



(51) International Patent Classification:

H04L 9/08 (2006.01)

(21) International Application Number:

PCT/FI2020/050282

(22) International Filing Date:

29 April 2020 (29.04.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201941025665 27 June 2019 (27.06.2019) IN

(71) Applicant: NOKIA TECHNOLOGIES OY [FI/FI];

Karakaari 7, 02610 Espoo (FI).

(72) Inventors: GEORGE, Jos; Thaikudom (H), V.P. Mar-

rikkar Road, Edappally, Kerala, Kochi 682024 (IN).

CHELLAPANDI, Jeyaraj; Flat No. 203, SLV Sunshine, A cross, Vijaya Bank Colony, Karnataka, Banaswadi 560043 (IN). S BYKAMPADI, Nagendra; 59 A Eastwood Layout, Haralur Road, Off Sarjapura Main Road, §Karnataka, Bangalore 560102 (IN).

(74) Agent: NOKIA TECHNOLOGIES OY et al.; Ari Aarnio, IPR Department, Karakaari 7, 02610 Espoo (FI).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) Title: ENCRYPTED COMMUNICATION BASED ON QUANTUM KEY

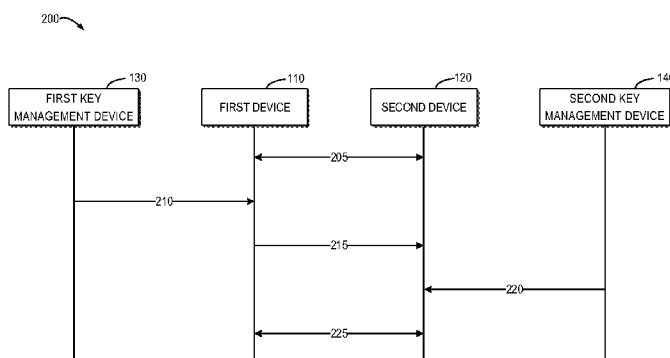


FIG. 2

(57) Abstract: Example embodiments of the present disclosure relate to an encrypted communication based on a quantum key. In an aspect, a first device determines a master key with a second device for an encrypted communication between the first device and the second device. The first device obtains a quantum key and a key identifier of the quantum key from a first key management device associated with the first device, the quantum key and the key identifier being shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol. The first device transmits the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key. With the example embodiments of the present disclosure, communication security between two devices can be improved.

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))*

ENCRYPTED COMMUNICATION BASED ON QUANTUM KEY

FIELD

- 5 [0001] Example embodiments of the present disclosure generally relate to the field of communication, and in particular to devices, methods, apparatuses and a computer readable medium for an encrypted communication based on a quantum key.

BACKGROUND

- 10 [0002] The fifth generation (5G) of mobile network technology is giving greater emphasis on cyber security compared to the previous generations. Capabilities of the 5G network will create more confidential data to get digitized and flow through the mobile network. Not only more humans are getting connected for their private and public uses, but also machines, robots, cars, Artificial Intelligence (AI) enabled devices, and the like will be using
15 the 5G network for their critical communications. Thus, the 5G network must be able to provide long-term security for the data transmitted through the network by enterprises, governments, militaries, transportation, critical infrastructures and many more. This will create a huge responsibility on the 5G network to ensure maximum security available when being designed and deployed.
- 20 [0003] However, as computing power of cracking devices increases, the communication security in the 5G network is now confronted with more and more challenges.

SUMMARY

- 25 [0004] In general, example embodiments of the present disclosure provide a solution for an encrypted communication based on a quantum key.

- [0005] In a first aspect, there is provided a first device. The first device comprises at least one processor and at least one memory storing computer program codes. The at least one memory and the computer program codes are configured to, with the at least one processor, cause the first device to determine a master key with a second device for an encrypted
30 communication between the first device and the second device. The at least one memory and the computer program codes are also configured to, with the at least one processor, cause

the first device to obtain a quantum key and a key identifier of the quantum key from a first key management device associated with the first device. The quantum key and the key identifier are shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol.

- 5 The at least one memory and the computer program codes are further configured to, with the at least one processor, cause the first device to transmit the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

- [0006] In a second aspect, there is provided a second device. The second device
10 comprises at least one processor and at least one memory storing computer program codes. The at least one memory and the computer program codes are configured to, with the at least one processor, cause the second device to determine a master key with a first device for an encrypted communication between the first device and the second device. The at least one memory and the computer program codes are also configured to, with the at least one
15 processor, cause the second device to receive a key identifier of a quantum key from the first device. The quantum key and the key identifier are shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol. The at least one memory and the computer program codes are further configured to, with the at least one processor,
20 cause the second device to obtain the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

- [0007] In a third aspect, there is provided a method. The method comprises determining, at a first device, a master key with a second device for an encrypted communication between
25 the first device and the second device. The method also comprises obtaining a quantum key and a key identifier of the quantum key from a first key management device associated with the first device. The quantum key and the key identifier are shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol. The method further comprises
30 transmitting the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

