CLAIMS

1. A computer-implemented method, comprising:

generating, by a first Bluetooth device, a code; encrypting, by the first Bluetooth device, the code to generate a first ciphertext in response to detecting that a Bluetooth connection is disconnected; generating, by the first Bluetooth device, a broadcast packet based on the first ciphertext, and broadcasting the broadcast packet to one or more Bluetooth devices, wherein the one or more Bluetooth devices includes a second Bluetooth device external to the first Bluetooth device; receiving, by the first Bluetooth device, a scanning request from the second Bluetooth device, the scanning request including a random private address generated by the second Bluetooth device; verifying the scanning request from the second Bluetooth device based on the random private address; sending, by the first Bluetooth device and in response to verifying the scanning request, a scanning response to the second Bluetooth device based on the random private address in the scanning request; and establishing, by the first Bluetooth device, a Bluetooth connection with the second Bluetooth device in response to determining that a connection request from the second Bluetooth device is received by the first Bluetooth device in response to the scanning response; wherein verifying the scanning request from the second Bluetooth device based on the random private address occurs after receiving, by the first Bluetooth device, the scanning request from the second Bluetooth device, and before sending the scanning response to the second Bluetooth device, and the verifying comprises: decrypting the random private address in the scanning request by using a second decryption algorithm based on the code and a locally-stored key, to obtain a decrypted fixed address; determining whether a pre-stored fixed address at the first Bluetooth device is the same as the decrypted fixed address, wherein the pre-stored fixed address at the first Bluetooth device, the locally-stored key, and the second decryption algorithm are agreed upon jointly by the first and second Bluetooth devices; and in response to determining that the prestored fixed address is the same as the decrypted fixed address, sending the scanning response to the second Bluetooth device.

2. The computer-implemented method according to claim 1, wherein generating, by the first Bluetooth device, the code comprises:

generating a random number to obtain the code; and

generating, by the first Bluetooth device, the broadcast packet based on the first ciphertext further comprises:

including the code in a plaintext form in the broadcast packet.

3. The computer-implemented method according to claim 1, wherein generating, by the first Bluetooth device, the code comprises:

periodically generating by using a pre-determined algorithm, wherein the pre-determined algorithm is agreed upon jointly by the first and second Bluetooth devices; and

encrypting, by the first Bluetooth device, the code comprises encrypting the code generated in a current period.

4. The computer-implemented method according to claim 1, wherein encrypting, by the first Bluetooth device, the code to generate the first ciphertext comprises:

encrypting the code and a locally-stored key by using a first encryption algorithm to obtain the first ciphertext, wherein the first encryption algorithm is a unidirectional function, and wherein the locally-stored key and the first encryption algorithm are agreed upon jointly by the first and second Bluetooth devices.

5. The computer-implemented method according to claim 1, wherein sending the scanning response to the second Bluetooth device based on the random private address in the scanning request comprises:

encrypting the random private address in the scanning request and a locally-stored key by using a third encryption algorithm to obtain a second ciphertext, wherein the third encryption algorithm is a unidirectional function, and the locally-stored key is agreed upon jointly by the first and second Bluetooth devices;

generating the scanning response by using the second ciphertext; and

sending the scanning response to the second Bluetooth device by using the random private address.

6. The computer-implemented method according to claim 3, wherein

generating, by the first Bluetooth device, the broadcast packet based on the first ciphertext further comprises:

not including the code in a plain text form in the broadcast packet; and

allowing the second Bluetooth device to validate the code using at least information of the current period and the pre-determined algorithm.

7. A computer-implemented system, comprising:

one or more computers; and one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising: generating, by a first Bluetooth device, a code; encrypting, by the first Bluetooth device, the code to generate a first ciphertext in response to detecting that a Bluetooth connection is disconnected; generating, by the first Bluetooth device, a broadcast packet based on the first ciphertext, and broadcasting the broadcast packet to one or more Bluetooth devices, wherein the one or more Bluetooth devices includes a second Bluetooth device external to the first Bluetooth device; receiving, by the first Bluetooth device, a scanning request from the second Bluetooth device, the scanning request including a random private address generated by the second Bluetooth device; verifying the scanning request from the second Bluetooth device based on the random private address; sending, by the first Bluetooth device and in response to verifying the scanning request, a scanning response to the second Bluetooth device based on the random private address in the scanning request; and establishing, by the first Bluetooth device, a Bluetooth connection with the second Bluetooth device in response to determining that a connection request from the second Bluetooth device is received by the first Bluetooth device in response to the scanning response; wherein verifying the scanning request from the second Bluetooth device based on the random private address occurs after receiving, by the first Bluetooth device, the scanning request from the second Bluetooth device, and before sending the scanning response to the second Bluetooth device, and the verifying comprises: decrypting the random private address in the scanning request by using a second decryption algorithm based on the code and a locally-stored key, to obtain a decrypted fixed address; determining whether a pre-stored fixed address at the first Bluetooth device is the same as the decrypted fixed address, wherein the pre-stored fixed address at the first Bluetooth

device, the locally-stored key, and the second decryption algorithm are agreed upon jointly by the first and second Bluetooth devices; and in response to determining that the pre-stored fixed address is the same as the decrypted fixed address, sending the scanning response to the second Bluetooth device.

