(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 July 2013 (11.07.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/103640 A2

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US20 13/020023

(22) International Filing Date:
3 January 2013 (03.01 .2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/345,438 6 January 2012 (06.01 .2012) US

(71) Applicant: **ALCATEL LUCENT** [FR/FR]; 3, avenue Octave Greard, F-75007 Paris (FR).

(72) Inventors: **BROUSTIS, Loannis;** 163 Main Street, Apartment 3B, Millburn, NJ 07041 (US). **CAKULEV, Violeta;** 4 Haran Circle, Millburn, NJ 07041 (US). **SUNDARAM, Ganapathy, Subramanian;** 10 Hickory Hill Road, Hillsborough, NJ 08844 (US).

(74) Agents: **RALSTON, Andrew, R.** et al; Alcatel-Lucent USA INC., Attention: Docket Administrator - Room 3B-212F, 600-700 Mountain Avenue, Murray Hill, NJ 07974-0636 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind cf national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

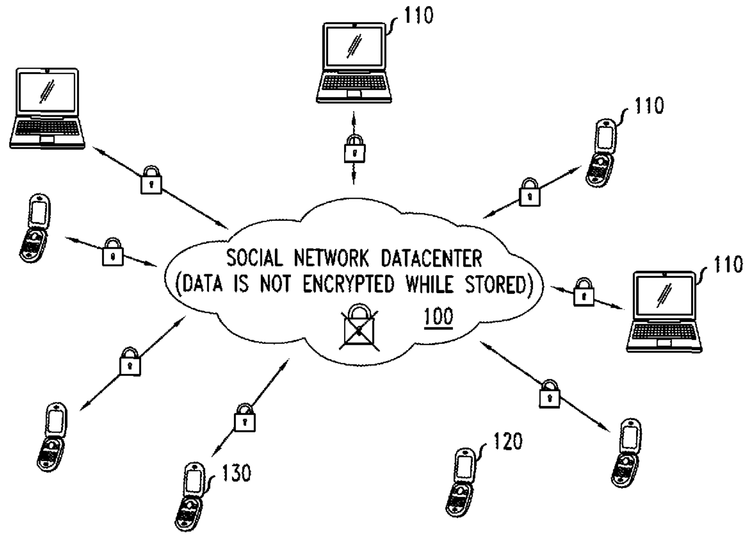
(84) **Designated States** *(unless otherwise indicated, for every kind cf regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt cf that report (Rule 48.2(g))*

(54) Title: METHODS AND APPARATUSES FOR MAINTAINING SECURE COMMUNICATION BETWEEN A GROUP OF USERS IN A SOCIAL NETWORK

FIG. 1


110
110
110
SOCIAL NETWORK DATACENTER
(DATA IS NOT ENCRYPTED WHILE STORED)
100
120
130

(57) Abstract: Embodiments address various methods and apparatuses that attempt to minimize the time that the security communication between group members may be at risk due to a user joining or leaving. For example, embodiments include methods of minimizing the time for which a joining member receives a secure commonly shared key and other embodiments include methods of minimizing the time that a user leaving the group has access to data shared within the group through updating the secure commonly shared key.

METHODS AND APPARATUSES FOR MAINTAINING SECURE COMMUNICATION BETWEEN A GROUP OF USERS IN A SOCIAL NETWORK

Cross-Reference

[0001] This application is related to U. S. Patent Application 13/345,241 filed January 6, 2012, titled Methods and Apparatuses for Secure Information Sharing in Social Networks Using Randomly-Generated Keys, by Ioannis Broustis, Violeta Cakulev, and Ganapathy Sundaram.

Field of the Invention

[0002] Embodiments of the present invention are directed to methods and apparatuses for maintaining secure communication between a group of users in a social network.

Background

[0003] This section introduces aspects that may be helpful in facilitating a better understanding of the invention. Accordingly, the statements of this section are to be read in this light and are not to be understood as admissions about what is in the prior art or what is not in the prior art.

[0004] During the last few years, social networking has become one of the main ways of communicating between people. Social networking and/or social networks are intended to be interpreted broadly and to be defined as a social structure made up of individuals (or organizations) called for example, "nodes", which can be tied (e.g., connected) by one or more specific types of

Claims

What is claimed is:

1. A method of maintaining security between a group of users in a social network, comprising:

identifying, by a social network host, a group of users, $U_1...U_m$ of the social network who securely communicate between each other using an initial commonly derived shared key that the social network host can not derive;

adding, by the social network host, at least one additional user U_{m+1} to the group of users of the social network, wherein the at least one additional user cannot derive the initial shared key; and

storing shared data Z¾ sent by one user in said group of users, the shared data being encrypted by an updated commonly derived shared key.

