IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for preventing attacks during a wireless pairing of an implanted device implanted in a subject and [[an]] a first external device, the method comprising:

receiving, by the implanted device from a second external device, a varying magnetic field that includes a pairing code, the second external device being different from the first external device and the implanted device,

detecting, by the implanted device, [[a]] the varying magnetic field received from the second external device that includes [[a]] the pairing code;

analyzing, by the implanted device, the varying magnetic field received from the second external device that includes the pairing code to identify the pairing code;

performing, by the implanted device, a key exchange using the pairing code;

determining, by the implanted device, whether values exchanged in the key exchange match; and

confirming or rejecting, by the implanted device, a wireless connection between the implanted device and the first external device based on determining whether the values exchanged in the key exchange match.

2. (Currently Amended) The method of claim 1, wherein:

the implanted device is implanted in a brain of the subject; and

the first external device is a computing device comprising an application for managing the implanted device.

3. (Currently Amended) 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]] the second external device.

4. (Original) 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.

5. (Original) The method of claim 3, wherein:

the second external device is a charging device.

6. (Original) The method of claim 3, wherein:

the second external device is a smartphone.

7. (Original) The method of claim 1, wherein:

the key exchange comprises a Diffie-Hellman key exchange.

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:

detecting, by the implanted device, neural signals from a brain of the subject;

analyzing, by the implanted device, the neural signals to identify a pairing code;

performing, by the implanted device, a key exchange using the pairing code;

determining, by the implanted device, whether values exchanged in the key exchange match; 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.

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.

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.

11. (Original) The method of claim 8, wherein:

the external device is a computing device comprising an application for managing the implanted device.

12. (Original) The method of claim 8, wherein:

the key exchange comprises a Diffie-Hellman key exchange.

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:

identifying, by the implanted device, a first pairing code via a key exchange with the first external device;

transmitting, by the implanted device, the first pairing code to a second external device to output the first pairing code;

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; and

confirming, by the implanted device, a wireless connection between the implanted device and the first external device based on receiving the code confirmation.

14. (Original) The method of claim 13, wherein:

the second external device outputs the first pairing code audibly to the subject for confirmation.

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.

16. (Original) The method of claim 13, wherein:

the second external device is a charging device.

17. (Original) The method of claim 13, wherein:

the second external device is a smartphone.

18. (Original) The method of claim 13, wherein:

the first external device is a computing device comprising an application for managing the implanted device.

19. (Original) The method of claim 13, wherein:

the key exchange comprises a Diffie-Hellman key exchange.

20. (Currently Amended) 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~~ second external device is a helper device or a charging device ~~or the smartphone being different from the external device and~~ that is configured to transmit power to the implanted device.