Claims

What is claimed is:

1. A method for collecting audience information of a group of users in an audience measurement, the method comprising:

each user dividing its private information into a private portion and a predetermined number of exchange portions;

each user transmitting each of its exchange portions to a respective user of the predetermined number of users selected from the group of users;

each user aggregating its private portion and exchange portions received from other users of the group of users, thereby producing randomized information; and

aggregating the randomized information of the group of users, thereby producing aggregated private information for the group of users.

2. The method of claim 1, further comprising

each user randomly dividing its private information into the private portion and the predetermined number of exchange portions.

3. The method of claim 1, further comprising

each user independently selecting the predetermined number of users from the group of users, and transmitting each of its exchange portions to the respective selected user.

4. The method of claim 1, further comprising

each user encrypting the predetermined number of exchange portions, and transmitting each of the encrypted exchange portions to the respective user selected from the group of users.

5. The method of claim 4,

wherein each user encrypts each of its exchange portions using a public key of the respective user selected to receive the respective encrypted exchange portion, said public key being of an additively homomorphic cryptosystem.

6. The method of claim 5, further comprising

each user receiving encrypted exchange portions from other users of the group of users, and decrypting the received encrypted exchange portions.

7. The method of claim 6, further comprising

each user consolidating the received encrypted exchange portions, and decrypting the consolidated encrypted exchange portions.

8. The method of claim 7, wherein

each user consolidating the received encrypted exchange portions by multiplying the received encrypted exchange portions, and decrypting the product of the received encrypted exchange portions.

9. The method of claim 6, further comprising

each user aggregating its private portion and the decrypted exchange portions, thereby producing the randomized information of the user.

10. The method of claim 1, further comprising

transmitting the aggregated private information for the group of users to an audience measurement server.

11. The method of claim 1, wherein

the predetermined number is less than the number of users in the group of users.

12. The method of claim 1, wherein the private information of each user comprises one or more pieces of information selected from the group consisting of:

a number of viewers;

demographic of viewers;

ratings;

audience movement across programs and applications;

audience engagement;

interaction of viewers.

13. The method of claim 1, wherein

the private information of each user is a number or is represented by a number, and

each user divides its private information by splitting the number into a plurality of sub-numbers, wherein a sum of the plurality of sub-numbers equals to the number.

14. The method of claim 13,

the aggregating by each user comprises summing its private portion and the exchange portions received from other users of the group of users; and

the aggregating of the randomized information comprises summing the randomized information of the group of users.

15. A user device for providing audience information in an audience measurement, the user device comprising:

a divider configured to divide its private information into a private portion and a predetermined number of exchange portions;

a transmitter configured to transmit each of its exchange portions to a respective user device of the predetermined number of user devices selected by the user device;

a receiver configured to receive exchange portions from other user devices of a group of user devices; and

an aggregator configured to aggregate its private portion and the exchange portions received from said other user devices, thereby producing randomized information of the user device.

16. The user device of claim 15, further comprising

an encryptor configured to encrypt its predetermined number of exchange portions.

17. The user device of claim 15, further comprising

a decryptor configured to decrypt the exchange portions received from said other user devices.

18. A device for collecting audience information of a group of users in an audience measurement, the device comprising

a receiver configured to receive randomized information from the group of users, said randomized information from each user representing an aggregation of parts of private information from a plurality of users; and

an aggregator configured to aggregate the received randomized information to produce aggregated private information for the group of users.

19. The device of claim 18, further comprising

a transmitter configured to transmit the aggregated private information to an audience measurement server.

Claims

What is claimed is:

1. A method for collecting audience information of a group of users user devices in an audience measurement, the method comprising:

each user device dividing a private information into a private portion and at least a first exchange portion and a second exchange portion, wherein the private information of each user device is a number or is represented by a number, and each user device divides its private information by splitting the number into a plurality of sub-numbers, wherein a sum of the plurality of sub-numbers equals to the number;

each user device transmitting the first exchange portion to a first user device and the second exchange portion to a second user device, the first user device and the second user device selected from the group of user devices;

each user device aggregating its private portion and exchange portions received from other user devices of the group of user devices, thereby producing randomized information, wherein the aggregating by each user device comprises summing its private portion and the exchange portions received from other user devices of the group of user devices; and

aggregating the randomized information from each user device of the group of user devices, thereby producing aggregated private information for the group of

user devices, wherein the aggregating of the randomized information comprises summing the randomized information of the group of user devices.

2. The method of claim 1, further comprising each user device randomly dividing its private information into the private portion and the predetermined number of exchange portions.

3. The method of claim 1, further comprising each user device independently selecting the predetermined number of user devices from the group of user devices, and transmitting each of its exchange portions to the respective selected user device.

4. The method of claim 1, further comprising each user device encrypting the predetermined number of exchange portions, and transmitting each of the encrypted exchange portions to the respective user device selected from the group of user devices.

5. The method of claim 4, wherein each user device encrypts each of its exchange portions using a public key of the respective user device selected to receive the respective encrypted exchange portion, said public key being of an additively homomorphic cryptosystem.

6. The method of claim 5, further comprising each user device receiving encrypted exchange portions from other user devices of the group of user devices, and decrypting the received encrypted exchange portions.

7. The method of claim 6, further comprising each user device consolidating the received encrypted exchange portions, and decrypting the consolidated encrypted exchange portions.

8. The method of claim 7, wherein each user device consolidating the received encrypted exchange portions by multiplying the received encrypted exchange portions, and decrypting the product of the received encrypted exchange portions.

9. The method of claim 6, further comprising each user device aggregating its private portion and the decrypted exchange portions, thereby producing the randomized information of the user device.

10. The method of claim 1, further comprising transmitting the aggregated private information for the group of user devices to an audience measurement server.

11. The method of claim 1, wherein the predetermined number is less than the number of user devices in the group of user devices.

12. The method of claim 1, wherein the private information of each user device comprises one or more pieces of information selected from the group consisting of: a number of viewers; demographic of viewers; ratings; audience movement across programs and applications; audience engagement; and interaction of viewers.

13. A user device for providing audience information in an audience measurement, the user device comprising:

a divider configured to divide its private information into a private portion and at least a first exchange portion and a second exchange portion, wherein the private information of each user device is a number or is represented by a number, and the user device divides its private information by splitting the number into a plurality of sub-numbers, wherein a sum of the plurality of sub-numbers equals to the number;

a transmitter configured to transmit the first exchange portion to a first user device and the second exchange portion to a second user device, the first user device and the second user device selected by the user device;

a receiver configured to receive exchange portions from other user devices of a group of user devices;

an aggregator configured to aggregate its private portion and the exchange portions received from said other user devices, wherein the aggregating by the user device comprises summing its private portion and the exchange portions received from other user devices of the group of user devices, thereby producing randomized information of the user device, and

wherein the transmitter is further configured to transmit the randomized information from the user device for aggregating the randomized information of the group of user devices thereby producing aggregated private information for the group of user devices, wherein the aggregating of the randomized information comprises summing the randomized information of the group of user devices.

14. The user device of claim 13, further comprising an encryptor configured to encrypt its predetermined number of exchange portions. ‘

15. The user device of claim 13, further comprising a decryptor configured to decrypt the exchange portions received from said other user devices.