WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, with at least one processor, first password data associated with a first password, first biometric input data associated with a first biometric input, and first secret key data associated with a first secret key;

generating, with at least one processor, a second secret key using the first secret key, the first password, and a password-to-random protocol;

generating, with at least one processor, fuzzy extractor helper data using the first biometric input and the second secret key;

storing, with at least one processor, the fuzzy extractor helper data and the first secret key

receiving, with at least one processor, one of attempted password data associated with an attempted password or second biometric input data associated with a second biometric input; and

obliviously generating, with at least one processor, a reconstructed second secret key using the first secret key and the attempted password in response to receiving the attempted password data or using the second biometric input and the fuzzy extractor helper data in response to receiving the second biometric input.

2. The method of claim 1, wherein receiving comprises receiving the password data and the first biometric input data from a user device and receiving the first secret key data from a server.

3. The method of claim 2, wherein the user device comprises a trusted enrollment device and the server comprises an authentication server.

4. The method of claim 1, further comprising:

determining, with at least one processor, that the reconstructed second secret key matches the second secret key; and

authenticating, with at least one processor, a user based on determining the reconstructed second secret key matches the second secret key.

5. The method of claim 4, wherein generating the reconstructed second secret key comprises generating the reconstructed second secret key using device-enhanced password-authenticated key exchange (DE-PAKE).

6. The method of claim 1, wherein generating the reconstructed second secret key comprises generating the reconstructed second secret key using a fuzzy vault opener (FV_{OPEN}).

7. The method of claim 6, wherein using the FV_{OPEN} comprises:

extracting, with at least one processor, a plurality of second biometric data points from the second biometric input;

communicating, with at least one processor, the plurality of second biometric data points;

receiving, with at least one processor, a plurality of polynomial encodings, each respective polynomial encoding of the plurality of polynomial encodings based on a respective second biometric data point of the plurality of second biometric data points, wherein the fuzzy extractor helper data comprises the plurality of polynomial encodings; and

generating, with at least one processor, the reconstructed second secret key based on the plurality of polynomial encodings.

8. The method of claim 1, wherein generating the second secret key comprises generating the second secret key using device-enhanced password-authenticated key exchange (DE-PAKE).

9. The method of claim 1, wherein generating the fuzzy extractor helper data comprises generating the fuzzy extractor helper data using a fuzzy vault generator (FV_{GEN}).

10. The method of claim 9, wherein using the FV_{GEN} comprises:

extracting, with at least one processor, a plurality of first biometric data points from the first biometric input;

generating, with at least one processor, a plurality of random data points;

generating, with at least one processor, a polynomial encoding of each first biometric data point of the plurality of first biometric data points based on the second secret key;

generating, with at least one processor, a random encoding of each random data point of the plurality of random data points; and

combining, with at least one processor, the polynomial encoding of each first biometric data point of the plurality of first biometric data points and the random encoding of each random data point of the plurality of random data points into a set of encodings,

wherein the fuzzy extractor helper data comprises the set of encodings.

11. The method of claim 10, wherein using the FV_{GEN} further comprises:

combining, with at least one processor, the plurality of first biometric data points and the plurality of random data points to form a first set of data points;

generating, with at least one processor, a respective set of neighboring data points for each respective data point of the first set of data points based on a threshold distance; and

storing each respective set of neighboring data points as a tuple with each respective data point in the set of encodings.

12. The method of claim 10, wherein using the FV_{GEN} further comprises:

permuting, with at least one processor, the set of encodings before storing the fuzzy extractor helper data comprising the set of encodings.

13. A computer-implemented method, comprising:

receiving, with at least one processor, first biometric input data associated with a first biometric input and first secret key data associated with a first secret key;

extracting, with at least one processor, a plurality of first biometric data points from the first biometric input;

generating, with at least one processor, a plurality of random data points, wherein a superset of datapoints comprises the plurality of first biometric data points and the plurality of random data points;

generating, with at least one processor, a polynomial encoding of each first biometric data point of the plurality of first biometric data points using the first secret key, wherein generating the polynomial encoding of each first biometric data point comprises encoding the first secret key as coefficients of a polynomial and encoding each first biometric data point using the polynomial;

generating, with at least one processor, a random encoding of each random data point of the plurality of random data points, wherein the random encoding of each random data point is associated with a different datapoint from the superset of datapoints;

combining, with at least one processor, the polynomial encoding of each first biometric data point of the plurality of first biometric data points and the random encoding of each random data point of the plurality of random data points into a set of encodings; and

storing, with at least one processor, the set of encodings as fuzzy extractor helper data.

