiving data over the NFC wireless link. In such an example, the NFC transceiver 306 receives data from the controller 300 to transmit the data via an inductor 308. In the event a current flows through the inductor 308, the inductor 308 creates an electric field that induces a voltage in a corresponding inductor. Similarly, a voltage can be induced on the inductor 308 that is received by the NFC transceiver 306, thereby receiving a signal from a transmitting device. The NFC transceiver 306 receives the transmitted signal, converts it into the transmitted signal into data, which is then provided to the controller 300. In other examples, the NFC transceiver 306 may be configured for simplex transmission as well.

[0032] The glucose sensor 110 also includes a sensor 310 that is configured to interface with the filament 115 and receive data therefrom. The sensor 310 converts the data into digital form and transmits the information to controller 300. Accordingly, the controller 300 receives the data and generates a glucose measurement of the user, and then transmits the measurement via the RF transmitter 304 to the glucose meter 105. Using the received data, the glucose meter 105 displays the current glucose measurement on its display 214. In another example, the sensor 310 may be integral with the controller 300. As noted above, the glucose sensor 110 may be modular such that different modules can be replaced at different time intervals. For example, the sensor 310 may be implemented in a separate module for replacement every week.

[0033] In the examples of FIGS. 2 and 3, the RF receiver 204 and the RF transmitter 304 are generally described using a simplex transmission scheme. However, in other examples, duplex communication may be required. As such, the glucose meter 105 and glucose sensor 110 would include an RF transceiver for duplex communication. Further, any suitable wireless link that allows encryption of traffic and an error check to determine that the data was properly decrypted may be implemented between the glucose meter 105 and glucose sensor 110. For example, a suitable communication link may be provided by standardized communication protocols such as ZigBee®, Bluetooth®, 802.11 related standards, radio frequency identification (RFID), and so forth. Generally, low power modes such as Bluetooth® low energy (BLE) are preferable due to the glucose sensor 110 being disposable.

[0034] FIG. 4 illustrates an example process 400 of synchronizing the glucose meter and glucose sensor. The particular sequence of communications is described with reference to the data that is transmitted and received, but without reference to the transmitting or receiving device because the glucose meter and glucose sensor may perform either function. That is, the glucose meter could be the transmitter, receiver, or both. Similarly, the glucose sensor could be the transmitter, the receiver, or both.

[0035] Initially, the glucose sensor is placed in proximity with the glucose meter at block 405. Generally, the glucose sensor must be placed within range to initiate an NFC link, as described above. In some examples, the glucose sensor may be placed in a receptacle of the glucose meter. Preferably, the glucose meter inductor 208 is energized in close proximity to the glucose sensor inductor 308, such that a current is induced in the glucose sensor inductor 308. The induced current in the glucose sensor inductor 308 preferably triggers the pairing process to begin. At block 410, the example process 400 receives an instruction to setup a secure channel between the glucose sensor and the glucose meter. For example, in the event the glucose meter includes a receptacle having a detector to detect when the sensor is disposed therein, the glucose meter generates a signal to indicate to setup a secure channel with the glucose sensor. In other examples, the glucose meter and/or glucose sensor may include a switch that a user depresses to pair the glucose sensor with the glucose meter.

[0036] In response to the instruction provided at block 410, a determination is made if the glucose sensor is suitable for operation at block 415 using the NFC wireless link. For example, a determination is made that the glucose sensor has suitable battery power to operate for a required period (e.g., at least one day, etc.). In another example, a determination is made that the glucose sensor has not spoiled due to an expiration date or due to exposure to unsuitable environmental conditions (e.g., temperature, humidity, etc.). If the sensor fails the determination at block 415, the glucose meter cannot pair the glucose sensor and the example process 400 ends.

[0037] In the event that the sensor succeeds in the determination at block 415, the example process 400 generates a secret key and transmits the secret key over the NFC link so that both the glucose sensor and the glucose meter share the same secret key at step 420. In one example, the secret key is generated by any suitable random process for securing a wireless link. For example, the example process 400 may implement a cryptographically secure pseudorandom number generator to generate a 128-bit secret key. Because the glucose meter and the glucose sensor must be close in proximity, it is unlikely any other device will be nearby to receive or intercept the secret key. Further, once transmitted, there generally is no need to exchange the secret key again.

