WHAT IS CLAIMED IS:

1. A method of performing privacy-preserving unsupervised learning, the method comprising:

jointly computing, by at least a first computer and a second computer, a secure distance, by at least performing a privacy-preserving multiplication of a first data value of the first computer and a second data value of the second computer based on a 1-out-of-N oblivious transfer (OT) corresponding to a number N of shares, the privacy-preserving multiplication further comprising:

expressing, by the first computer, the first data value as a first vector having a number L of components, wherein a respective component, having an index i, comprises a respective decomposition coefficient of the first data value in a base equal to N; and

forming, by the second computer, a respective N-component vector having the index i of the respective decomposition coefficient and a second index;

receiving, by the first computer, an output vector of the 1-out-of-N OT, wherein a component, having an index i, of the output vector comprises a component of the respective N-component vector, the component having the index i and having the second index corresponding to the respective decomposition coefficient of the first data value in the base equal to N; and

privately assigning data to a respective cluster of a plurality of clusters based on the secure distance by:

based on the secure distance, jointly computing, by the first computer and the second computer, a distance between a respective position vector of a respective element of the data and a respective centroid of the respective cluster, wherein the respective position vector is shared among the first computer and the second computer.

2. The method of claim 1, wherein:

a first component of the respective N-component vector, having the second index equal to 0, comprises a respective pseudo-random number; and

a respective remaining component, having the second index equal to j, comprises the second data value multiplied by j and by N raised to a power of i, minus the first component of the respective N-component vector.

3. The method of claim 1, wherein privately assigning the data to the respective cluster of the plurality of clusters further comprises:

identifying, via a garbled circuit, a best match cluster of the plurality of clusters for a respective element of a plurality of elements of the data, wherein the best match cluster has a centroid with a minimum distance to the respective element; and

representing the best match cluster as a binary vector comprising a cluster flag for the respective element.

4. The method of claim 1, wherein performing the privacy-preserving unsupervised learning further comprises privately updating a centroid of a cluster by at least:

multiplying, for a respective element of a plurality of elements of the data and via a second OT and a third OT, a combined first share and second share of a cluster flag for the cluster and the respective element by a combined first share and second share of a position vector for the respective element, wherein:

the first share of the cluster flag and the first share of the position vector belong to the first computer; and

the second share of the cluster flag and the second share of the position vector belong to the second computer;

summing a product of the multiplying over the plurality of elements;

dividing the summed product by a sum over the plurality of elements of the combined first share and second share of the cluster flag; and

updating the centroid based on a result of the dividing.

5. The method of claim 4, wherein the first share and second share of the cluster flag are combined by exclusive OR.

6. The method of claim 1, wherein the privacy-preserving unsupervised learning comprises k-means clustering, the k-means clustering further comprising:

selecting a plurality of seed clusters;

jointly computing, based on the secure distance, ~~a~~ the distance between a respective position vector of ~~a~~ the respective element of the data and a respective centroid of a respective seed cluster~~, wherein the respective position vector is shared among the first computer and the second computer~~;

identifying a first cluster having a minimum distance to the respective position vector;

assigning the respective element to the first cluster; and

updating a first centroid of the first cluster based on an average of position vectors of elements of the data assigned to the first cluster, including the respective position vector.

7. The method of claim 1, wherein:

N equals 2 and the 1-out-of-N OT comprises 1-out-of-2 OT; or

N equals 4 and the 1-out-of-N OT comprises 1-out-of-4 OT.

8. The method of claim 1, wherein the secure distance comprises a secure Euclidean distance.

9. The method of claim 1, wherein:

the first computer initially has the first data value and receives a first output share value;

the second computer initially has the second data value and receives a second output share value; and

the first output share value and second output share value sum to a product of the first data value and the second data value.

10. The method of claim 1, further comprising obtaining, by the second computer, a second output vector of the 1-out-of-N OT, wherein a component, having an index i, of the second output vector comprises a component of the respective N-component vector, the component having the index i and having the second index 0.

