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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 May 2017 (04.05.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/071770 Al

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/04* (2009.01)

(21) International Application Number:
PCT/EP20 15/075225

(22) International Filing Date:
30 October 2015 (30.10.201 5)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERIC¬SSON (PUBL)** [SE/SE]; Torshamnsgatan 21-23, SE-164 83 Stockholm (SE).

(72) Inventors: **ZHANG, Guoqiang;** Huvudstagatan 28, 1003, S-171 58 Solna (SE). **ARAÚJO, Jose;** Sandhamnsgatan 57A, 1307, S-1 15 28 Stockholm (SE). **ANDERSSON, Lars;** EdvinAdolphsons v. 9, S-169 40 Solna (SE).

(74) Agent: **ERICSSON;** Patent Development, Torshamn s-gatan 21-23, S-164 80 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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 of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, 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, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

WO 2017/071770 A1

(54) Title: ESTABLISHING A SECRET SHARED BETWEEN A FIRST COMMUNICATIONS DEVICE AND AT LEAST ONE SECOND COMMUNICATIONS DEVICE

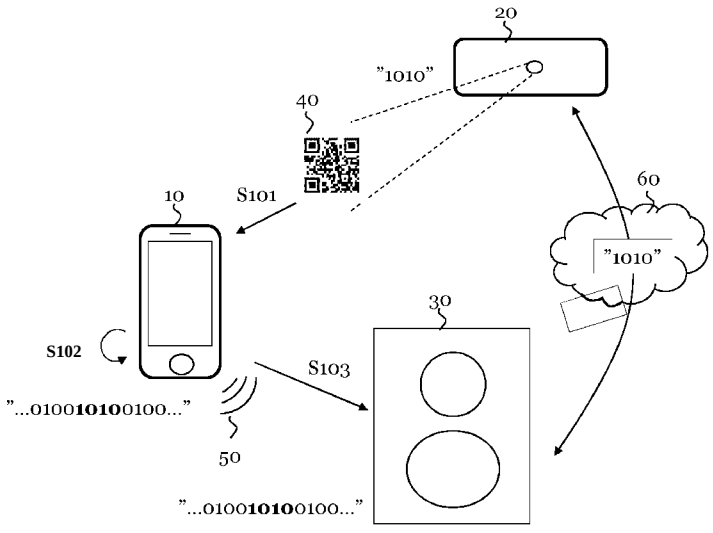

Figure l

(57) Abstract: A method performed by a computing device (10) of establishing a secret shared between a first communications device (20) and at least one second communications device (30) is provided. The method comprises acquiring (SlOl), using a first means of communication with the first communications device (20), a first data representation from which the shared secret can be derived. The method further comprises generating (S102) a second data representation from the first data representation, from which second data representation the shared secret can be derived. Moreover, the method comprises providing (SI 03), using a second means of communication, the second communications device (30) with the second data representation, the first means of communic - ation being different from the second means of communication.

ESTABLISHING A SECRET SHARED BETWEEN A FIRST COMMUNICATIONS DEVICE AND AT LEAST ONE SECOND COMMUNICATIONS DEVICE

TECHNICAL FIELD

The invention relates to methods of establishing a secret shared between a first communications device and at least one second communications device, and corresponding computing devices. The invention further relates to computer programs for causing computing devices to perform the methods according to the invention, and corresponding computer program products.

BACKGROUND

As regards electronic devices, from a client point-of-view, a user usually needs one desktop for work or leisure. When it comes to other electronic devices, a user may have a few devices, one for each particular application, such as gaming consoles, set-top boxes, smartphones and watches, tablets, network music players, etc.

Further, since the advent of Internet of Things (IoT), a user may have a great number of electronic devices in her home, commonly referred to as Machine-to-Machine (M2M) devices in the form of, e.g., temperature sensors, smart clothes, thermostat controllers, etc.

For instance, a user may wear a smart watch for health monitoring and a head-mounted device (HMD) for entertainment, and at the same time have a smartphone for communicating with the smart watch and the HMD.

As the number of electronic devices increases in daily life, device association, or pairing, will play an important role for data sharing among two or more devices. In many situations, a few electronic devices are required to be connected temporally to exchange information, such as sharing a bill in a restaurant, or sharing a PowerPoint file among the audience for a presentation.

Many different approaches exist for device association or pairing. For instance, a tablet lacking a subscriber identity module (SIM) card may, after having completed an authentication process, set up a local WiFi connection with a smartphone to use to the smartphone as a HotSpot for accessing the Internet.

As another example, the so called "Bump" application initiates pairing of two devices upon a user bumping the two devices together. Then, sensor data from motion and/or acceleration sensors is processed for associating the two devices. Further examples exist where visual tags, such as for instance Quick Response (QR) codes are used for associating many devices; a first device generates and displays a visual tag on its screen, and other devices may then scan the visual tag by using their cameras to join in a group communication. In a further example, US 7,907,901 discloses shaking of two devices, wherein if the two device are shaken in the same way they will generate identical motion data on the basis of which they subsequently can be paired.

A problem with the approaches utilized in these examples is that the same type of sensors and means of communication must be used among the devices; in the first example, the devices engage in radio communication, in the second and fourth example, orientation sensors are employed, while in the third example, the devices interact by means of visual communication.

SUMMARY

An object of the invention is to solve, or at least mitigate, this problem in the art, and to provide an improved method for facilitating establishment of a secret which is shared between communications devices.

This object is attained in a first aspect of the invention by a method performed by a computing device of establishing a secret shared between a first communications device and at least one second communications device. The method comprises acquiring, using a first means of communication with the first communications device, a first data representation from which the shared secret can be derived. The method further comprises generating a

second data representation from the first data representation, from which second data representation the shared secret can be derived. Moreover, the method comprises providing, using a second means of communication, the second communications device with the second data representation, the first means of communication being different from the second means of communication.

This object is attained in a second aspect of the invention by a computing device configured to establish a secret shared between a first communications device and at least one second communications device, which computing device comprises a processing unit and a memory, said memory containing instructions executable by said processing unit, whereby said computing device is operative to acquire, using a first means of communication with the first communications device, a first data representation from which the shared secret can be derived. The computing device is further operative to generate a second data representation from the first data representation, from which second data representation the shared secret can be derived. Moreover, the computing device is operative to provide, using a second means of communication, the second communications device with the second data representation, the first means of communication being different from the second means of communication.