[0038] After both the glucose meter and the glucose sensor have identical secret keys, the glucose sensor and glucose meter setup a secure wireless channel that is different from the NFC link (e.g., Bluetooth® low power, ZigBee®, a custom wireless link, etc). In particular, the glucose meter and glucose sensor transmit data over the wireless channel that is encrypted using any suitable encryption algorithm (e.g., advanced encryption standard, data encryption standard, etc.) using the secret key, thereby forming a secure wireless link. In one example, using the data for transmission, the transmitting device generates an error check infor-

mation such as a cyclic redundancy check (CRC) or a hash such as MD5, which is encrypted and transmitted with the data. The receiving device will decrypt the received information using the secret key and verify that the decryption is successful using the error check information. In another example, the CGM system 100 may verify that the secret key was successfully received before transmission of glucose measurement data over the secure wireless link.

[0039] After the glucose meter and the glucose sensor are transmitting the data via the secure wireless link at step 430, the example process 400 ends. Generally, the glucose meter or the glucose sensor will provide a perceptible indication to the user that communication has initiated and the user may fasten the glucose sensor to their skin.

[0040] Although example process 400 describes a particular sequence of events, the example process 400 is not limited and could be modified to perform all or some of the described functionality. For instance, determining that the sensor is suitable for operation at block 415 may be omitted.

[0041] FIGS. 5-8 illustrate examples of different sequences of communication between the glucose meter 105 and the glucose sensor 110 to implement the example process 400. In the described examples, the glucose meter 105 and glucose sensor 110 are close in proximity such that they communicate via the NFC wireless link. Unless otherwise indicated, the described communications are generally performed over the NFC wireless link until the secure wireless link is fully setup.

[0042] FIG. 5 illustrates an example of a CGM system 100 that determines the health of the glucose sensor 110 before data transmission can begin. At step 502, the glucose meter 105 receives an instruction to setup a secure wireless link with the glucose sensor 110. In response, the glucose meter 105 transmits a request to the glucose sensor 110 for health information at step 504. In some examples, an initial message would indicate that the glucose meter 105 is requesting the information without explicit instructions. The glucose sensor 110 generates its health information (e.g., battery voltage, spoilage information, temperature information, expiration date, etc.) and transmits the health information to the glucose meter 105 at step 506. Using the received health information of the glucose sensor 110, the glucose meter 105 determines if the glucose sensor 110 is suitable for use in the CGM system at step 508. If the glucose sensor 110 is not suitable, the communications ends and the glucose sensor 110 is not paired with the glucose meter 105, as described above. For example, the glucose meter 105 could transmit a kill signal to the glucose sensor 110, which fully disables the glucose sensor 110.

[0043] If the glucose sensor 110 is determined to be suitable for use at step 508, the glucose meter 105 generates a secret key that is transmitted to the glucose sensor at step 510. As noted above, the secret key may be generated by any suitable random process for securing the wireless link. At step 512, the glucose sensor 110 stores the secret key and sets up the channel with the glucose meter 105. The glucose sensor 110 then begins transmitting data associated with a measurement of the user (e.g., glucose information, etc.) to the glucose meter at step 514 over the secure channel.

[0044] FIG. 6 illustrates another example of a CGM system that implements a passive glucose sensor that has a one-time programmable (OTP) radio frequency identification (RFID) tag. In such an example, at step 602, the glucose meter 105 receives an instruction to setup a secure wireless

link with the glucose sensor 110. In response, the glucose meter 105 generates a secret key and transmits the secret key to the glucose sensor 110 at step 604. Using the received secret key, the glucose sensor 110 programs the secret key into its memory at step 606. For example, the glucose sensor 110 could include a Class 1 RFID tag that is programmable a single time with the secret key. In this example, the glucose meter 105 initiates reception of data using the secret key in response to transmitting the secret key. After the glucose sensor 110 has programmed the secret key, it begins transmitting data over the secure channel at step 608. In other examples, the glucose sensor 110 can be disabled by providing a kill instruction from the glucose meter 105.

[0045] In the example of FIG. 6, the OTP glucose sensor 110 implements a simple, low cost passive NFC link that provides limited functionality and is disposable. In this example, the glucose sensor 110 cannot be programmed with another secret key, thereby preventing it from being used again for safety purposes.

