

WE CLAIM

1. A computer implemented method for authenticating a first device of a user to a second device, the method comprising:
 - receiving a ciphertext and a public key from a first device, wherein the ciphertext is created by:
 - preparing a first biometric template for the user using the first device;
 - packing the first biometric template with a plurality of packing values to create a packed biometric template; and,
 - encrypting the packed biometric template using homomorphic encryption to create a ciphertext;
 - obtaining, using one or more sensors of the second device, a second biometric measurement of the user;
 - computing an encrypted similarity metric using the ciphertext and the second biometric template;
 - computing an encrypted code using the encrypted similarity metric, a masking value, and homomorphic encryption via the public key, wherein the masking value is added to the similarity metric to create a masked similarity metric;
 - sending the encrypted code to the first device, wherein the first device decrypts the encrypted code using the public key;
 - receiving from the first device the masked similarity metric;
 - computing a comparison metric using the masked similarity metric and the masking value;
 - comparing the comparison metric to a threshold value; and,
 - providing access to a resource when the comparison metric is less than the threshold value.
2. The method of claim 1, wherein the first biometric template includes a first vector of biometric values.
3. The method of claim 2, wherein preparing a biometric template comprises:
 - using one or more sensors of the first device to obtain a first biometric measurement of the user; and

sending the first biometric measurement of the user to a neural network to compute the first vector of biometric values.

4. The method of claim 3, wherein the first biometric measurement is a picture of the user's face.
5. The method of claim 1, wherein the ciphertext is saved in a memory of the first device.
6. The method of claim 1, wherein the second biometric measurement is a picture of the user's face.
7. The method of claim 1, wherein the second biometric template includes a second vector of biometric values.
8. The method of claim 1, wherein the plurality of packing values comprises eight values.
9. The method of claim 1, wherein the ciphertext is sent to the second device over a communications network.
10. The method of claim 9, wherein the communications network is a Wi-Fi network or a Bluetooth enabled network.
11. A computer implemented method for authenticating a first device of a user to a second device, the method comprising:

receiving a ciphertext and a public key from a first device, wherein the ciphertext is created by encrypting a first biometric template using homomorphic encryption;

obtaining, using one or more sensors of the second device, a second biometric measurement of the user;

computing an encrypted similarity metric using the ciphertext and the second biometric template;

computing an encrypted code using the encrypted similarity metric, a first masking value, a second masking value, and homomorphic encryption via the public key, wherein the similarity metric is multiplied by the first masking value to create a first masked similarity metric and the second masking value is added to the first masked similarity metric to create a second masked similarity metric;

- sending the encrypted code to the first device, wherein the first device decrypts the encrypted code using the public key;
- receiving from the first device the second masked similarity metric;
- computing a comparison metric using the second masked similarity metric, the first masking value, and the second masking value;
- comparing the comparison metric to a threshold value; and,
- providing access to a resource when the comparison metric is less than the threshold value.
12. The method of claim 11, wherein the first biometric template includes a first vector of biometric values.
 13. The method of claim 12, wherein the first vector of biometric values is obtained using one or more sensors of the first device to obtain a first biometric measurement of the user, wherein the first biometric measurement of the user is sent to a neural network to compute the first vector of biometric values.
 14. The method of claim 13, wherein the first biometric measurement is a picture of the user's face.
 15. The method of claim 11, wherein the ciphertext is saved in a memory of the first device.
 16. The method of claim 11, wherein the second biometric measurement is a picture of the user's face.
 17. The method of claim 11, wherein the second biometric template includes a second vector of biometric values.
 18. The method of claim 11, wherein the ciphertext is sent to the second device over a communications network.
 19. The method of claim 18, wherein the communications network is a Wi-Fi network or a Bluetooth enabled network.
 20. The method of claim 19, wherein the first masking value is a 2000 bit number.

