UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 18/153,336 | 01/11/2023 | Julian C. Borrey | 556430US | 1456 |

22850 7590 03/03/2025

OBLON, MCCLELLAND, MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| BROWN, ANTHONY D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2408 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 03/03/2025 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

OBLONPAT@OBLON.COM
iahmadi@oblon.com
patentdocket@oblon.com

| Office Action Summary | Application No. 18/153,336 | Applicant(s) Borrey, Julian C. | |
|---|---|---|---|
| | Examiner ANTHONY D BROWN | Art Unit 2408 | AIA (FITF) Status Yes |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☑ Responsive to communication(s) filed on 2/6/2025.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims***

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

**Application Papers**

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

### *Notice of Pre-AIA or AIA Status*

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

### *Response to Arguments*

Applicant's arguments, filed 2/6/2025, with respect to the rejection(s) of claim(s) 1-20 under 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Lamenza.

### *Claim Rejections - 35 USC § 103*

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis (i.e., changing from AIA to pre-AIA) for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim(s) 1-20 are rejected under 35 U.S.C. 103 as being unpatentable over Andersen (US Patent Pub. 2014/0185805) in view of Lamenza (US Patent Pub. 2015/0061404).

**As per claims 1**: A method for preventing attacks during a wireless pairing of an implanted device implanted in a subject and an external device, the method comprising (**see abstract**):

detecting, by the implanted device a varying magnetic field that includes a pairing code (**Paragraph 35; the implantable neurostimulator detects the magnet and, in conjunction with the programmer requesting authorization, (i.e., when a secure channel has been established.), the implant delivers its cipher key to the programmer**);

analyzing, by the implanted device, the varying magnetic field that includes the pairing code to identify the pairing code (**Paragraph 62; detect a magnetic field. For example, such a magnet sensor 130 can be configured to detect the presence of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator 106 by the patient 124 or a caregiver**);

performing, by the implanted device, a key exchange using the pairing code (**Paragraph 89; after the clinician instructs the external device to cause a request for authorization to be transmitted to the implantable device, the external device receives the clinician's request and generates 502 an authorization request transmittal instruction. This authorization request transmittal instruction instructs an authorization request to be transmitted to the implantable device**);

determining, by the implanted device, whether values exchanged in the key exchange match (**Paragraph 25; providing a secure channel that requires relatively high overhead, in terms of computational resources, is the well-known key exchange protocol, Diffie-Hellman, requires high computational resources. In a Diffie-Hellman key exchange protocol, each communication session requires software running in the implanted device and in the external device to generate a random number, x**); and

confirming or rejecting, by the implanted device, a wireless connection between the implanted device and the external device based on determining whether the values exchanged in the key exchange match (**Paragraph 91; After the implantable device receives 506 the authorization request and receives 508 the indication of a detected magnet, the implantable device generates 510 a first cipher key transmittal instruction**).

However, Andersen does not specifically disclose a varying magnetic field that includes a pairing code.

Lamenza discloses magnetic field in proximity of the source...The source may transmit first information to the device. The device may receive the first information by detecting change...The first information may include a Bluetooth pairing code for the source Bluetooth communication module and/or other unique code. The device may initiate out-of-band communication and send a second information to the source via the out-of-band communication channel. The second information may include the unique Bluetooth pairing code (**Paragraph 252**).

Therefore, it would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains, having the teachings of Andersen and Lamenza in it's entirety, to modify the technique of Andersen for detect the presence of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator by adopting Lamenza's teaching for first information may include a Bluetooth pairing code. The motivation would have been to improve preventing attacks during a wireless pairing of an implanted device implanted in a subject and an external device.

**As per claim 2**: The method of claim 1, wherein: the implanted device is implanted in a brain of the subject; and the external device is a computing device comprising an application for managing the implanted device (**Paragraph 57; the implantable neurostimulator 106 may selectively be put in communication with a programmer 120 or a patient remote monitor 126 to wirelessly transmit data from the implantable neurostimulator 106 (i.e., to interrogate the implantable neurostimulator 106 and/or monitor electrographic signals from the patient 124 in real time with an external component) or to transmit information to the implantable neurostimulator 106 (e.g., programming instructions, updates to code the neurostimulator uses to carry out its functions, etc.)**).

**As per claim 3**: The method of claim 1, wherein: the external device is a first external device; and the implanted device comprises an induction coil that receives the varying magnetic field from a second external device (**Paragraph 62; detect a magnetic field. For example, such a magnet sensor 130 can be configured to detect the presence**

**of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator 106 by the patient 124 or a caregiver**).

**As per claim 4**: The method of claim 3, further comprising: translating, by the second external device, numerical values corresponding to the pairing code into field strength values corresponding to the varying magnetic field; and inducing, by the second external device, the varying magnetic field in the implanted device (**Paragraph 35; the implantable neurostimulator detects the magnet and, in conjunction with the programmer requesting authorization, (i.e., when a secure channel has been established.), the implant delivers its cipher key to the programmer**).