[0046] In other examples, the glucose sensor 110 may provide more functionality and thereby require a longer operational period. As such, it may be beneficial to enable the glucose sensor 110 to be reconfigured with the glucose meter 105. In the example of FIG. 7, at step 702, the glucose sensor 110 receives instruction to setup a secure wireless link with the glucose meter 105. In response, at step 704, the glucose sensor 110 generates a secret key and transmits it to the glucose meter 105. In response to receiving the secret key, the glucose meter 706 initiates reception of the wireless channel using the secret key at step 706. The glucose sensor 110 may wait a predetermined period of time (e.g., 1 second) for the glucose meter 105 to initiate data reception. After this period of time expires, the glucose sensor 110 transmits data over the secure channel at step 708.

[0047] In the example of FIG. 7, the glucose sensor 110 is reprogrammable and therefore can be reused. For instance, the glucose meter 105 may also include an insulin pump that is replaced monthly by the user. In such an example, the glucose meter 105 may need its power source (e.g. a battery, etc.) to be replaced, thereby requiring the secure wireless channel to be temporarily disabled. As such, after actuating the glucose meter 105 with a new power source, the glucose meter 105 and the glucose sensor 110 would exchange another secret key to initiate communication again. In another example, the battery in the glucose sensor 110 may be fastened such that it is not replaceable, and a new glucose sensor would be needed.

[0048] FIG. 8 illustrates another CGM system 100 that verifies successful reception of the secret key. At step 802, the glucose meter 105 receives an instruction to setup a secure wireless link with the glucose sensor 110. In response, the glucose meter 105 generates and transmits a secret key to the glucose sensor 110 at step 804. The glucose sensor 110 stores the secret key at step 806 to initiate setup of the secure wireless link. Initially, the glucose sensor 110 transmits test data to the glucose meter 105 at step 808. The test data could be a random data or predetermined data that the glucose meter 105 also possesses. In the event the data is random, the transmitted data would include error check information to determine successful reception and decryption of the random data.

[0049] In response to receiving the test data, the glucose meter 105 decrypts the test data and determines if the test data was successfully received at step 810. If the test data is

successfully received, the glucose meter **105** then determines that the secret key was successfully received by the glucose sensor **110**. The glucose meter **105** then transmits an acknowledge message to the glucose sensor **110** via either the NFC link of the secure wireless channel at step **812**. Upon reception of the acknowledge message, the glucose sensor **110** has fully setup the secure wireless channel and begins transmission of data using the secure wireless channel at step **814**. In the event that the glucose meter **105** does not verify the secret key at **810**, the sequence of communication would return to step **804** until the secret key is successfully determined to be received by the glucose sensor **110**.

**[0050]** In accordance with an illustrative embodiment of the present invention, an inductive coupling link is provided to extend product shelf-life and improve patient data security of RF-controlled devices having factory-installed, non-accessible primary-cell batteries such as an internal sensor (such as an internal patch, subcutaneous sensor, or internal electrode, among other sensing devices). RF receiver circuitry for the heavily used bands available to such devices demodulates and examines received signals in order to determine whether the signal is of interest to the device. This can require too much power to be performed continuously. Therefore, low-power RF devices generally synchronize with their counterparts, and thereafter operate intermittently (e.g., on a predetermined schedule).

**[0051]** In the case of a sealed consumable product (such as an implanted consumable sensor **110**), linked via RF communication to a reusable/durable user interface and control device (such as a durable handheld meter **105**), deployment of a new device involves, in part, the synchronization and “pairing” of the consumable device and the durable device (s). In order for this initial, unscheduled exchange to take place, the consumable device must be listening for a message from an as-yet unknown instance of a durable device. Because the initial communication may occur days or months after manufacture, the consumable device’s pre-synchronization listening would occur only at fairly infrequent intervals. The length of the interval would directly affect the user, as synchronization at time of deployment would require maintaining the new consumable device **30** within communication range of the durable device(s) for at least the length of this interval prior to use.