WE CLAIM

1. A computer implemented method for authenticating a first device of a user to a second device, the method comprising:
 - receiving a ciphertext and a public key of a public/private key pair from a first device, wherein the ciphertext is created by:
 - obtaining, using one or more sensors of the first device, a first biometric measurement of the user;
 - sending the first biometric measurement to a neural network to compute a first vector of biometric values to include in a first biometric template for the user;
 - adding, to the first biometric template, a plurality of packing values to create a packed biometric template; and
 - encrypting the packed biometric template using homomorphic encryption to create the ciphertext;
 - obtaining, using one or more sensors of the second device, a second biometric measurement of the user;
 - computing an encrypted similarity metric using a cosine similarity function to compare the ciphertext and a second biometric template including the second biometric measurement;
 - computing an encrypted code by adding a masking value to the encrypted similarity metric to create a masked similarity metric and encrypting the masked similarity metric using homomorphic encryption via the public key;
 - sending the encrypted code to the first device, wherein the first device decrypts the encrypted code using a private key of the public/private key pair resulting in a decrypted code;
 - receiving, from the first device, the decrypted code;
 - computing a comparison metric by subtracting the masking value from the decrypted code;
 - comparing the comparison metric to a threshold value; and
 - providing access to a resource when the comparison metric is less than the threshold value.
2. The method of claim 1, wherein the first biometric measurement is a picture of the user's face.

3. The method of claim 1, wherein the ciphertext is saved in a memory of the first device.
4. The method of claim 1, wherein the second biometric measurement is a picture of the user's face.
5. The method of claim 1, wherein the second biometric template includes a second vector of biometric values.
6. The method of claim 5, wherein preparing the second biometric template comprises:
 - sending the second biometric measurement of the user to a neural network to compute the second vector of biometric values.
7. The method of claim 1, wherein the plurality of packing values comprises eight values.
8. The method of claim 1, wherein the ciphertext is sent to the second device over a communications network.
9. The method of claim 8, wherein the communications network is a Wi-Fi network or a Bluetooth enabled network.
10. A computer implemented method for authenticating a first device of a user to a second device, the method comprising:
 - receiving a ciphertext and a public key of a public/private key pair from a first device, wherein the ciphertext is created by encrypting a first biometric template using homomorphic encryption;
 - obtaining, using one or more sensors of the second device, a second biometric measurement of the user;
 - computing an encrypted similarity metric using a cosine similarity function to compare the ciphertext and a second biometric template including the second biometric measurement;

computing an encrypted code by:

- multiplying the encrypted similarity metric by a first masking value to create a first masked similarity metric;
- adding a second masking value to the first masked similarity metric to create a second masked similarity metric; and
- encrypting the first and second masked similarity metrics using homomorphic encryption via the public key;

sending the encrypted code to the first device, wherein the first device decrypts the encrypted code using the private key of the public/private key pair resulting in a decrypted code;

receiving, from the first device, the decrypted code;

computing a comparison metric by subtracting the second masking value from the decrypted code to create a result and dividing the result by the first masking value;

comparing the comparison metric to a threshold value;

and,

providing access to a resource when the comparison metric is less than the threshold value.

11. The method of claim 10, wherein the first biometric template includes a first vector of biometric values.

12. The method of claim 11, wherein the first vector of biometric values is obtained using one or more sensors of the first device to obtain a first biometric measurement of the user, wherein the first biometric measurement of the user is sent to a neural network to compute the first vector of biometric values.

13. The method of claim 12, wherein the first biometric measurement is a picture of the user's face.

14. The method of claim 10, wherein the ciphertext is saved in a memory of the first device.

15. The method of claim 10, wherein the second biometric measurement is a picture of the user's face.

16. The method of claim 10, wherein the second biometric template includes a second vector of biometric values.

17. The method of claim 10, wherein the ciphertext is sent to the second device over a communications network.

18. The method of claim 17, wherein the communications network is a Wi-Fi network or a Bluetooth enabled network.

19. The method of claim 18, wherein the first masking value is a 2000 bit number.