**As per claim 5**: The method of claim 3, wherein: the second external device is a charging device (**Paragraph 58; laptops or tablets or other computers**).

**As per claim 6**: The method of claim 3, wherein: the second external device is a smartphone (**Paragraph 58; laptops or tablets or other computers**).

**As per claims 7, 12 and 19**: The method of claim 1, wherein: the key exchange comprises a Diffie-Hellman key exchange (**Paragraph 25; providing a secure channel that requires relatively high overhead, in terms of computational resources, is the well-known key exchange protocol, Diffie-Hellman, requires high computational resources. In a Diffie-Hellman key exchange protocol, each communication session requires software running in the implanted device and in the external device to generate a random number, x**).

**As per claim 8**: (Original) A method for preventing attacks during a wireless pairing of an implanted device implanted in a subject and an external device, the method comprising (**see abstract**):

detecting, by the implanted device, neural signals from a brain of the subject (**Paragraph 35; the implantable neurostimulator detects the magnet and, in conjunction with the programmer requesting authorization, (i.e., when a secure channel has been established.), the implant delivers its cipher key to the programmer**);

analyzing, by the implanted device, the neural signals to identify a pairing code (**Paragraph 62; detect a magnetic field. For example, such a magnet sensor 130 can be configured to detect the presence of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator 106 by the patient 124 or a caregiver**);

performing, by the implanted device, a key exchange using the pairing code (**Paragraph 89; after the clinician instructs the external device to cause a request for authorization to be transmitted to the implantable device, the external device receives the clinician's request and generates 502 an authorization request transmittal instruction. This authorization request transmittal instruction instructs an authorization request to be transmitted to the implantable device**);

determining, by the implanted device, whether values exchanged in the key exchange match (**Paragraph 25; providing a secure channel that requires relatively high overhead, in terms of computational resources, is the well-known key exchange protocol, Diffie-Hellman, requires high computational resources. In a Diffie-Hellman key exchange protocol, each communication session requires software running in the implanted device and in the external device to generate a random number, x**); and

confirming or rejecting, by the implanted device, a wireless connection between the implanted device and the external device based on determining whether the values exchanged in the key exchange match (**Paragraph 91; After the implantable device receives 506 the authorization request and receives 508 the indication of a detected magnet, the implantable device generates 510 a first cipher key transmittal instruction**).

However, Andersen does not specifically disclose identify a pairing code and a key exchange using the pairing code.

Lamenza discloses magnetic field in proximity of the source...The source may transmit first information to the device. The device may receive the first information by detecting change...The first information may include a Bluetooth pairing code for the source Bluetooth communication module and/or other unique code. The device may initiate out-of-band communication and send a second information to the source via the out-of-band communication channel. The second information may include the unique Bluetooth pairing code (**Paragraph 252**).

Therefore, it would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains, having the teachings of Andersen and Lamenza in it's entirety, to modify the technique of Andersen for detect the presence of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator by adopting Lamenza's teaching for first information may include a Bluetooth pairing code. The motivation would have been to improve preventing attacks during a wireless pairing of an implanted device implanted in a subject and an external device.

**As per claim 9**: (Original) The method of claim 8, wherein the neural signals are detected via a plurality of electrodes implanted in the brain of the subject and communicatively coupled to the implanted device (**Paragraph 57; the implantable neurostimulator 106 may selectively be put in communication with a programmer 120 or a patient remote monitor 126 to wirelessly transmit data from the implantable neurostimulator 106 (i.e., to interrogate the implantable neurostimulator 106 and/or monitor electrographic signals from the patient 124 in real time with an external component) or to transmit information to the implantable neurostimulator 106 (e.g., programming instructions, updates to code the neurostimulator uses to carry out its functions, etc.)**).

**As per claim 10**: (Original) The method of claim 8, further comprising:

indicating, by the external device, the pairing code to the subject, wherein the neural signals are detected responsive to the indicating of the pairing code (**Paragraph 62; detect a magnetic field. For example, such a magnet sensor 130 can be configured to detect the presence of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator 106 by the patient 124 or a caregiver**).

**As per claim 11**: (Original) The method of claim 8, wherein: the external device is a computing device comprising an application for managing the implanted device (**Paragraph 58; laptops or tablets or other computers**).