**[0052]** In accordance with an aspect of an illustrative embodiment of the present invention, the inductive coupling link augments the consumable device **110** by including a second means of communication between the durable device (s) **105** and the consumable device **110**. This second communication mechanism is used, for example, in lieu of the normal RF link (that is, the RF link used during regular operation of the sensor **30** following initialization) for the purpose of initial synchronization and pairing. By employing inductive (quasi-static H-field) coupling with relatively simple modulation, for example, a passive detector on the consumable product **110** can draw its operating power from the signal itself, and remain ready-to-detect at all times without consuming battery power. This improves responsiveness of the sensor **110**, while extending its shelf life.

**[0053]** The pairing operation mentioned above allows the durable device(s) **105** and consumable devices **110** to exchange cryptographic keys and identifying information that ensures that subsequent communication between the devices **110** and **105** is secure. The pairing operation itself,

however, is vulnerable to attack, if the pairing is compromised, the security of subsequent operations may also be compromised. By using an inductive coupling link to perform certain steps of the pairing operation, however, the security of the transaction is greatly increased because of the unlikelihood of the short-range, relatively nonstandard inductive coupling transmission being correctly received and decoded.

**[0054]** It should further be appreciated that the nature of the inductive coupling described above is capable of delivering energy to the consumable device **110** from the durable device **105** via the inductive link, further lengthening the battery and shelf life of the consumable device **110**.

**[0055]** A diabetes management system (e.g., a continuous glucose monitoring system) is described for illustrative purposes, but it is to be understood that the improved methods, devices and systems can be used for monitors or other devices for management of other physiological conditions such as, but not limited to, arrhythmia, heart failure, coronary heart disease, diabetes, sleep apnea, seizures, asthma, chronic obstructive pulmonary disease (COPD), pregnancy complications, tissue or wound state, state of wellness and fitness of a person (e.g., weight loss, obesity, heart rate, cardiac performance, dehydration rate, blood glucose, physical activity or caloric intake), or combinations thereof.

**[0056]** Some examples of a meter **105** can be, but is not limited to, a personal computer, a portable computer such as a laptop or a handheld device (e.g., personal digital assistant (PDA), iPod), mobile telephone such as a cellular telephone, Blackberry device, Palm device, or Apple iPhone device, a watch, a portable exercise device or other physiological data monitor (e.g., a meter connectable to a patient via a strap or incorporated into an article of clothing), among other user devices, each of which may be configured for data communication with the sensor or consumable device **110**.

**[0057]** Some examples of measured or monitored physiological data include, but are not limited to ECG, EEG, EMG, SpO<sub>2</sub>, tissue impedance, heart rate, accelerometer, blood glucose, coagulation (e.g., PT-INR or prothrombin time (PT) and its derived measures of prothrombin ratio (PR) and international normalized ratio), respiration rate and airflow volume, body tissue state, bone state, pressure, physical movement, body fluid density, skin or body impedance, body temperature, patient physical location, or audible body sounds, among others, or a combination thereof.

**[0058]** The measured data can also be related to analytes such as, but not limited to, a substance or chemical constituent in a biological fluid (for example, blood, interstitial fluid, cerebral spinal fluid, lymph fluid or urine) that can be analyzed. Analytes can include naturally occurring substances, artificial substances, medicaments, metabolites, and/or reaction products. By way of examples, one or more analytes for measurement can be glucose; insulin; acarboxy-prothrombin; acylcarnitine; adenine phosphoribosyl transferase; adenosine deaminase; albumin; alpha-fetoprotein; amino acid profiles (arginine (Krebs cycle), histidine/urocanic acid, homocysteine, phenylalanine/tyrosine, tryptophan); androstenedione; antipyrine; arabinitol enantiomers; arginase; benzoylecgonine (cocaine); blotinidase; bioprotein; c-reactive protein; carnitine; carnosinase; CD4; ceruloplasmin; chenodeoxycholic acid; chloroquine; cholesterol; cholinesterase; conjugated 1-beta. hydroxy-cholic acid; cortisol; creatine kinase; creatine kinase MM isoen-