This object is attained in a third aspect of the invention by a method performed by a computing device of establishing a secret shared between a first communications device and at least one second communications device. The method comprises acquiring sensor data from which the shared secret can be derived, the sensor data representing motion which both the computing device and the first communications device are subjected to. The method further comprises generating a second data representation from the sensor data, from which second representation the shared secret can be derived. Moreover, the method comprises providing the second communications device with the second data representation.

This object is attained in a fourth aspect of the invention by a computing device configured to establish a secret shared between a first communications device and at least one second communications device, which computing device comprises a processing unit and a memory, said memory containing instructions executable by said processing unit, and further a motion sensor, whereby said computing device is operative to acquire sensor data of the motion sensor from which the shared secret can be derived. The sensor data represents motion which both the computing device and the first communications device are subjected to. The computing device is further operative to generate a second data representation from the sensor data, from which second representation the shared secret can be derived. Moreover, the computing device is operative to provide the second communications device with the second data representation.

This object is attained in a fifth aspect of the invention by a computer program comprising computer-executable instructions for causing a device to perform steps according to an embodiment of the first and/or third aspect of the invention when the computer-executable instructions are executed on a processing unit included in the device.

This object is attained in a sixth aspect of the invention by a computer program product comprising a computer readable medium, the computer readable medium having the computer program according to the fifth aspect embodied thereon.

Advantageously, with a computing device acting as a relay or proxy for associating a group of devices with each, association of heterogeneous devices, i.e., devices utilizing different means of communication, is made possible.

For instance, in the first aspect of the invention, assuming that a first device in the form of a projector is to be paired/associated with a second device embodied by a conference phone; the projector is equipped with a light

source for projecting visual objects, while the conference phone is equipped with a microphone via which it is capable of receiving audio signals.

A user may thus have the projector display a visual tag, such as a Quick Response (QR) code or the like. This may be effected for instance by instructing the projector accordingly by pressing a dedicated button of a remote control associated with the projector, or by having the projector display the QR code upon power-on.

The user thus sets up communication between the projector and the relay device of the invention, being , e.g., a smartphone, using a first means of communication, in this exemplifying embodiment by having the smartphone read the QR code displayed by the projector onto a wall or projection screen, using the smartphone's camera. The read QR code constitutes a first data representation from which a secret shared by the projector and the smartphone can be derived, for instance in the form of a particular binary sequence.

Now, the user subsequently sets up communication between the conference phone and her smartphone via a second means of communication, in this example by transmitting an audio signal which is picked-up by a microphone of the conference phone, in order to provide the shared secret to the conference phone.

Prior to submitting the audio signal, the smartphone generates a second data representation from the acquired first data representation, from which second data representation the shared secret can be derived by the conference phone. Hence, in order to provide the conference phone with data from which the shared secret can be derived, the first data representation is coded into the audio signal which is transmitted to the conference phone. Thereby, the second data representation is generated from which the shared secret (in the form of the above mentioned binary sequence) can be derived by the conference phone.

Advantageously, the smartphone has enabled secure communication between the projector and the conference phone; when the two devices subsequently establish communication via for example Bluetooth, WiFi, or the Internet, etc, they both have access to the shared secret, i.e., the binary sequence used as an example hereinabove, and secure communication can be undertaken.

In the second aspect of the invention, assuming that a first device in the form of a tablet is to be paired/associated with a second device, again embodied by a conference phone; the tablet is equipped with a motion sensor such as an accelerometer, while the conference phone is equipped with a microphone via which it is capable of receiving audio signals.

The user initiates the pairing, e.g., by bumping her smartphone relay device against the tablet, or alternatively by shaking the smartphone together with the tablet. Either way, the motion sensor of the smartphone will produce sensor data from which the shared secret can be derived, the sensor data representing motion which both the smartphone and the tablet are subjected to. The shared secret may be represented by a particular binary sequence.

Similar to the exemplifying embodiment given for the first aspect of the invention, a second data representation from which the shared secret can be derived is generated by the smartphone and provided to the conference phone.

However, in the second aspect, the smartphone generates the second data representation from the acquired sensor data, from which second data representation the shared secret can be derived by the conference phone. Hence, in order to provide the conference phone with data from which the shared secret can be derived, at least a part of the sensor data is coded into the audio signal which is transmitted to the conference phone. Thereby, the second data representation is generated from which the shared secret (in the form of the above mentioned binary sequence) can be derived by the conference phone.

Advantageously, the smartphone has enabled secure communication between of the tablet and the conference phone; when the two devices subsequently establish communication via for example Bluetooth, WiFi, or the Internet, etc, they both have access to the shared secret, i.e. the binary sequence that was created upon bumping or shaking the tablet and the smartphone together, and secure communication can be undertaken.

In an embodiment of the invention, the motion sensor data represents physical contact with the first communications device. Hence, the computing device and the first communications device may advantageously be bumped together to initiate establishment of a shared secret.

In another embodiment of the invention, the motion sensor data represents a movement pattern common with the first communications device. Hence, the computing device and the first communications device may advantageously be shaken together to initiate establishment of a shared secret.

In a further embodiment of the invention, a secret shared between a first communications device and a group of second communications devices is established, in which case the group of second communications device is provided with the second data representation.

In still a further embedment of the invention, at least two of the second communication devices comprised in the group are provided with the second data representation via different means of communication. For instance, one of the second communications devices is provided with the second data representation visually while the other is provided with the second data representation audibly.

In still another embodiment of the invention, the computing device derives the shared secret from the first data representation or the motion sensor data, whichever is applicable, and establishes secure communication with the first communications device and/or the at least one second communications device using the derived shared secret.

In an embodiment, the acquiring of a first data representation from which the shared secret can be derived comprises one of: visually acquiring the first data representation, audibly acquiring the first data representation, and acquiring the first data representation over a wireless radio communication channel.

In another embodiment, the providing of a second data representation from which the shared secret can be derived comprises one of: visually providing the second data representation, audibly providing the second data representation, and providing the second data representation over a wireless radio communication channel.

Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is now described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 illustrates a computing device according to an embodiment of the invention, configured to establish a secret shared between a first communications device and at least one second communications device;

Figure 2 illustrates a flowchart of an embodiment of a method performed by the computing device of Figure 1, of establishing a secret shared between the first communications device and the second communications device;

Figure 3 illustrates a computing device according to another embodiment of the invention, configured to establish a secret shared between a first communications device and at least one second communications device;

Figure 4 illustrates a flowchart of an embodiment of a method performed by the computing device of Figure 3, of establishing a secret shared between the first communications device and the second communications device;

Figure 5 illustrates a computing device according to an embodiment of the invention;

Figure 6 illustrates a computing device according to another embodiment of the invention;

Figure 7 illustrates a computing device according to a further embodiment of the invention, configured to establish a secret shared between a first communications devices and a group of second communications devices;

Figure 8 illustrates a computing device according to an embodiment of the invention; and

Figure 9 illustrates a computing device according to another embodiment of the invention.

DETAILED DESCRIPTION

The invention will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout the description.

Figure 1 illustrates a computing device 10 according to an embodiment of the invention, configured to establish a secret shared between a first communications device 20 and at least one second communications device 30.

Figure 2 illustrates a flowchart of an embodiment of a method performed by the computing device 10 of Figure 1 of establishing a secret shared between the first communications device 20 and the second communications device 30.

The computing device 10 is embodied in the form of a smartphone in Figure 1, while the first communications device 20 is embodied in the form of a projector and the second communications device 30 in the form of a conference phone.

In order to establish a shared secret between the projector 20 and the conference phone 30 for enabling subsequent secure communication between the two devices, a user may have the projector display a visual tag, in this particular example a QR code 40.

The user will have the smartphone 10 read the QR code 40 by means of a camera in order to acquire a first data representation from which a shared secret can be derived. In the illustration of Figure 1, the first data representation comprises a binary sequence "...010010100100..." from which the shared secret may be derived. In this particular example, the shared secret is embodied by the 4-bit sequence "1010" interspersed into the first data representation.

In step S102, the mobile phone 10 generates a second data representation from the first data representation, from which second data representation the shared secret can be derived.

In this example, the second data representation is provided to the conference phone 30 from the smartphone 10 via an audio signal 50 picked-up by a microphone of the conference phone 30. Hence, in order to provide the conference phone with data from which the shared secret can be derived, the first data representation is coded into the audio signal 50 which is transmitted to the conference phone 30 in step S103. Thereby, the second data representation is generated from which the shared secret (in the form of the above mentioned 4-bit sequence) can be derived by the conference phone.

Advantageously, the smartphone 10 has enabled secure communication between the projector 20 and the conference phone 30, each communicating with the smartphone 10 by different means of communication. When the two devices subsequently establish communication via for example a local WiFi network 60, they both have access to the shared secret, i.e. the 4-bit sequence "1010", and secure communication can be undertaken.

It should be noted that the shared secret and the first and second data representation may have a different structure than that illustrated with reference to Figure 1. It should further be noted that establishment of secure communication between the projector 20 and the conference phone 30 may be effected via a device such as a server (not shown) before a secure communication channel can be setup between the two. Moreover, the first and second data representations are illustrated to comprise the 4-bit shared secret interspersed in a longer code. However, it can also be envisaged that the first and second data representation indeed comprises the shared secret only.

Figure 3 illustrates a computing device 10 according to a further embodiment of the invention configured to establish a secret shared between a first communications device 20 and at least one second communications device 30.

Figure 4 illustrates a flowchart of an embodiment of a method performed by the computing device 10 of Figure 3 of establishing a secret shared between the first communications device 20 and the second communications device 30.

Again, the computing device 10 is embodied in the form of a smartphone and the second communications device 30 in the form of a conference phone, while the first communications device 20 in this particular embodiment is embodied by a tablet.

In this embodiment, in order to establish a shared secret between the tablet 20 and the conference phone 30 for enabling subsequent secure

communication between the two devices, a user bumps her smartphone 10 against the tablet. A respective inertia measurement unit (IMU) in the smartphone 10 and the tablet 20 will register the motion that the two devices are subjected to. The IMU may be an accelerometer, a gyroscope, a magnetometers or a combination of two or more of these types of motion sensors.

From the motion that the smartphone 10 and the tablet 20 are subjected to, it is possible to conclude whether these exact two devices were bumped together, and a shared secret may thus be established. As previously was mentioned, the motion may be embodied by movement of the smartphone 10 and the tablet according to a common pattern, such as the user holding the two devices in the same hand and shaking them back and forth.

By shaking the two devices, the motion (i.e., accelerations) which the two devices are subjected to are used to generate a secret, such as a key, which key subsequently is used to establish the secure connection. Since the two devices are moved together, they have performed an identical motion, and thus captured substantially identical motion data. From the identical motion data, identical copies of the shared secret may be established.

The smartphone 10 hence acquires sensor data in step S201 from its IMU, from which data the shared secret can be derived. The acquired sensor data represents the bumping motion that the smartphone 10 and the tablet 20 was subjected to. In the illustration of Figure 3, the sensor data comprises a binary sequence "...010010100100..." from which the shared secret may be derived. In this particular example, the shared secret is embodied by the 4-bit sequence "1010" interspersed into the sensor data.

As in the embodiment previously described with reference to Figure 1, the smartphone 10 needs to generate a second data representation in a format that can be transmitted to, and interpreted by, the conference phone 30.

In step S202, the mobile phone 10 thus generates a second data representation from the sensor data, from which second data representation the shared secret can be derived.

Again, the second data representation is provided to the conference phone 30 from the smartphone 10 via an audio signal 50 picked-up by a microphone of the conference phone 30. Hence, in order to provide the conference phone with data from which the shared secret can be derived, the sensor data is coded into the audio signal 50 which is transmitted to the conference phone 30 in step S203. Thereby, the second data representation is generated from which the shared secret (in the form of the above mentioned 4-bit sequence) can be derived by the conference phone 30.

Advantageously, the smartphone 10 has enabled secure communication between the tablet 20 and the conference phone 30. When the tablet 20 and the conference phone 30 subsequently establish communication via the WiFi network 60, they both have access to the shared secret, i.e. the 4-bit sequence "1010", and secure communication can be undertaken.

