

WHAT IS CLAIMED IS:

1 1. A method of using biometric information to authenticate a first
2 electronic device of a user to a second electronic device, the method comprising performing,
3 by the first electronic device:

4 storing a first key share of a private key, wherein the second electronic device
5 stores a public key associated with the private key, and wherein one or more other electronic
6 devices of the user store other key shares of the private key;

7 storing a first template share of a biometric template of the user, wherein the
8 one or more other electronic devices of the user store other template shares of the biometric
9 template;

10 receiving a challenge message from the second electronic device;

11 measuring, by a biometric sensor of the first electronic device, a set of
12 biometric features of the user to obtain a measurement vector comprised of measured values
13 of the set of biometric features, and wherein the biometric template includes a template
14 vector comprised of measured values of the set of biometric features previously measured
15 from the user;

16 sending, by the first electronic device, the measurement vector measured by
17 the first electronic device, and the challenge message received from the second electronic
18 device, to the one or more other electronic devices;

19 receiving ~~at least T~~ a plurality of partial computations ~~signatures~~, including one
20 or more partial ~~computations~~ signatures from the one or more other electronic devices,
21 wherein each of the ~~at least T~~ plurality of partial computations ~~signatures~~ are is generated
22 using a respective template share, a respective key share, the measurement vector, and the
23 challenge message;

24 generating a signature of the challenge message using the ~~at least T~~ plurality
25 of partial computations ~~signatures~~; and

26 sending the signature to the second electronic device.

1 2. The method of claim 1, further comprising:

2 generating a first partial ~~computation~~ signature using the first template share,
3 the first key share, and the challenge message, and wherein the signature of the challenge
4 message is further generated using at least the first partial ~~computation~~ signature.

1 3. The method of claim 2, wherein the first partial computation signature
2 is one of the at least T plurality of partial computation signatures.

1 4. The method of claim 1, wherein each of the one or more other
2 electronic devices generate one of the ~~at least T~~ plurality of partial computations-signatures
3 using a respective template share, respective key share, and the challenge message.

1 5. The method of claim 1, wherein the first template share and the other
2 template shares are an encryption of the biometric template.

1 6. The method of claim 1, further comprising encrypting the
2 measurement vector.

1 7. The method of claim 1, further comprising performing a registration
2 process by:
3 measuring, by the biometric sensor of the first electronic device, the biometric
4 template of the user;
5 generating the public key, the private key, and the key shares of the private
6 key;
7 generating the first template share and the other template shares of the
8 biometric template;
9 deleting the private key and the biometric template; and
10 sending the public key to the second electronic device.

1 8. The method of claim 7, further comprising:
2 generating a cryptographic program that conditionally uses a set of keys shares
3 to generate the signature when the measurement vector is within a threshold of the template
4 vector.

1 9. The method of claim 8, wherein the cryptographic program includes a
2 garbled circuit.

1 10. The method of claim 8, wherein the cryptographic program uses
2 additively homomorphic encryption.

1 11. The method of claim 8, wherein the measurement vector and the
2 template vector are encrypted using threshold fully homomorphic encryption, and wherein
3 the cryptographic program determines that the measurement vector is within the threshold of

the template vector by computing an inner product of the measurement vector and the template vector.

12. The method of claim 8, wherein the cryptographic program reconstructs the biometric template using the template shares.

13. The method of claim 1, wherein generating the signature of the challenge message using the ~~at least T~~ plurality of partial computations-signatures includes:
adding shares of additively homomorphic encryptions of partial distances between the template shares and the measurement vector to obtain a total distance;
comparing the total distance to a threshold; and
signing the challenge message using ~~partial signatures of the at least T~~ plurality of partial computations-signatures when the total distance is less than the threshold.

14. The method of claim 13, wherein the adding and comparing are performed using a garbled circuit.

15. The method of claim 14, wherein the garbled circuit outputs a string and wherein the string is used to decrypt, ~~the encrypted~~ partial signatures of the at least T plurality of partial computations-signatures.

16. The method of claim 14, wherein the garbled circuit outputs the partial signatures of the ~~at least T~~ plurality of partial computations-signatures.

17. The method of claim 13, wherein the shares of the additively homomorphic encryptions of the partial distances have been partially decrypted by the one or more other electronic devices.

18. The method of claim 13, wherein the partial distances are determined using a cosine similarity or a Hamming distance measure.

19. The method of claim 13, further comprising:
generating a zero knowledge proof that verifies the comparison of the total distance to the threshold; and
sending the zero knowledge proof to the one or more other electronic devices for verification.

1 20. The method of claim 1, further comprising:
2 generating a zero knowledge proof that verifies the ~~at least T~~ plurality of
3 ~~partial computations~~ signatures; and
4 sending the zero knowledge proof to the one or more other electronic devices
5 for verification.

1 21. A computer product comprising a computer readable medium storing a
2 plurality of instructions for controlling a computer system to perform the method of any one
3 of the preceding claims.

1 22. A system comprising:
2 the computer product of claim 21; and
3 one or more processors for executing instructions stored on the computer
4 readable medium.

1 23. A system comprising means for performing any of the above methods.

1 24. A system comprising one or more processors configured to perform
2 any of the above methods.

1 25. A system comprising modules that respectively perform the steps of
2 any of the above methods.