zyme; cyclosporin A; d-penicillamine; de-ethylchloroquine; dehydroepiandrosterone sulfate; DNA (acetylator polymorphism, alcohol dehydrogenase, alpha 1-antitrypsin, cystic fibrosis, Duchenne/Becker muscular dystrophy, glucose-6-phosphate dehydrogenase, hemoglobin A, hemoglobin S, hemoglobin C, hemoglobin D, hemoglobin E, hemoglobin F, D-Punjab, beta-thalassemia, hepatitis B virus, HCMV, HIV-1, HTLV-1, Leber hereditary optic neuropathy, MCAD, RNA, PKU, Plasmodium vivax, sexual differentiation, 21-deoxycortisol); desbutylhalofantrine; dihydropteridine reductase; diphtheria/tetanus antitoxin; erythrocyte arginase; erythrocyte protoporphyrin; esterase D; fatty acids/acylglycines; free.beta.-human chorionic gonadotropin; free erythrocyte porphyrin; free thyroxine (FT4); free tri-iodothyronine (FT3); fumarylacetoacetase; galactose/gal-1-phosphate; galactose-1-phosphate uridylyltransferase; gentamicin; glucose-6-phosphate dehydrogenase; glutathione; glutathione peroxidase; glycocholic acid; glycosylated hemoglobin; halofantrine; hemoglobin variants; hexosaminidase A; human erythrocyte carbonic anhydrase I; 17-alpha-hydroxyprogesterone; hypoxanthine phosphoribosyl transferase; immunoreactive trypsin; lactate; lead; lipoproteins ((a), B/A-1, .beta.); lysozyme; mefloquine; netilmicin; phenobarbitone; phenyloloin; phytanic/pristanic acid; progesterone; prolactin; prolidase; purine nucleoside phosphorylase; quinine; reverse tri-iodothyronine (rT3); selenium; serum pancreatic lipase; sissomicin; somatomedin C; specific antibodies (adenovirus, anti-nuclear antibody, anti-zeta antibody, arbovirus, Aujeszkzy's disease virus, dengue virus, *Dracunculus medinensis*, *Echinococcus granulosus*, *Entamoeba histolytica*, enterovirus, *Giardia duodenalis*, *Helicobacter pylori*, hepatitis B virus, herpes virus, HIV-1, IgE (atopic disease), influenza virus, *Leishmania donovani*, leptospira, measles/mumps/rubella, *Mycobacterium leprae*, *Mycoplasma pneumoniae*, Myoglobin, *Onchocerca volvulus*, parainfluenza virus, *Plasmodium falciparum*, poliovirus, *Pseudomonas aeruginosa*, respiratory syncytial virus, *rickettsia* (scrub typhus), *Schistosoma mansoni*, *Toxoplasma gondii*, *Treponema pallidum*, *Trypanosoma cruzi/rangeli*, vesicular stomatitis virus, *Wuchereria bancrofti*, yellow fever virus); specific antigens (hepatitis B virus, HIV-1); succinylacetone; sulfadoxine; theophylline; thyrotropin (TSH); thyroxine (T4); thyroxine-binding globulin; trace elements; transferrin; UDP-galactose-4-epimerase; urea; uroporphyrinogen I synthase; vitamin A; white blood cells; and zinc protoporphyrin.

**[0059]** Salts, sugar, protein, fat, vitamins and hormones naturally occurring in blood or interstitial fluids can also constitute analytes, for example. Further, the analyte can be naturally present in the biological fluid, for example, a metabolic product, a hormone, an antigen, an antibody, and the like. Alternatively, the analyte can be introduced into the body such as, for example but not limited to, a contrast agent for imaging, a radioisotope, a chemical agent, a fluorocarbon-based synthetic blood, or a drug or pharmaceutical composition, including but not limited to insulin; ethanol; *cannabis* (marijuana, tetrahydrocannabinol, hashish); inhalants (nitrous oxide, amyl nitrite, butyl nitrite, chlorohydrocarbons, hydrocarbons); cocaine (crack cocaine); stimulants (amphetamines, methamphetamines, Ritalin, Cylert, Preludin, Didrex, PreState, Voranil, Sandrex, Plegine); depressants (barbituates, methaqualone, tranquilizers such as Valium, Librium, Miltown, Serax, Equanil, Tranxene); hallucinogens (phencyclidine, lysergic acid, mescaline, peyote,

psilocybin); narcotics (heroin, codeine, morphine, opium, meperidine, Percocet, Percodan, Tussionex, Fentanyl, Darvon, Talwin, Lomotil); designer drugs (analogs of fentanyl, meperidine, amphetamines, methamphetamines, and phencyclidine, for example, Ecstasy); anabolic steroids; and nicotine. The metabolic products of drugs and pharmaceutical compositions can also be considered analytes. Analytes such as neurochemicals and other chemicals generated within the body can also be analyzed, such as, for example, ascorbic acid, uric acid, dopamine, noradrenaline, 3-methoxytyramine (3MT), 3,4-dihydroxyphenylacetic acid (DOPAC), homovanillic acid (HVA), 5-hydroxytryptamine (SHT), and 5-hydroxyindoleacetic acid (FHIAA).