With reference to Figures 5 and 6, the steps of the method performed by the computing device 10 according to embodiments of the invention are in practice performed by a processing unit 11 embodied in the form of one or more microprocessors arranged to execute a computer program 12 downloaded to a suitable storage medium 13 associated with the microprocessor, such as a Random Access Memory (RAM), a Flash memory or a hard disk drive. The processing unit 11 is arranged to cause the computing device 10 to carry out the method according to embodiments of the present invention when the appropriate computer program 12 comprising computer-executable instructions is downloaded to the storage medium 13 and executed by the processing unit 11. The storage medium 13 may also be a computer program product comprising the computer program 12. Alternatively, the computer program 12 may be transferred to the storage medium 13 by means of a suitable computer program product, such as a Digital Versatile Disc (DVD) or a memory stick. As a further alternative, the

computer program 12 may be downloaded to the storage medium 13 over a network. The processing unit 11 may alternatively be embodied in the form of a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field-programmable gate array (FPGA), a complex programmable logic device (CPLD), etc.

With reference to Figure 6, in case motion sensor data is acquired from which the shared secret can be derived, the computing device 10 is equipped with an IMU 14 as previously described. Advantageously, the computing device 10 is embodied by a smartphone, as a smartphone typically is provided with an IMU 14.

Figure 7 illustrates a computing device 10 according to a further embodiment of the invention, configured to establish a secret shared between tablet 20 and a group of second communications devices, in this exemplifying embodiment the conference phone 30 and a network music player 70 communicating via for instance infrared (IR) signals.

In order to establish a shared secret between the tablet 20 and the conference phone 30 and network music player 70 for enabling subsequent secure communication between the three devices, a user bumps the smartphone 10 against the tablet 20. A respective IMU in the smartphone 10 and the tablet 20 will register the motion that the two devices are subjected to, as was described with reference to Figure 3.

The smartphone 10 hence acquires sensor data in step S201 from its IMU, from which data the shared secret can be derived. The acquired sensor data represents the bumping motion that the smartphone 10 and the table 20 was subjected to. In the illustration of Figure 7, the sensor data comprises a binary sequence "...010010100100..." from which the shared secret may be derived. Again, the shared secret is embodied by the 4-bit sequence "1010" interspersed into the sensor data.

In step S202, the mobile phone 10 generates a second data representation from the sensor data, from which second data representation the shared

secret can be derived. In case the group of second communications devices had been communicating with the smartphone 10 via the same means of communication, the group of devices could have used the same second data representation.

However, in this exemplifying embodiment, the smartphone 10 needs to generate a second data representation in a format that can be transmitted to, and interpreted by, the conference phone 30 as well as by the network music player 70.

As previously has been described, the second data representation is provided to the conference phone 30 from the smartphone 10 via an audio signal 50 picked-up by a microphone of the conference phone 30. Hence, in order to provide the conference phone with data from which the shared secret can be derived, the sensor data is coded into the audio signal 50 which is transmitted to the conference phone 30 in step S203. Thereby, the second data representation is generated from which the shared secret (in the form of the above mentioned 4-bit sequence) can be derived by the conference phone 30.

Further, the second data representation is provided to the network music player 70 from the smartphone 10 via an IR signal 80 picked-up by an IR sensor of the music player 70. Hence, in order to provide the network music player with data from which the shared secret can be derived, the sensor data is coded into the IR signal 80 which is transmitted to the network music player 70 in step S203, using a suitable protocol. Thereby, the second data representation is generated from which the 4-bit shared secret can be derived by the network music player 70.

In this particular embodiment, the network music player 70 is provided with the second data representation via a third means of communication - in this case IR signals - different from the second means of communication (and the first means of communication), in this case being audio signals. It should be noted that it is envisaged that the means of communication used for

supplying the second data representation to the conference phone 30 and the network music player 70 may be the same.

Advantageously, the smartphone 10 has enabled secure communication between the tablet 20 and the conference phone 30 and the music player 70. When the tablet 20 subsequently establishes communication via the WiFi network 60 with the conference phone 30 and the network music player 70, they all have access to the shared secret, i.e. the 4-bit sequence "1010", and secure communication can be undertaken.

It should be noted that the first data representation/sensor data, and subsequently the second data representation, may include information such as identification number of a secure communication session to be established, the allowed duration of the session, geographic location, timestamp, maximum number of devices engaged in the communication, etc.

In a further embodiment of the invention, secure communication channel(s) may be set up between the computing device and the first communications device 20, and possibly with any one or more of the second communications device(s) 30, 70, and the computing device 10 may thus take part in establishing a communication session; the computing device 10 readily has access to the first data representation/sensor data from which the shared secret can be derived.

Figure 8 illustrates a computing device 10 according to a further embodiment of the invention, configured to establishing a secret shared between a first communications device and at least one second communications device. The computing device 10 comprises acquiring means 101 adapted to acquire, using a first means of communication with the first communications device, a first data representation from which the shared secret can be derived, generating means 102 adapted to generate a second data representation from the first data representation, from which second data representation the shared secret can be derived, and providing means 103 adapted to provide, using a second means of communication, the second communications device

with the second data representation, the first means of communication being different from the second means of communication.

The means 101-103 may comprise a communications interface for receiving and providing information, and further a local storage for storing data, and may (in analogy with the description given in connection to Figure 5) be implemented by a processor embodied in the form of one or more microprocessors arranged to execute a computer program downloaded to a suitable storage medium associated with the microprocessor, such as a RAM, a Flash memory or a hard disk drive.

Figure 9 illustrates a computing device 10 according to a further embodiment of the invention, configured to establishing a secret shared between a first communications device and at least one second communications device. The computing device 10 comprises acquiring means 201 adapted to acquire sensor data from which the shared secret can be derived, the sensor data representing motion which both the computing device and the first communications device are subjected to, generating means 202 adapted to generate a second data representation from the sensor data, from which second representation the shared secret can be derived, and providing means 203 adapted to provide the second communications device with the second data representation.

The means 201-203 may comprise a communications interface for receiving and providing information, and further a local storage for storing data, and may (in analogy with the description given in connection to Figure 6) be implemented by a processor embodied in the form of one or more microprocessors arranged to execute a computer program downloaded to a suitable storage medium associated with the microprocessor, such as a RAM, a Flash memory or a hard disk drive.

The disclosure has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the

art, other embodiments than the ones disclosed above are equally possible within the scope of the disclosure, as defined by the appended patent claims.