14. The method of claim 13, comprising:

receiving, with at least one processor, second biometric input data associated with a second biometric input;

extracting, with at least one processor, a plurality of second biometric data points from the second biometric input;

communicating, with at least one processor, the plurality of second biometric data points;

receiving, with at least one processor, a plurality of encodings, each respective encoding of the plurality of encodings based on a respective second biometric data point of the plurality of second biometric data points, wherein the set of encodings of the fuzzy extractor helper data comprises the plurality of encodings;

generating, with at least one processor, a reconstructed first secret key based on the plurality of polynomial encodings;

determining, with at least one processor, that the reconstructed first secret key matches the first secret key; and

authenticating, with at least one processor, a user based on determining the reconstructed first secret key matches the first secret key.

15. A system, comprising:

at least one processor; and

at least one non-transitory computer-readable medium comprising instructions to direct the at least one processor to:

receive first password data associated with a first password, first biometric input data associated with a first biometric input, and first secret key data associated with a first secret key;

generate a second secret key using the first secret key, the first password, and a password-to-random protocol;

generate fuzzy extractor helper data based on the first biometric input and the second secret key;

store the fuzzy extractor helper data and the first secret key;

receive one of attempted password data associated with an attempted password or second biometric input data associated with a second biometric input; and

obliviously generate a reconstructed second secret key using the first secret key and the attempted password in response to receiving the attempted password data or using the second biometric input and the fuzzy extractor helper data in response to receiving the second biometric input.

16. A system, comprising:

at least one processor; and

at least one non-transitory computer-readable medium comprising instructions to direct the at least one processor to:

receive first biometric input data associated with a first biometric input and first secret key data associated with a first secret key;

extract a plurality of first biometric data points from the first biometric input;

generate a plurality of random data points, wherein a superset of datapoints comprises the plurality of first biometric data points and the plurality of random data points;

generate a polynomial encoding of each first biometric data point of the plurality of first biometric data points using the first secret key, wherein generating the polynomial encoding of each first biometric data point comprises encoding the first secret key as coefficients of a polynomial and encoding each first biometric data point using the polynomial;

generate a random encoding of each random data point of the plurality of random data points, wherein the random encoding of each random data point is associated with a different datapoint from the superset of datapoints;

combine the polynomial encoding of each first biometric data point of the plurality of first biometric data points and the random encoding of each random data point of the plurality of random data points into a set of encodings; and

store the set of encodings as fuzzy extractor helper data.

17. A computer program product, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

receive first password data associated with a first password, first biometric input data associated with a first biometric input, and first secret key data associated with a first secret key;

generate a second secret key using the first secret key, the first password, and a password-to-random protocol;

generate fuzzy extractor helper data using the first biometric input and the second secret key;

store the fuzzy extractor helper data and the first secret key;

receive one of attempted password data associated with an attempted password or second biometric input data associated with a second biometric input; and

obliviously generate a reconstructed second secret key using the first secret key and the attempted password in response to receiving the attempted password data or using the second biometric input and the fuzzy extractor helper data in response to receiving the second biometric input.

18. A computer program product, the computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

receive first biometric input data associated with a first biometric input and first secret key data associated with a first secret key;

extract a plurality of first biometric data points from the first biometric input;

generate a plurality of random data points, wherein a superset of datapoints comprises the plurality of first biometric data points and the plurality of random data points;

generate a polynomial encoding of each first biometric data point of the plurality of first biometric data points using the first secret key, wherein generating the polynomial encoding of each first biometric data point comprises encoding the first secret key as coefficients of a polynomial and encoding each first biometric data point using the polynomial;

generate a random encoding of each random data point of the plurality of random data points, wherein the random encoding of each random data point is associated with a different datapoint from the superset of datapoints;

combine the polynomial encoding of each first biometric data point of the plurality of first biometric data points and the random encoding of each random data point of the plurality of random data points into a set of encodings; and

store the set of encodings as fuzzy extractor helper data.