

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:
 - during an enrollment process using an authentication application on a mobile device:
 - initiating the enrollment process for enrolling a user in an authentication program;
 - capturing a biometric enrollment sample of the user using the mobile device;
 - generating a biometric enrollment template using the biometric enrollment sample of the user;
 - storing the biometric enrollment template locally or at an authentication computer;
 - during an authentication process using a resource provider application on the mobile device:
 - obtaining a biometric authentication sample captured by the mobile device;
 - generating a biometric authentication template of a user from the biometric authentication sample;
 - obtaining biometric matching information related to the biometric authentication template, wherein the biometric matching information comprises the biometric enrollment template;
 - authenticating a user of the mobile device based on the biometric authentication template, the biometric matching information, and a cryptographic comparison protocol, wherein the cryptographic comparison protocol includes one or more of: secure multi-party computation, homomorphic encryption, or a fuzzy extractor, the fuzzy extractor being configured to i) generate a first cryptographic key from the biometric authentication template and a first function and a second cryptographic key from the biometric enrollment template and a second function and ii) use the first and second cryptographic keys to authenticate the user, wherein the cryptographic comparison protocol is configured to compare the first cryptographic key representing the biometric authentication template to the second cryptographic key representing the biometric enrollment template without retrieving the biometric enrollment sample of the user; and

executing at least one operation in response to the user being authenticated.

2. The computer-implemented method of claim 1, further comprising:
initiating, by the resource provider application of the mobile device, the authentication process for authenticating the user of the mobile device;
sending, by the resource provider application, a user identifier to an authentication gateway computer;
receiving, by the resource provider application, user enrollment information from the authentication gateway computer, the user enrollment information comprising an indication of enrollment and one or more identifiers managed by the authentication computer.

3. The computer-implemented method of claim 2, wherein the biometric matching information comprises an obfuscated matching circuit configured to provide an output from which a match between two biometric templates is identifiable.

4. The computer-implemented method of claim 2, comprising:
generating, by the authentication application, the biometric matching information comprising the biometric enrollment template of the user from the biometric enrollment sample obtained by the mobile device during the enrollment process;
associating, by the authentication application, the biometric enrollment template of the user to at least one of: the user identifier or an identifier of the one or more identifiers managed by the authentication computer; and
storing, by the authentication application, the biometric enrollment template.

5. The computer-implemented method of claim 1, wherein the at least one operation comprises delivering access to a resource provided by a resource provider based on the user being authenticated.

6. A user device comprising:
one or more biometric capture devices;
one or more processors; and
one or more memories storing an authentication application, a resource provider application, and computer-executable instructions, wherein executing the

computer-executable instructions by the one or more processors causes the user device to:

 during an enrollment process using the authentication application:

 initiate the enrollment process for enrolling a user in an authentication program;

 capture biometric enrollment sample of the user using the user device;

 generate a biometric enrollment template using the biometric enrollment sample of the user;

 store the biometric enrollment template locally or at an authentication computer;

 during an authentication process using the resource provider application:

 obtain a biometric authentication sample captured by the user device;

 generate a biometric authentication template of a user from the biometric authentication sample;

 obtain biometric matching information related to the biometric authentication template, wherein the biometric matching information comprises the biometric enrollment template;

 authenticate a user of the user device based on the biometric authentication template, the biometric matching information, and a cryptographic comparison protocol, wherein the cryptographic comparison protocol includes one or more of: secure multi-party computation, homomorphic encryption, or a fuzzy extractor, the fuzzy extractor being configured to i) generate a first cryptographic key from the biometric authentication template and a first function and a second cryptographic key from the biometric enrollment template and a second function and ii) use the first and second cryptographic keys to authenticate the user, wherein the cryptographic comparison protocol is configured to compare the first cryptographic key representing the biometric authentication template to the second cryptographic key representing the biometric enrollment template without retrieving the biometric enrollment sample of the user; and

 execute at least one operation in response to the user being authenticated.

7. The user device of claim 6, wherein the one or more processors further cause the user device to:

- initiate, by the resource provider application, the authentication process for authenticating the user of the user device;
- send, by the resource provider application, a user identifier to an authentication gateway computer; and
- receive, by the resource provider application, user enrollment information from the authentication gateway computer, the user enrollment information comprising an indication of enrollment and one or more identifiers managed by the authentication computer.

8. The user device of claim 7, wherein the biometric matching information comprises an obfuscated matching circuit configured to provide an output from which a match between two biometric templates is identifiable.

9. The user device of claim 7, wherein the one or more processors further cause the user device to perform an enrollment process, the enrollment process comprising:

- generating, by the authentication application, the biometric matching information comprising the biometric enrollment template of the user from the biometric enrollment sample obtained by the user device during the enrollment process;

- associating, by the authentication application, the biometric enrollment template of the user to at least one of: the user identifier or an identifier of the one or more identifiers managed by the authentication computer; and

- storing, by the authentication application, the biometric enrollment template.

10. The user device of claim 6, wherein the at least one operation comprises delivering access to a resource provided by a resource provider based on the user being authenticated.