CLAIMS

1. A method performed by a computing device (10) of establishing a secret shared between a first communications device (20) and at least one second communications device (30), the method comprising:

acquiring (S101), using a first means of communication with the first communications device (20), a first data representation from which the shared secret can be derived;

generating (S102) a second data representation from the first data representation, from which second data representation the shared secret can be derived; and

providing (S103), using a second means of communication, the second communications device (30) with the second data representation, the first means of communication being different from the second means of communication.

2. A method performed by a computing device (10) of establishing a secret shared between a first communications device (20) and at least one second communications device (30), the method comprising:

acquiring (S201) sensor data from which the shared secret can be derived, the sensor data representing motion which both the computing device (10) and the first communications device (20) are subjected to;

generating (S202) a second data representation from the sensor data, from which second representation the shared secret can be derived; and

providing (S203) the second communications device (30) with the second data representation.

3. The method according to claim 2, wherein the sensor data represents physical contact with the first communications device (20).

4. The method according to claim 2, wherein the sensor data represents a movement pattern common with the first communications device (20).

5. The method according to any one of the preceding claims, wherein a secret shared between a first communications device (20) and a group of second communications devices (30, 70) is established, further comprising:

providing the group of second communications device (30, 70) with the second data representation.

6. The method according to claim 5, wherein at least one of the second communication devices (30, 70) comprised in said group are provided with the second data representation via a third means of communication being different from the second means of communication.

7. The method according to any one of the preceding claims, further comprising:

deriving the shared secret from the first data representation or the sensor data; and

establishing communication with the first communications device (20) and/or the at least one second communications device (30) using the derived shared secret.

8. The method according to claim 1, wherein the acquiring (S101) of a first data representation from which the shared secret can be derived comprises one of: visually acquiring the first data representation, audibly acquiring the first data representation, and acquiring the first data representation over a wireless communication channel.

9. The method according to any one of the preceding claims, wherein the providing (S103, S203) of a second data representation from which the shared secret can be derived comprises one of: visually providing the second data representation, audibly providing the second data representation, and providing the second data representation over a wireless radio communication channel.

10. A computer program (12) comprising computer-executable instructions for causing a device (10) to perform steps recited in any one of claims 1-9

when the computer-executable instructions are executed on a processing unit (11) included in the device.

11. A computer program product comprising a computer readable medium (13), the computer readable medium having the computer program (12) according to claim 10 embodied thereon.

12. A computing device (10) configured to establish a secret shared between a first communications device (20) and at least one second communications device (30), which computing device (10) comprises a processing unit (11) and a memory (13), said memory containing instructions (12) executable by said processing unit, whereby said computing device (10) is operative to:

acquire, using a first means of communication with the first communications device (20), a first data representation from which the shared secret can be derived;

generate a second data representation from the first data representation, from which second data representation the shared secret can be derived; and

provide, using a second means of communication, the second communications device (30) with the second data representation, the first means of communication being different from the second means of communication.

13. A computing device (10) configured to establish a secret shared between a first communications device (20) and at least one second communications device (30), which computing device (10) comprises a processing unit (11) and a memory (13), said memory containing instructions (12) executable by said processing unit, and a motion sensor (14), whereby said computing device (10) is operative to:

acquire sensor data of the motion sensor (14) from which the shared secret can be derived, the sensor data representing motion which both the computing device (10) and the first communications device (20) are subjected to;

generate a second data representation from the sensor data, from which

second representation the shared secret can be derived; and

provide the second communications device (30) with the second data representation.

14. The computing device (10) according to claim 13, wherein the sensor data represents physical contact with the first communications device (20).

15. The computing device (10) according to claim 13, wherein the sensor data represents a movement pattern common with the first communications device (20).

16. The computing device (10) according to any one of claims 12-15, wherein a secret shared between a first communications device (20) and a group of second communications devices (30, 70) is established, the computing device further being operative to:

provide the group of second communications device (30, 70) with the second data representation.

17. The computing device (10) according to claim 16, wherein at least two of the second communication devices (30, 70) comprised in said group are provided with the second data representation via different means of communication.

18. The computing device (10) according to any one of claims 12-17, further being operative to:

derive the shared secret; and

perform pairing with the first communications device (20) and/or the at least one second communications device (30) using the derived shared secret.

19. The computing device (10) according to claim 12, wherein the acquiring of a first data representation from which the shared secret can be derived comprises one of: visually acquiring the first data representation, audibly acquiring the first data representation, and acquiring the first data representation over a wireless radio communication channel.

20. The computing device (10) according to claim 19, further comprising one or more of microphone, camera, optical receiver, and radio frequency receiver, in order to acquire said first data representation.

21. The computing device (10) according to any one of claims 12-20, wherein the providing of a second data representation from which the shared secret can be derived comprises one of: visually providing the second data representation, audibly providing the second data representation, and providing the second data representation over a wireless radio communication channel.

22. The computing device (10) according to claim 21, further comprising one or more of conference phone, display, optical transmitter, and radio frequency transmitter, in order to provide said second data representation.

