**WHAT IS CLAIMED IS:**

1. A method comprising:

obtaining, by an access device, a first biometric sample of a user;

generating a first biometric template from the first biometric sample;

for each mobile device of a plurality of mobile devices within a proximate vicinity of the access device, the plurality of mobile devices comprising a first mobile device:

retrieving a public value of the mobile device, wherein:

the public value of the mobile device was generated by passing a biometric template of the mobile device to a first function of a fuzzy extractor; and

the biometric template of the mobile device was generated from a biometric sample of the mobile device;

generating a secret cryptographic key by passing the first biometric template and the public value of the mobile device to a second function of the fuzzy extractor;

encrypting the first biometric template with the secret cryptographic key; and

broadcasting the encrypted first biometric template to the plurality of mobile devices;

receiving, from the first mobile device, a confirmation of a match between the first biometric template and a biometric template of the first mobile device, wherein the biometric template of the first mobile device is generated from a biometric sample of the first mobile device; and

responsive to the confirmation, conducting a transaction between the access device and the first mobile device.

2. The method of claim 1:

wherein generating the first biometric template from the first biometric sample comprises generating a first small biometric template and a first large biometric template;

~~wherein the public value of the mobile device that was generated by passing the biometric template of the mobile device to the first function of the fuzzy extractor was generated by passing a small biometric template of the mobile device to the first function of the fuzzy extractor;~~

~~wherein the small biometric template of the mobile device was generated from the biometric sample of the mobile device;~~

~~wherein generating the secret cryptographic key by passing the first biometric template and the public value of the mobile device to the second function of the fuzzy extractor comprises generating the secret cryptographic key by passing the first small biometric template and the public value of the mobile device to the second function of the fuzzy extractor;~~

~~wherein encrypting the first biometric template with the secret cryptographic key comprises encrypting the first large biometric template with the secret cryptographic key;~~

~~wherein broadcasting the encrypted first biometric template to the plurality of mobile devices comprises broadcasting the encrypted first large biometric template to the plurality of mobile devices;~~

~~wherein the match is between the first large biometric template and a large biometric template of the first mobile device; and~~

~~wherein the large biometric template of the first mobile device is generated from the biometric sample of the first mobile device.~~

~~3. The method of claim 2, wherein the first small biometric template is one of:~~

~~an obfuscated copy of the first large biometric template; and~~

~~an incomplete copy of the first large biometric template.~~

~~4. The method of claim 2, wherein generating the first large biometric template from the first biometric sample comprises:~~

~~extracting one or more distinct characteristics from the first biometric sample; and~~

~~generating digital reference of the one or more distinct characteristics.~~

~~5. The method of claim 2, wherein subsequent to receiving the encrypted first large biometric template from the access device, the first mobile device:~~

~~attempts to decrypt the encrypted first large biometric template with a secret cryptographic key of the first mobile device, wherein the secret cryptographic key of the first mobile device was generated by passing a small biometric template of the first mobile device to the first function of the fuzzy extractor, wherein the small biometric template of the first mobile device was generated from the biometric sample of the first mobile device;~~

~~responsive to decrypting the encrypted first large biometric template, determines whether the first large biometric template matches the large biometric template of the first mobile device; and~~

~~responsive to determining that the first large biometric template matches the large biometric template of the first mobile device, sends the confirmation of the match to the access device.~~

~~6. The method of claim 5:~~

~~wherein the plurality of mobile devices comprises a second mobile device; and~~

~~wherein subsequent to receiving the encrypted first large biometric template from the access device, the second mobile device attempts unsuccessfully to decrypt the encrypted first large biometric template with a secret cryptographic key of the second mobile device;~~

~~wherein the secret cryptographic key of the second mobile device was generated by passing a small biometric template of the second mobile device to the first function of the fuzzy extractor; and~~

~~wherein the small biometric template of the second mobile device was generated from a biometric sample of a different user.~~

~~7. The method of claim 5, wherein a similarity between the first small biometric template and the small biometric template of the first mobile device exceeds a threshold matching score.~~

8. The method of claim 2, wherein prior to obtaining the first biometric sample of the user, the method further comprises:

broadcasting a transmitting station identifier to each of the plurality of mobile devices; and

for each of the plurality of mobile devices:

receiving from the mobile device, the public value of the mobile device and storing the public value of the mobile device.

9. The method of claim 2 wherein obtaining the first biometric sample of the user comprises one of:

taking a photographic image of the user's face;

taking a fingerprint of the user;

taking a voice sample of the user;

taking a DNA sample of the user;

taking a retinal scan of the user; and

taking a hair sample of the user.