8. The computer-implemented system according to claim 7, wherein generating, by the first Bluetooth device, the code comprises:

generating a random number to obtain the code; and

generating, by the first Bluetooth device, the broadcast packet based on the first ciphertext further comprises:

including the code in a plaintext form in the broadcast packet.

9. The computer-implemented system according to claim 7, wherein generating, by the first Bluetooth device, the code comprises:

periodically generating by using a pre-determined algorithm, wherein the pre-determined algorithm is agreed upon jointly by the first and second Bluetooth devices; and

encrypting, by the first Bluetooth device, the code comprises encrypting the code generated in a current period.

10. The computer-implemented system according to claim 7, wherein encrypting, by the first Bluetooth device, the code to generate the first ciphertext comprises:

encrypting the code and a locally-stored key by using a first encryption algorithm to obtain the first ciphertext, wherein the first encryption algorithm is a unidirectional function, and wherein the locally-stored key and the first encryption algorithm are agreed upon jointly by the first and second Bluetooth devices.

11. The computer-implemented system according to claim 7, wherein sending the scanning response to the second Bluetooth device based on the random private address in the scanning request comprises:

encrypting the random private address in the scanning request and a locally-stored key by using a third encryption algorithm to obtain a second ciphertext, wherein the third encryption

algorithm is a unidirectional function, and the locally-stored key is agreed upon jointly by the first and second Bluetooth devices;

generating the scanning response by using the second ciphertext; and

sending the scanning response to the second Bluetooth device by using the random private address.

12. The computer-implemented system according to claim 9, wherein

generating, by the first Bluetooth device, the broadcast packet based on the first ciphertext further comprises:

not including the code in a plain text form in the broadcast packet; and

allowing the second Bluetooth device to validate the code using at least information of the current period and the pre-determined algorithm.

13. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising: generating, by a first Bluetooth device, a code; encrypting, by the first Bluetooth device, the code to generate a first ciphertext in response to detecting that a Bluetooth connection is disconnected; generating, by the first Bluetooth device, a broadcast packet based on the first ciphertext, and broadcasting the broadcast packet to one or more Bluetooth devices, wherein the one or more Bluetooth devices includes a second Bluetooth device external to the first Bluetooth device; receiving, by the first Bluetooth device, a scanning request from the second Bluetooth device, the scanning request including a random private address generated by the second Bluetooth device; verifying the scanning request from the second Bluetooth device based on the random private address; sending, by the first Bluetooth device and in response to verifying the scanning request, a scanning response to the second Bluetooth device based on the random private address in the scanning request; and establishing, by the first Bluetooth device, a Bluetooth connection with the second Bluetooth device in response to determining that a connection request from the second Bluetooth device is received by the first Bluetooth device in response to the scanning response; wherein verifying the scanning request from the second Bluetooth device based on the random private address occurs after receiving, by the first Bluetooth device, the scanning request from the second Bluetooth device, and before sending the scanning response to the second Bluetooth

device, and the verifying comprises: decrypting the random private address in the scanning request by using a second decryption algorithm based on the code and a locally-stored key, to obtain a decrypted fixed address; determining whether a pre-stored fixed address at the first Bluetooth device is the same as the decrypted fixed address, wherein the pre-stored fixed address at the first Bluetooth device, the locally-stored key, and the second decryption algorithm are agreed upon jointly by the first and second Bluetooth devices; and in response to determining that the pre-stored fixed address is the same as the decrypted fixed address, sending the scanning response to the second Bluetooth device.

14. The non-transitory, computer-readable medium according to claim 13, wherein generating, by the first Bluetooth device, the code comprises:

generating a random number to obtain the code; and

generating, by the first Bluetooth device, the broadcast packet based on the first ciphertext further comprises:

including the code in a plaintext form in the broadcast packet.

15. The non-transitory, computer-readable medium according to claim 13, wherein generating, by the first Bluetooth device, the code comprises:

periodically generating by using a pre-determined algorithm, wherein the pre-determined algorithm is agreed upon jointly by the first and second Bluetooth devices; and

encrypting, by the first Bluetooth device, the code comprises encrypting the code generated in a current period.

16. The non-transitory, computer-readable medium according to claim 13, wherein encrypting, by the first Bluetooth device, the code to generate the first ciphertext comprises:

encrypting the code and a locally-stored key by using a first encryption algorithm to obtain the first ciphertext, wherein the first encryption algorithm is a unidirectional function, and wherein the locally-stored key and the first encryption algorithm are agreed upon jointly by the first and second Bluetooth devices.

17. The non-transitory, computer-readable medium according to claim 13, wherein sending the scanning response to the second Bluetooth device based on the random private address in the scanning request comprises:

encrypting the random private address in the scanning request and a locally-stored key by using a third encryption algorithm to obtain a second ciphertext, wherein the third encryption algorithm is a unidirectional function, and the locally-stored key is agreed upon jointly by the first and second Bluetooth devices;

generating the scanning response by using the second ciphertext; and

sending the scanning response to the second Bluetooth device by using the random private address.