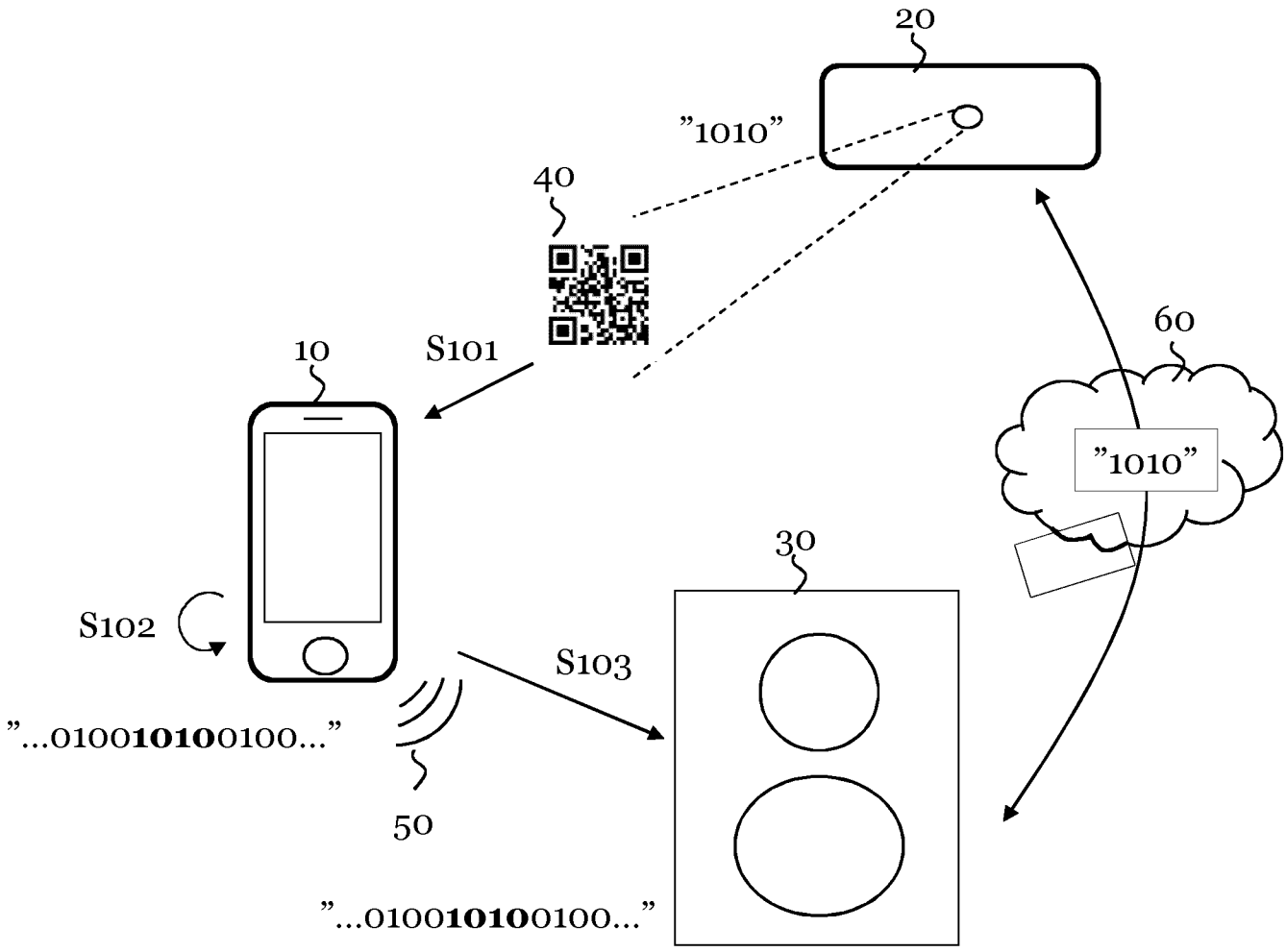

Figure 1

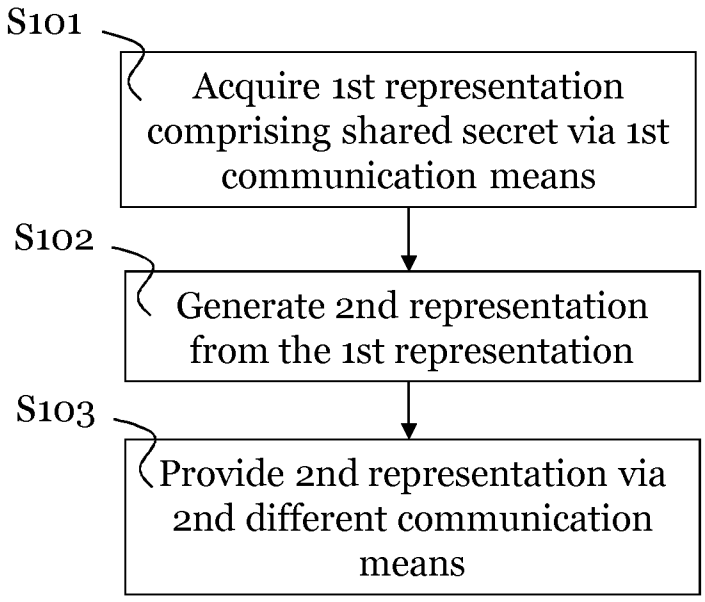

Figure 2

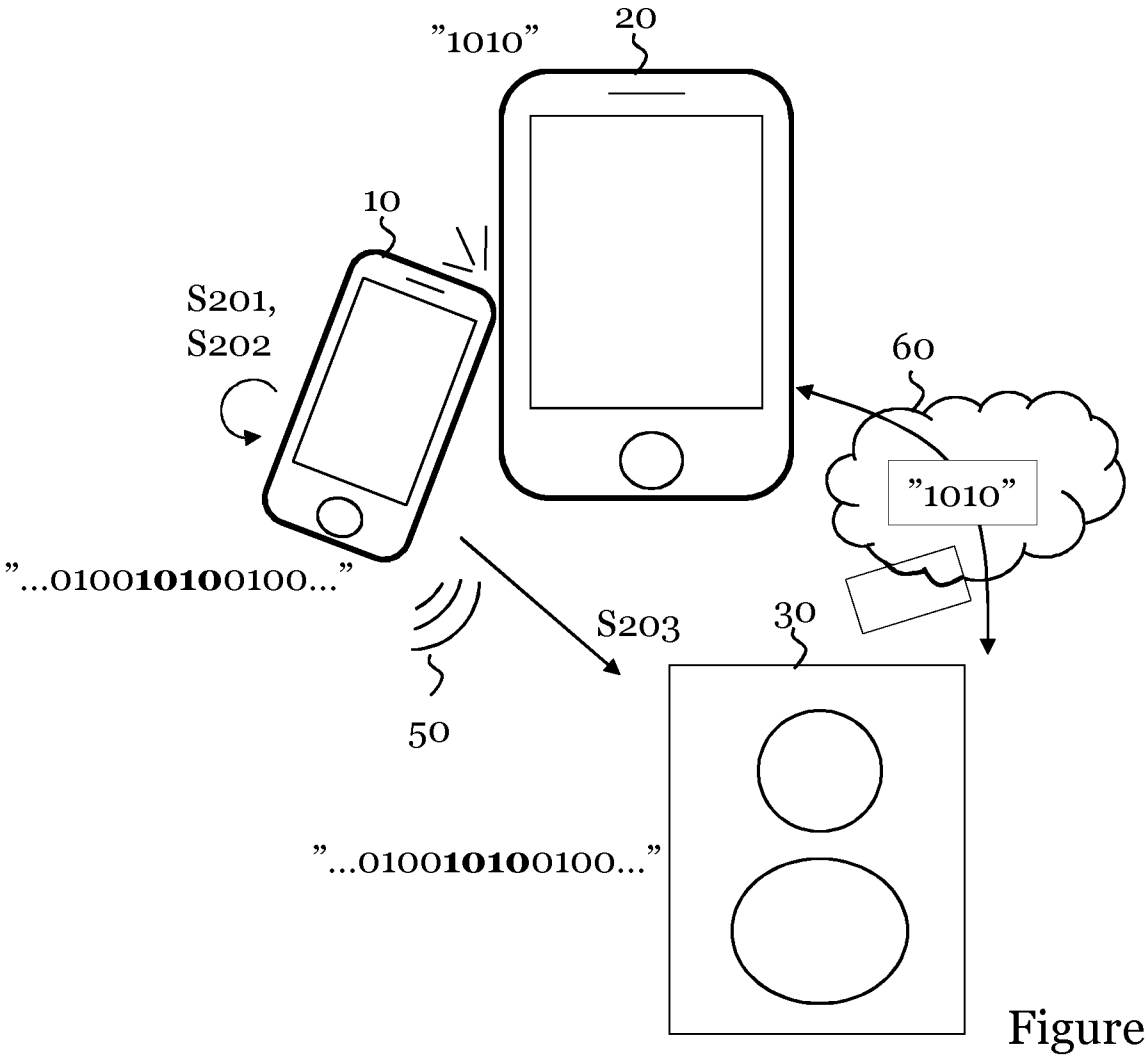

Figure 3

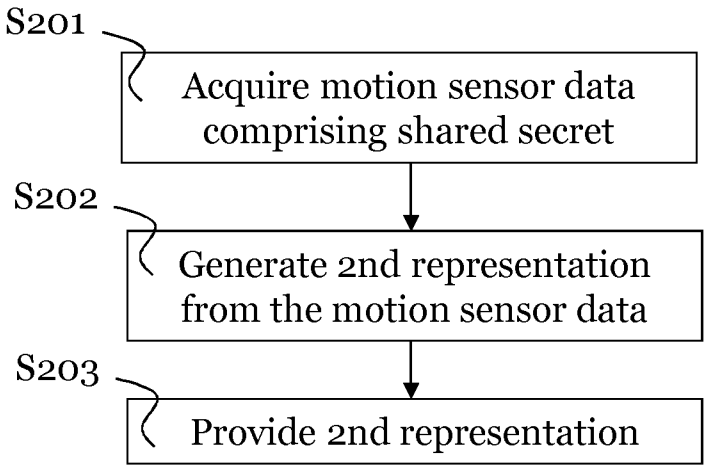

Figure 4

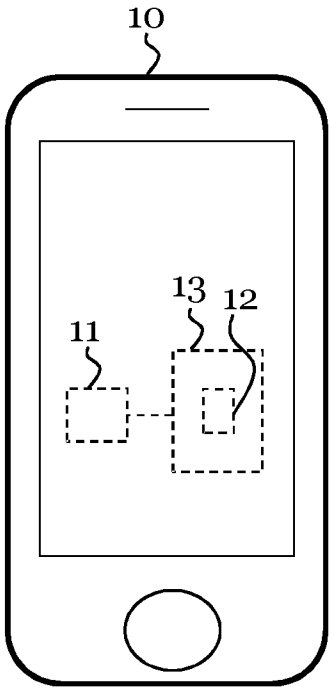