10. An access device comprising:

a processor; and

a computer readable medium comprising code, executable by the processor, for implementing a method comprising:

obtaining a first biometric sample of a user;

generating a first biometric template from the first biometric sample;

for each mobile device of a plurality of mobile devices within a proximate vicinity of the access device, the plurality of mobile devices comprising a first mobile device:

retrieving a public value of the mobile device, wherein:

the public value of the mobile device was generated by passing a biometric template of the mobile device to a first function of a fuzzy extractor; and

the biometric template of the mobile device was generated from a biometric sample of the mobile device;

generating a secret cryptographic key by passing the first biometric template and the public value of the mobile device to a second function of the fuzzy extractor;

encrypting the first biometric template with the secret cryptographic key; and

broadcasting the encrypted first biometric template to the plurality of mobile devices;

receiving, from the first mobile device, a confirmation of a match between the first biometric template and a biometric template of the first mobile device, wherein the biometric template of the first mobile device is generated from a biometric sample of the first mobile device; and

responsive to the confirmation, conducting a transaction between the access device and the first mobile device.

11. The access device of claim 10,

wherein generating the first biometric template from the first biometric sample comprises generating a first small biometric template and a first large biometric template;

wherein the public value of the mobile device that was generated by passing the biometric template of the mobile device to the first function of the fuzzy extractor was generated by passing a small biometric template of the mobile device to the first function of the fuzzy extractor;

wherein the small biometric template of the mobile device was generated from the biometric sample of the mobile device;

wherein generating the secret cryptographic key by passing the first biometric template and the public value of the mobile device to the second function of the fuzzy extractor comprises generating the secret cryptographic key by passing the first small biometric template and the public value of the mobile device to the second function of the fuzzy extractor;

~~wherein encrypting the first biometric template with the secret cryptographic key comprises encrypting the first large biometric template with the secret cryptographic key;~~

~~wherein broadcasting the encrypted first biometric template to the plurality of mobile devices comprises broadcasting the encrypted first large biometric template to the plurality of mobile devices;~~

~~wherein the match is between the first large biometric template and a large biometric template of the first mobile device; and~~

~~wherein the large biometric template of the first mobile device is generated from the biometric sample of the first mobile device.~~

~~12. The access device of claim 11, wherein the first small biometric template is one of:~~

~~an obfuscated copy of the first large biometric template; and~~

~~an incomplete copy of the first large biometric template.~~

~~13. The access device of claim 11, wherein generating the first large biometric template from the first biometric sample comprises:~~

~~extracting one or more distinct characteristics from the first biometric sample; and~~

~~generating digital reference of the one or more distinct characteristics.~~

~~14. The access device of claim 11, wherein subsequent to receiving the encrypted first large biometric template from the access device, the first mobile device:~~

~~attempts to decrypt the encrypted first large biometric template with a secret cryptographic key of the first mobile device, wherein the secret cryptographic key of the first mobile device was generated by passing a small biometric template of the first mobile device to the first function of the fuzzy extractor, wherein the small biometric template of the first mobile device was generated from the biometric sample of the first mobile device;~~

~~responsive to decrypting the encrypted first large biometric template, determines whether the first large biometric template matches the large biometric template of the first mobile device; and~~

responsive to determining that the first large biometric template matches the large biometric template of the first mobile device, sends the confirmation of the match to the access device.

15. The access device of claim 14:

wherein the plurality of mobile devices comprises a second mobile device; and

wherein subsequent to receiving the encrypted first large biometric template from the access device, the second mobile device attempts unsuccessfully to decrypt the encrypted first large biometric template with a secret cryptographic key of the second mobile device;

wherein the secret cryptographic key of the second mobile device was generated by passing a small biometric template of the second mobile device to the first function of the fuzzy extractor; and

wherein the small biometric template of the second mobile device was generated from a biometric sample of a different user.

16. The access device of claim 14, wherein a similarity between the first small biometric template and the small biometric template of the first mobile device exceeds a threshold matching score.

17. The access device of claim 11:

broadcasting a transmitting station identifier to each of the plurality of mobile devices; and

for each of the plurality of mobile devices:

receiving from the mobile device, the public value of the mobile device and storing the public value of the mobile device.

18. The access device of claim 11, wherein obtaining the first biometric sample of the user comprises one of:

taking a photographic image of the user's face;

taking a fingerprint of the user;

taking a voice sample of the user;

taking a DNA sample of the user;

taking a retinal scan of the user; and

taking a hair sample of the user.

19. A method comprising:

obtaining, by an access device, a first biometric sample of a user;

generating a first biometric template from the first biometric sample;

for each mobile device of a plurality of mobile devices within a proximate vicinity of the access device, the plurality of mobile devices comprising a first mobile device:

retrieving a public key of the mobile device;

encrypting the first biometric template with the public key of the mobile device; and

broadcasting the encrypted first biometric template to the plurality of mobile devices;

receiving, from the first mobile device, a confirmation of a match between the first biometric template and a biometric template of the first mobile device, wherein the biometric template of the mobile device is generated from a biometric sample of the first mobile device; and

reponsive to the confirmation, conducting a transaction between the access device and the first mobile device.