**[0060]** Although only a few illustrative embodiments of the present invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the illustrative embodiments without materially departing from the novel teachings and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method for pairing first and second wireless devices in a physiological condition management system, comprising:

placing a first wireless device in proximity with a second wireless device;

generating an indication that the first and second wireless devices are in proximity with each other to establish communication via a near field communication (NFC) link;

generating a secret key at the first wireless device using a random process and sharing the secret key with the second wireless device in response to the indication that the first and second wireless devices are in proximity with each other to establish communication via the NFC link; and

transmitting signals between the first and second wireless devices via a secure radio frequency (RF) link that is different from the NFC link and on which the signals are encrypted using the secret key;

wherein the secret key is not generated until after the first and second wireless devices are placed proximally to each other to establish the NFC link.

2. The method of claim 1, wherein the signals comprise physiological condition data, and the first and second wireless devices are configured to perform physiological condition management operations selected from the group consisting of sensing physiological condition data, displaying physiological condition data, monitoring physiological condition data during a selected time period, monitoring physiological condition data and relevant events during a selected time period wherein the relevant events comprise at least one of food consumption and beverage consumption.

3. The method of claim 1, wherein generating the secret key does not employ user input of an identifier of the second wireless device

4. The method of claim 1, wherein the first and second wireless devices are selected from the group consisting of a handheld device, a physiological condition sensor, a glucose monitoring device, a wireless medical device, and a physiological condition management device, a mobile telephone, an Apple iPhone device, a watch, a portable exercise device, and a physiological data monitor.

5. The method of claim 1, wherein the indication is generated by at least one of the first and second wireless devices in response to an event selected from the group consisting of the first and second wireless devices being electrically coupled to each other, activation of a switch on at least one of the first and second wireless devices, detection of one of the first and second wireless devices being disposed in a receptacle of the other one of the first and second wireless devices, and generation of an induced current in at least one of the first and second wireless devices by the other one of the first and second wireless devices.

6. The method recited in claim 1, wherein the first wireless device is a physiological condition monitoring device and the second wireless device is a physiological condition sensor, and further comprising:

receiving operational information from the physiological condition sensor at the physiological condition monitoring device via the NFC link, the operational information comprising at least one of battery status, expiration data, and spoilage of the physiological condition sensor; and

determining if the physiological condition monitoring device can transmit the secret key to the physiological condition sensor based on the operational information.

7. The method of claim 1, wherein the NFC link is an inductive link and the range of the secure wireless link exceeds the range of the NFC link.

8. The method of claim 7, wherein the first and second wireless devices are proximate when placed within approximately 20 centimeters.

9. The method of claim 1, further comprising the steps of: after placing the first and second wireless devices in proximity with each other, energizing an inductive element in one of the first and second wireless devices, and

inducing a current in an inductive element in the other one of the first and second wireless devices.

10. The method of claim 9, further comprising storing energy in the other one of the first and second wireless devices from the induced current.

11. The method of claim 9, further comprising the step of, when inductive element in one of the first and second wireless devices induces the current in the inductive element of the other one of the first and second wireless devices, generating the indication that the NFC link is established to initialize the generating of a secret key.

12. A physiological condition management system, comprising:

first and second wireless devices configured to perform physiological condition management operations, at least one of the first and second wireless devices being configured to generate an indication when the first and second wireless devices are in proximity with each other and have established communication via a near field communication (NFC) link;

the first wireless device being configured to generate a secret key using a random process and share the secret key with the second wireless device in response to the indication that the first and second wireless devices are in proximity with each other to establish communication via the NFC link; and

the first and second wireless devices being configured to transfer data via a secure radio frequency (RF) link that is different from the NFC link and on which the data is

encrypted using the secret key by at least one of the first and second wireless devices, and at least the other one of the first and second wireless devices being configured to decrypt the data using the secret key;

wherein the secret key is not generated until after the first and second wireless devices are placed proximally to each other to establish the NFC link.