Figure 5

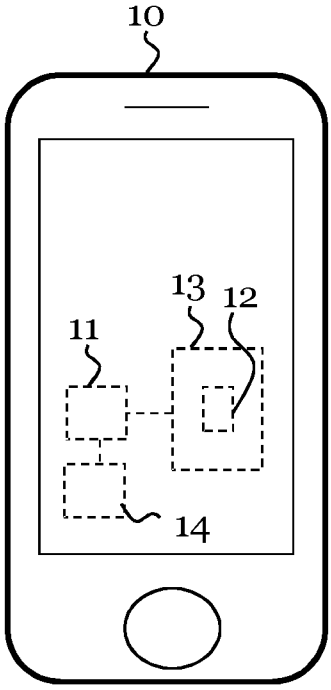

Figure 6

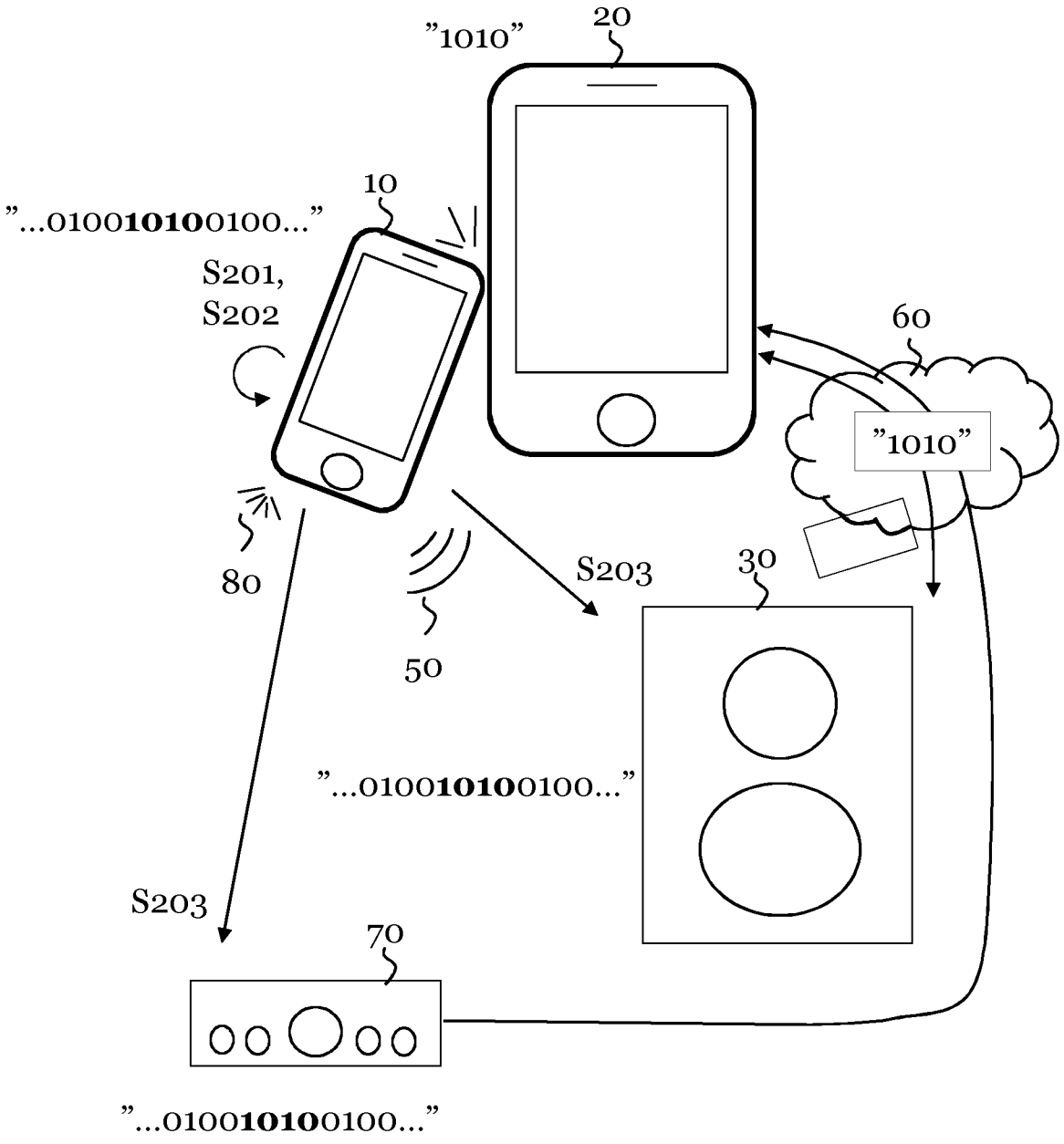
"1010"
20
10
"...0100**1010**0100..."
S201,
S202
60
"1010"
80
50
S203
30
"...0100**1010**0100..."
S203
70
"...0100**1010**0100..."