2. The method of claim 1, further comprising:

sending a temporary key to users $U_2...U_{m+i}$ prior to the updating the at least one published parameter step.

3. The method of claim 2, further comprising:

sending the temporary key to users $U_2...U_m$ using the initial commonly derived shared key.

4. The method of claim 1, further comprising:

sending the initial commonly derived shared key to user t/$_{m+1}$ prior to the at least updating parameter step.

5. A method of maintaining security between a group of users in a social network, comprising:

identifying a group of users, $\upsilon_1 ... \upsilon_m$ of the social network, by a social network host, who securely communicate between each other using a commonly derived shared key that the social network host can not derive;

removing a user $\boldsymbol{II}_i$ from the group of users who securely communicate between each other; and

updating at least one published parameter on which the updated commonly derived shared key is to be based, wherein the group of users minus the removed user can now securely communicate between each other without the removed user being able to derive the commonly shared key without the social network host being able to derive the commonly shared key.

6. The method of claim 5, wherein the at least one published parameter is either $\boldsymbol{X}_{i-1}$ or $\boldsymbol{X}_{i+l}$ corresponding to user U_{i-1} or $\boldsymbol{U}_{M\ /}$ respectively, and defined as $X_i = \alpha_i \{\alpha_{i+1}P - a_{i-1}P)$, where a_i is a secret random number and P is

7. A method of maintaining security between a group of users in a social network, comprising:

identifying a group of users, $U_1 .. U_m$ of the social network, by a social network host, who securely communicate between each other using a initial commonly derived shared key that the social network host can not derive;

adding at least one additional user U_{m+1},who can not derive the shared key, to the group of users of the social network, by the social network host;

switching users U_m and U_{m+l} upon the expiration of a timer, wherein user u_m did not update its X_m value by the end of the timer; and

updating at least the x_m value, now corresponding to the joining user on which an updated commonly derived shared key is to be based, wherein the group of users and the additional new user, except for switched user $U_{m\div l}$, can now securely communicate between each other using the updated commonly derived shared key based on the updated X_m value, without the social network host being able to derive the updated commonly shared key.

8. An apparatus comprising:

a memory; and

at least one processor coupled to the memory and configured to:

identify a group of users, $U_1 .. U_m$of the social network, by a social network host who securely, communicate between each other using an initial commonly derived shared key that the social network host can not derive;

add at least one additional user U_{m+1}who can not derive the shared key to the group of users of the social network, by the social network host; and

update at least one published parameter on which an updated commonly derived shared key is to be based, wherein the group of users and the additional user can now securely communicate between each other using the updated commonly derived shared key based on the updated at least one published parameter without the social network host being able to derive the updated commonly shared key.

9. An apparatus comprising:

a memory; and

at least one processor coupled to the memory and configured to:

identify a group of users, $U_1..U_m$ of the social network, by a social network host who securely, communicate between each other using a commonly derived shared key that the social network host can not derive;

remove a user U_i from the group of users who securely communicate between each other; and

update at least one published parameter on which an updated commonly derived shared key is to be based, wherein the group of users minus the removed user can now securely communicate between each other without the removed user being able to derive the updated commonly shared key and without the social network host being able to derive the updated commonly shared key.

10. A method of maintaining security between a first user and additional

users in a social network, comprising:

securely communicating between members of a first group of users that includes the first user and a first number of the additional users using an initial commonly shared key derived by the first user from parameters provided by the first number of additional users;

deriving an updated commonly derived shared key by the first user from parameters provided by a second different number of additional users; and

securely communicating between members of a second group of users that includes the first user and the second number of additional users.

11. The method of claim 10, further comprising the first user publishing at least one parameter from which the first user and the additional users derive the updated common derived shared key.