13. The physiological condition management system of claim 12, wherein at least one of the first and second wireless devices comprises a first inductive element adapted to provide an inductive link between the first inductive element and a second inductive element in the other one of the first and second wireless devices.

14. The physiological condition management system of claim 13, wherein the indication is generated and sent in response to an induced current of one of the inductive elements induced by energization in the other of the inductive elements.

15. The physiological condition management system of claim 14, wherein at least one of the first and second wireless devices comprises an energy storage element, and the energy storage element is adapted to be charged by an induced current in the corresponding one of the first inductive element and the second inductive element.

16. The physiological condition management system of claim 12, wherein generating the secret key does not employ user input of an identifier of the second wireless device at the first wireless device.

17. A first wireless device securely paired with a second wireless device in a physiological condition management system, the first wireless device comprising:

a controller configured to perform a physiological condition management operation; and

at least one wireless communication interface for transmitting physiological condition management signals to and from the second wireless device;

wherein the controller is configured

to generate a secret key using a random process and share the secret key with the second wireless device via the at least one wireless communication interface in response to an indication that the first and second wireless devices are in proximity with each other to establish communication via the near field communication (NFC) link, and

to transmit physiological condition management signals to the second wireless device using a secure radio frequency (RF) link that is different from the NFC link based on the secret key, the first wireless device encrypting the physiological condition management signals using the secret key;

wherein the secret key is not generated until after the physiological condition meter and the physiological condition sensor are placed proximally to each other.

18. The first wireless device of claim 17, further comprising a first inductive element adapted to provide an inductive link between the first inductive element and a second inductive element in the second wireless device.

19. The first wireless device of claim 18, wherein the indication is generated by the first wireless device in response to an induced current in the first inductive element.

20. The first wireless device of claim 19, wherein the first inductive element comprises an energy storage element, and the energy storage element is adapted to be charged by an induced current in the first inductive element.

**21.** The first wireless device of claim **17**, wherein generating the secret key by the controller does not employ user input of an identifier of the second wireless device.

\* \* \* \* \*

专利名称(译)	用于传递共享秘密的近场遥测链路在生理条件管理系统中建立安全的射频通信链路		
公开(公告)号	<a href="#">US20180338726A1</a>	公开(公告)日	2018-11-29
申请号	US16/036184	申请日	2018-07-16
[标]申请(专利权)人(译)	贝克顿·迪金森公司		
申请(专利权)人(译)	碧迪公司		
当前申请(专利权)人(译)	碧迪公司		
[标]发明人	YARGER MICHAEL PETISCE JAMES DIRESTA ELLEN BURNS DEBORAH MASON DAVID		
发明人	YARGER, MICHAEL PETISCE, JAMES DIRESTA, ELLEN BURNS, DEBORAH MASON, DAVID		
IPC分类号	A61B5/00 G16H50/20 G06F19/00 A61B5/145 G08C17/02 G16H15/00 H04W4/80 A61B5/024 G16H20/10 G16H20/60		
CPC分类号	G06F19/00 G16H20/10 Y02A90/26 G16H15/00 G16H50/20 H04W4/80 A61B5/72 G08C17/02 A61B5/742 A61B5/002 A61B5/7275 A61B5/14532 A61B5/02438 G16H20/60 G16H40/67 G16H50/30 G06F19/3456		
优先权	14/364597 2014-06-11 US PCT/US2012/069860 2012-12-14 WO 61/576309 2011-12-15 US		
其他公开文献	US10327706		
外部链接	<a href="#">Espacenet</a> <a href="#">USPTO</a>		

摘要(译)

在生理状况管理系统中的第一和第二无线设备之间提供配对。第一和第二无线设备被放置在附近以通过其中一个设备的随机过程发起秘密密钥的生成，并使用无线近场通信 (NFC) 链路与另一设备交换秘密密钥。然后，共享秘密密钥用于加密数据，以通过不同的安全射频 (RF) 无线信道在第一和第二无线设备之间进行通信。