Figure 7

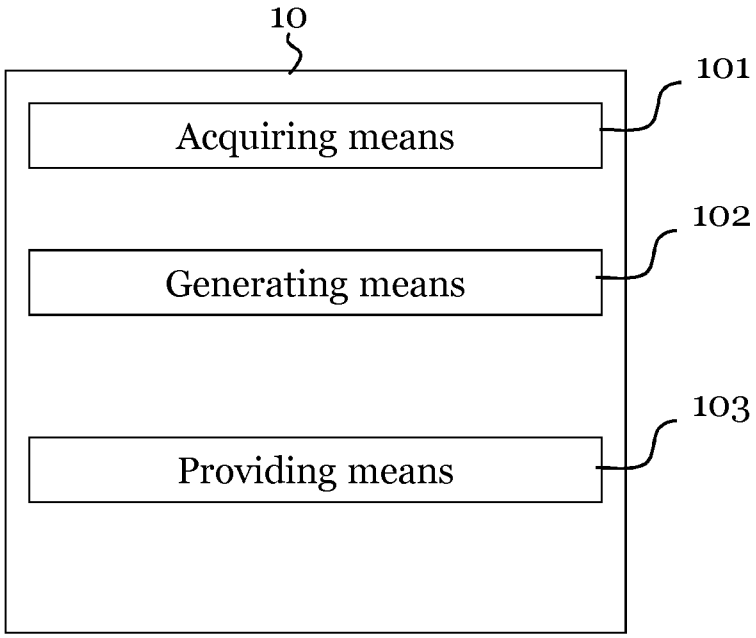

Figure 8

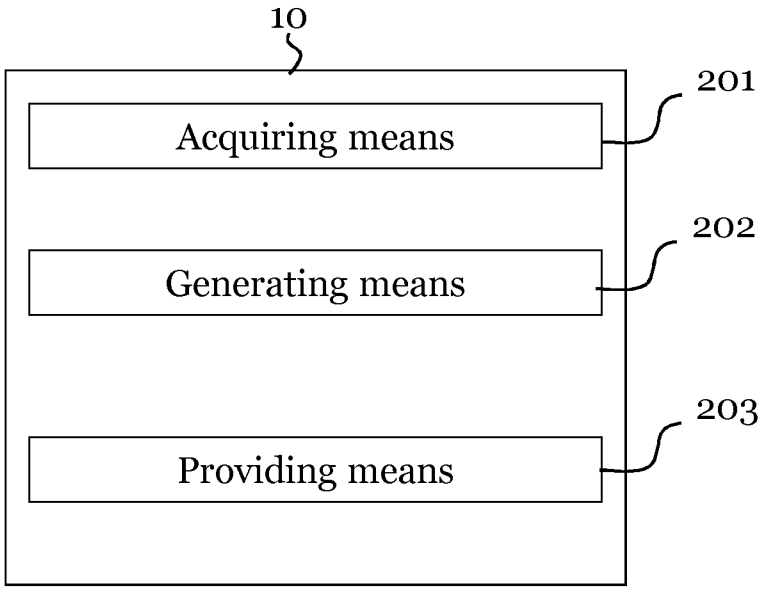

Figure 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/075225

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/04
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal , WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/044395 Al (APPLE INC [US] ; GILES MICHAEL J [US] ; FU JACK I-CHI EH [US] ; MULLENS CH) 5 April 2012 (2012-04-05)	1,5-12 , 16-22
A	paragraph [0005] paragraph [0034] - paragraph [0038] paragraph [0048] ; figure 2C	2-4, 13-15
A	US 2014/325222 Al (KIM SEUNGIL [KR] ET AL) 30 October 2014 (2014-10-30) the whole document	1-22
A	US 2015/288667 Al (ALDER CHRISTOPHER MARK [GB]) 8 October 2015 (2015-10-08) paragraph [0061] - paragraph [0074] ; figure 1	1-22

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" documentwhich may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 June 2016	07/07/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Raposo Pires , Joao

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/075225

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012044395 A1	05-04-2012	CN 103210383 A	17-07-2013
		EP 2622493 A1	07-08-2013
		JP 2013542510 A	21-11-2013
		KR 20130106842 A	30-09-2013
		TW 201232277 A	01-08-2012
		WO 2012044395 A1	05-04-2012
US 2014325222 A1	30-10-2014	NONE	
US 2015288667 A1	08-10-2015	NONE	