FIG. 1

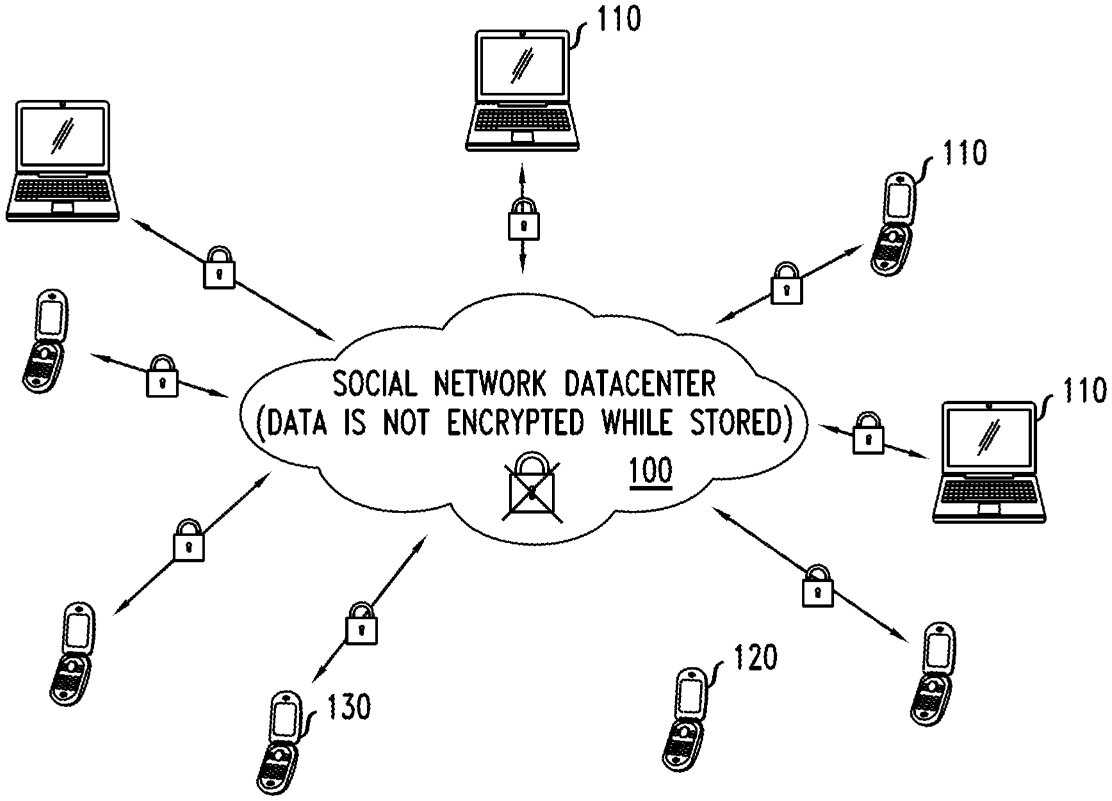

110
110
110
SOCIAL NETWORK DATACENTER
(DATA IS NOT ENCRYPTED WHILE STORED)
100
120
130

FIG. 2

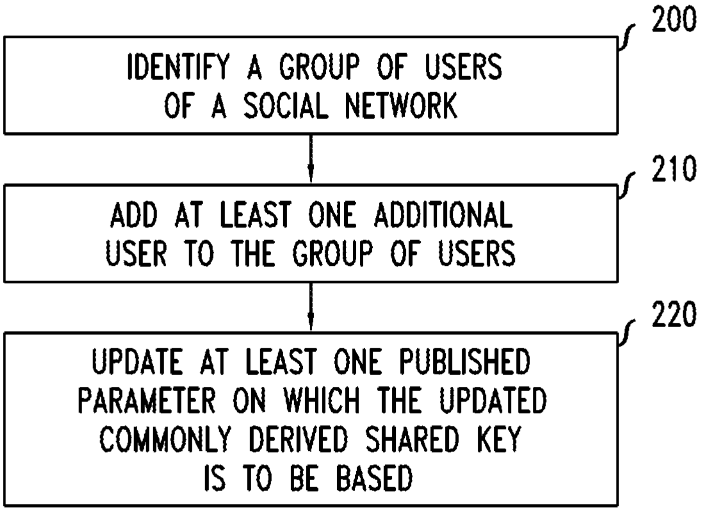

200
IDENTIFY A GROUP OF USERS OF A SOCIAL NETWORK
210
ADD AT LEAST ONE ADDITIONAL USER TO THE GROUP OF USERS
220
UPDATE AT LEAST ONE PUBLISHED PARAMETER ON WHICH THE UPDATED COMMONLY DERIVED SHARED KEY IS TO BE BASED