11. A computing system comprising:

a first computer comprising a first processor;

a second computer comprising a second processor; and

one or more memories including instructions that, when executed with the first processor and/or the second processor, cause the computing system to perform a privacy-preserving unsupervised learning heuristic, comprising:

jointly computing a secure distance, by at least performing privacy-preserving multiplication of a first data value of the first computer and a second data value of the second computer based on a 1-out-of-N oblivious transfer (OT) corresponding to a number N of shares, the privacy-preserving multiplication further comprising:

expressing, by the first computer, the first data value as a first vector having a number L of components, wherein a respective component, having an index i, comprises a respective decomposition coefficient of the first data value in a base equal to N; and

forming, by the second computer, a respective N-component vector having the index i of the respective decomposition coefficient and a second index;

receiving, by the first computer, an output vector of the 1-out-of-N OT, wherein a component, having an index i, of the output vector comprises a component of the respective N-component vector, the component having the index i and having the second index corresponding to the respective decomposition coefficient of the first data value in the base equal to N; and

privately assigning data to a respective cluster of a plurality of clusters based on the secure distance by:

based on the secure distance, jointly computing, by the first computer and the second computer, a distance between a respective position vector of a respective element of the data and a respective centroid of the respective cluster, wherein the respective position vector is shared among the first computer and the second computer.

12. The computing system of claim 11, wherein:

a first component of the respective N-component vector, having the second index equal to 0, comprises a respective pseudo-random number; and

a respective remaining component, having the second index equal to j, comprises the second data value multiplied by j and by N raised to a power of i, minus the first component of the respective N-component vector.

13. The computing system of claim 11, wherein privately assigning the data to the respective cluster of the plurality of clusters further comprises:

identifying, via a garbled circuit, a best match cluster of the plurality of clusters for a respective element of a plurality of elements of the data, wherein the best match cluster has a centroid with a minimum distance to the respective element; and

representing the best match cluster as a binary vector comprising a cluster flag for the respective element.

14. The computing system of claim 11, wherein performing the privacy-preserving unsupervised learning heuristic further comprises privately updating a centroid of a cluster by at least:

multiplying, for a respective element of a plurality of elements of the data and via a second OT and a third OT, a combined first share and second share of a cluster flag for

the cluster and the respective element by a combined first share and second share of a position vector for the respective element, wherein:

the first share of the cluster flag and the first share of the position vector belong to the first computer; and

the second share of the cluster flag and the second share of the position vector belong to the second computer;

summing a product of the multiplying over the plurality of elements;

dividing the summed product by a sum over the plurality of elements of the combined first share and second share of the cluster flag; and

updating the centroid based on a result of the dividing.

15. The computing system of claim ~~11~~ 14, wherein the first share and second share of the cluster flag are combined by exclusive OR.

16. The computing system of claim 11, wherein performing the privacy-preserving unsupervised learning heuristic comprises k-means clustering, the k-means clustering further comprising:

selecting a plurality of seed clusters;

jointly computing, based on the secure distance, ~~a~~ the distance between a respective position vector of ~~a~~ the respective element of the data and a respective centroid of a respective seed cluster~~, wherein the respective position vector is shared among the first computer and the second computer~~;

identifying a first cluster having a minimum distance to the respective position vector;

assigning the respective element to the first cluster; and

updating a first centroid of the first cluster based on an average of position vectors of elements of the data assigned to the first cluster, including the respective position vector.

17. The computing system of claim 11, wherein:

N equals 2 and the 1-out-of-N OT comprises 1-out-of-2 OT; or

N equals 4 and the 1-out-of-N OT comprises 1-out-of-4 OT.

18. The computing system of claim 11, wherein the secure distance comprises a secure Euclidean distance.

19. The computing system of claim 11, wherein:

the first computer initially has the first data value and receives a first output share value;

the second computer initially has the second data value and receives a second output share value; and

the first output share value and second output share value sum to a product of the first data value and the second data value.

20. The computing system of claim 11, wherein performing the privacy-preserving unsupervised learning heuristic further comprises obtaining, by the second computer, a second output vector of the 1-out-of-N OT, wherein a component, having an index i, of the second output vector comprises a component of the respective N-component vector, the component having the index i and having the second index 0.