20. The method of claim 19, wherein prior to obtaining the first biometric sample of the user, the method further comprises:

broadcasting a transmitting station identifier to each of the plurality of mobile devices; and

for each of the plurality of mobile devices, receiving, from the mobile device, the public key of the mobile device and storing the public key of the mobile device

**WHAT IS CLAIMED IS:**

1. A method comprising:

obtaining, by an access device, a first biometric sample of a user;

generating a first biometric template from the first biometric sample;

for each mobile device of a plurality of mobile devices within a proximate vicinity of the access device, the plurality of mobile devices comprising a first mobile device:

retrieving a public value of the mobile device, wherein:

the public value of the mobile device was generated by passing a biometric template of the mobile device to a first function of a fuzzy extractor; and

the biometric template of the mobile device was generated from a biometric sample of the mobile device;

generating a secret cryptographic key by passing the first biometric template and the public value of the mobile device to a second function of the fuzzy extractor;

encrypting the first biometric template with the secret cryptographic key; and

broadcasting the encrypted first biometric template to the plurality of mobile devices;

receiving, from the first mobile device, a confirmation of a match between the first biometric template and a biometric template of the first mobile device, wherein the biometric template of the first mobile device is generated from a biometric sample of the first mobile device; and

responsive to the confirmation, conducting a transaction between the access device and the first mobile device.

2. The method of claim 1, wherein prior to obtaining the first biometric sample of the user, the method further comprises:

broadcasting a transmitting station identifier to each of the plurality of mobile devices; and

for each of the plurality of mobile devices:

receiving from the mobile device, the public value of the mobile device and storing the public value of the mobile device.

3. The method of claim 1, wherein obtaining the first biometric sample of the user comprises one of:

taking a photographic image of the user's face;

taking a fingerprint of the user;

taking a voice sample of the user;

taking a DNA sample of the user;

taking a retinal scan of the user; and

taking a hair sample of the user.

4. An access device comprising:

a processor;

and a computer readable medium comprising code, executable by the processor, for implementing a method comprising:

obtaining a first biometric sample of a user;
generating a first biometric template from the first biometric sample;
for each mobile device of a plurality of mobile devices within a proximate vicinity of the access device, the plurality of mobile devices comprising a first mobile device:
retrieving a public value of the mobile device, wherein:
the public value of the mobile device was generated by passing a biometric template of the mobile device to a first function of a fuzzy extractor; and
the biometric template of the mobile device was generated from a biometric sample of the mobile device;
generating a secret cryptographic key by passing the first biometric template and the public value of the mobile device to a second function of the fuzzy extractor;
encrypting the first biometric template with the secret cryptographic key; and
broadcasting the encrypted first biometric template to the plurality of mobile devices;
receiving, from the first mobile device, a confirmation of a match between the first biometric template and a biometric template of the first mobile device, wherein the biometric template of the first mobile device is generated from a biometric sample of the first mobile device; and
responsive to the confirmation, conducting a transaction between the access device and the first mobile device.

5. The access device of claim 4:
broadcasting a transmitting station identifier to each of the plurality of mobile devices; and
for each of the plurality of mobile devices:
receiving from the mobile device, the public value of the mobile device and storing the public value of the mobile device.

6. The access device of claim 4, wherein obtaining the first biometric sample of the user comprises one of:
taking a photographic image of the user's face;
taking a fingerprint of the user;
taking a voice sample of the user;
taking a DNA sample of the user;
taking a retinal scan of the user; and
taking a hair sample of the user.

7. A method comprising:
obtaining, by an access device, a first biometric sample of a user;
generating a first biometric template from the first biometric sample;
for each mobile device of a plurality of mobile devices within a proximate vicinity of the access device, the plurality of mobile devices comprising a first mobile device:
retrieving a public key of the mobile device;
encrypting the first biometric template with the public key of the mobile device; and

broadcasting the encrypted first biometric template to the plurality of mobile devices;

receiving, from the first mobile device, a confirmation of a match between the first biometric template and a biometric template of the first mobile device, wherein the biometric template of the mobile device is generated from a biometric sample of the first mobile device; and

responsive to the confirmation, conducting a transaction between the access device and the first mobile device.

8. The method of claim 7, wherein prior to obtaining the first biometric sample of the user, the method further comprises:

broadcasting a transmitting station identifier to each of the plurality of mobile devices; and

for each of the plurality of mobile devices, receiving, from the mobile device, the public key of the mobile device and storing the public key of the mobile device.

9. The method of claim 7, wherein obtaining the first biometric sample of the user comprises one of:

taking a photographic image of the user's face;
taking a fingerprint of the user;
taking a voice sample of the user;
taking a DNA sample of the user;
taking a retinal scan of the user; and
taking a hair sample of the user.

10. The method of claim 7, wherein the access device is a point of sale terminal.

11. The method of claim 7, wherein the transaction is a payment transaction.

12. The method of claim 7, further comprising:

receiving public values of a plurality of mobile devices within a proximity vicinity of an access device, and storing the public values of the plurality of mobile devices.

13. The method of claim 1, further comprising:

receiving public values of a plurality of mobile devices within a proximity vicinity of an access device, and storing the public values of the plurality of mobile devices.

14. The method of claim 1, wherein the access device is a point of sale terminal.

15. The method of claim 1, wherein the transaction is a payment transaction.

16. The method of claim 1, wherein the plurality of mobile devices and the access device communicate via Bluetooth.