FIG. 3

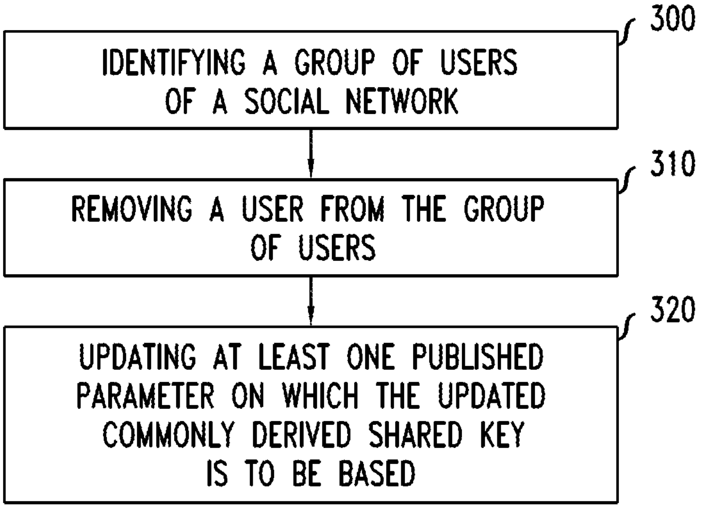
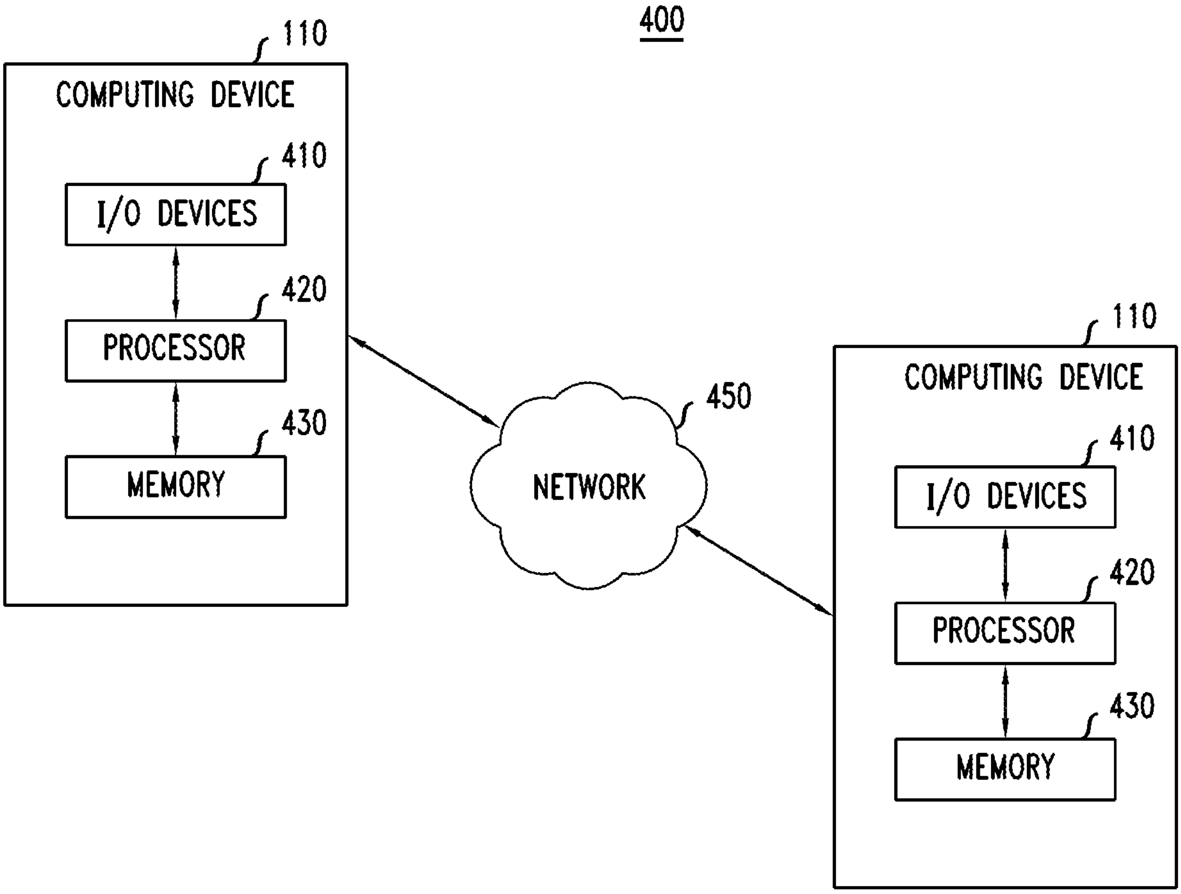

300
IDENTIFYING A GROUP OF USERS OF A SOCIAL NETWORK
310
REMOVING A USER FROM THE GROUP OF USERS
320
UPDATING AT LEAST ONE PUBLISHED PARAMETER ON WHICH THE UPDATED COMMONLY DERIVED SHARED KEY IS TO BE BASED

FIG. 4


400
110
COMPUTING DEVICE
410
I/O DEVICES
420
PROCESSOR
430
MEMORY
450
NETWORK
110
COMPUTING DEVICE
410
I/O DEVICES
420
PROCESSOR
430
MEMORY