**As per claim 13**: (Original) A method for preventing attacks during a wireless pairing of an implanted device implanted in a brain of a subject and a first external device, the method comprising (**see abstract**):

identifying, by the implanted device, a first pairing code via a key exchange with the first external device (**Paragraph 35; the implantable neurostimulator detects the magnet and, in conjunction with the programmer requesting authorization, (i.e., when a secure channel has been established.), the implant delivers its cipher key to the programmer**);

transmitting, by the implanted device, the first pairing code to a second external device to output the first pairing code (**Paragraph 89; after the clinician instructs the external device to cause a request for authorization to be transmitted to the implantable device, the external device receives the clinician's request and generates 502 an authorization request transmittal instruction. This authorization request transmittal instruction instructs an authorization request to be transmitted to the implantable device**);

responsive to transmitting the first pairing code to the second external device, receiving, by the implanted device, a code confirmation from the subject via the second external device, wherein the code confirmation indicates a match between the first pairing code and a second pairing code output by the first external device (**Paragraph 25; providing a secure channel that requires relatively high overhead, in terms of computational resources, is the well-known key exchange protocol, Diffie-Hellman, requires high computational resources. In a Diffie-Hellman key exchange protocol, each communication session requires software running in the implanted device and in the external device to generate a random number, x**); and

confirming, by the implanted device, a wireless connection between the implanted device and the first external device based on receiving the code confirmation (**Paragraph 91; After the implantable device receives 506 the authorization request and receives 508 the indication of a detected magnet, the implantable device generates 510 a first cipher key transmittal instruction**).

However, Andersen does not specifically disclose the first pairing code.

Lamenza discloses magnetic field in proximity of the source...The source may transmit first information to the device. The device may receive the first information by detecting change...The first information may include a Bluetooth pairing code for the source Bluetooth communication module and/or other unique code. The device may initiate out-of-band communication and send a second information to the source via the out-of-band communication channel. The second information may include the unique Bluetooth pairing code (**Paragraph 252**).

Therefore, it would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains, having the teachings of Andersen and Lamenza in it's entirety, to modify the technique of Andersen for detect the presence of a magnetic field when an external magnet is moved into the vicinity of the implantable neurostimulator by adopting Lamenza's teaching for first information may include a Bluetooth pairing code. The motivation would have been to improve preventing attacks during a wireless pairing of an implanted device implanted in a subject and an external device.

**As per claim 14**: (Original) The method of claim 13, wherein:

the second external device outputs the first pairing code audibly to the subject for confirmation (**Paragraph 35; the implantable neurostimulator detects the magnet and, in conjunction with the programmer requesting authorization, (i.e., when a secure channel has been established.), the implant delivers its cipher key to the programmer**).

**As per claim 15**: (Original) The method of claim 13, wherein: the first external device identifies the second pairing code via the key exchange; and the first external device displays the second pairing code to the subject for confirmation (**Paragraph 25; providing a secure channel that requires relatively high overhead, in terms of computational resources, is the well-known key exchange protocol, Diffie-Hellman, requires high computational resources. In a Diffie-Hellman key exchange protocol, each communication session requires software running in the implanted device and in the external device to generate a random number, x**).

**As per claim 16**: (Original) The method of claim 13, wherein: the second external device is a charging device (**Paragraph 58; laptops or tablets or other computers**).

**As per claim 17**: (Original) The method of claim 13, wherein: the second external device is a smartphone (**Paragraph 58; laptops or tablets or other computers**).

**As per claim 18**: (Original) The method of claim 13, wherein: the first external device is a computing device comprising an application for managing the implanted device (**Paragraph 35; the implantable neurostimulator detects the magnet and, in conjunction with the programmer requesting authorization, (i.e., when a secure**

**channel has been established.), the implant delivers its cipher key to the programmer**).

**As per claim 20**: (New) The method of claim 1, wherein:

the varying magnetic field that includes the pairing code is received from a charging device or a smartphone, the charging device or the smartphone being different from the external device and the implanted device (**Paragraph 58; laptops or tablets or other computers**) (**see Lamenza; Pargraph 252; magnetic field in proximity of the source…The source may transmit first information to the device. The device may receive the first information by detecting change…The first information may include a Bluetooth pairing code for the source Bluetooth communication module and/or other unique code. The device may initiate out-of-band communication and send a second information to the source via the out-of-band communication channel. The second information may include the unique Bluetooth pairing code**).

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

nonprovisional extension fee (37 CFR 1.17(a)) pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

## *Contact Information*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY D BROWN whose telephone number is (571)270-1472. The examiner can normally be reached 730-330pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Linglan Edwards can be reached on 5712705440. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For

additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANTHONY D BROWN/
Primary Examiner, Art Unit 2408