- [0008] In a fourth aspect, there is provided a method. The method comprises determining,

at a second device, a master key with a first device for an encrypted communication between the first device and the second device. The method also comprises receiving a key identifier of a quantum key from the first device. The quantum key and the key identifier are shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol. The method further comprises obtaining the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

[0009] In a fifth aspect, there is provided an apparatus. The apparatus comprises means for determining, at a first device, a master key with a second device for an encrypted communication between the first device and the second device. The apparatus also comprises means for obtaining a quantum key and a key identifier of the quantum key from a first key management device associated with the first device. The quantum key and the key identifier are shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol. The apparatus further comprises means for transmitting the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

[0010] In a sixth aspect, there is provided an apparatus. The apparatus comprises means for determining, at a second device, a master key with a first device for an encrypted communication between the first device and the second device. The apparatus also comprises means for receiving a key identifier of a quantum key from the first device. The quantum key and the key identifier are shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol. The apparatus further comprises means for obtaining the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

[0011] In a seventh aspect, there is provided a non-transitory computer readable medium storing program instructions for causing an apparatus to perform at least the method according to the third or fourth aspect.

[0012] It is to be understood that the summary section is not intended to identify key or

essential features of example embodiments of the present disclosure, nor is it intended to be used to limit the scope of the present disclosure. Other features of the present disclosure will become easily comprehensible through the following description.

5 BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Some example embodiments will now be described with reference to the accompanying drawings, in which:

[0014] Fig. 1 illustrates a schematic diagram of a communication environment in which some example embodiments of the present disclosure can be implemented;

10 [0015] Fig. 2 illustrates an example communication process among a first device, a second device, a first key management device, and a second key management device in accordance with some example embodiments of the present disclosure;

15 [0016] Fig. 3 illustrates an example communication process between a first device and a first key management device in accordance with some example embodiments of the present disclosure;

[0017] Fig. 4 illustrates an example communication process between a second device and a second key management device in accordance with some example embodiments of the present disclosure;

20 [0018] Fig. 5 illustrates a schematic diagram of an example dual key agreement according to some example embodiments of the present disclosure;

[0019] Fig. 6 illustrates a flowchart of an example method in accordance with some example embodiments of the present disclosure;

[0020] Fig. 7 illustrates a flowchart of another example method in accordance with some example embodiments of the present disclosure;

25 [0021] Fig. 8 illustrates a simplified block diagram of an apparatus that is suitable for implementing example embodiments of the present disclosure; and

[0022] Fig. 9 illustrates a block diagram of an example computer readable medium in accordance with some example embodiments of the present disclosure.

30 [0023] Throughout the drawings, the same or similar reference numerals represent the same or similar element.

DETAILED DESCRIPTION

[0024] Principles of the present disclosure will now be described with reference to some example embodiments. It is to be understood that these example embodiments are described only for the purpose of illustration and help those skilled in the art to understand and implement the present disclosure, without suggesting any limitation as to the scope of the disclosure. The disclosure described herein can be implemented in various manners other than the ones described below.

[0025] In the following description and claims, unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skills in the art to which this disclosure belongs.

[0026] References in the present disclosure to “one embodiment,” “an embodiment,” “an example embodiment,” and the like indicate that the embodiment described may include a particular feature, structure, or characteristic, but it is not necessary that every example embodiment includes the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same example embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an example embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other example embodiments whether or not explicitly described.

[0027] It shall be understood that although the terms “first” and “second” or the like may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another. For example, a first element could be termed a second element, and similarly, a second element could be termed a first element, without departing from the scope of example embodiments. As used herein, the term “and/or” includes any and all combinations of one or more of the listed terms.

[0028] The terminology used herein is for the purpose of describing particular example embodiments only and is not intended to be limiting of example embodiments. As used herein, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the

terms “comprises”, “comprising”, “has”, “having”, “includes” and/or “including”, when used herein, specify the presence of stated features, elements, components and/or the like, but do not preclude the presence or addition of one or more other features, elements, components and/or combinations thereof.

5 **[0029]** As used in this application, the term “circuitry” may refer to one or more or all of the following:

 (a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry) and

 (b) combinations of hardware circuits and software, such as (as applicable):

10 (i) a combination of analog and/or digital hardware circuit(s) with software/firmware and

 (ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions) and

15 (c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

[0030] This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry
20 also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other
25 computing or network device.

[0031] As used herein, the term “communication network” refers to a network following any suitable communication standards, such as Long Term Evolution (LTE), LTE-Advanced (LTE-A), Wideband Code Division Multiple Access (WCDMA), High-Speed Packet Access (HSPA), Narrow Band Internet of Things (NB-IoT) and so on. Furthermore, the
30 communications between a terminal device and a network device in the communication network may be performed according to any suitable generation communication protocols,

including, but not limited to, the first generation (1G), the second generation (2G), 2.5G, 2.75G, the third generation (3G), the fourth generation (4G), 4.5G, the future fifth generation (5G) communication protocols, and/or any other protocols either currently known or to be developed in the future. Example embodiments of the present disclosure may be applied in various communication systems. Given the rapid development in communications, there will of course also be future type communication technologies and systems with which the present disclosure may be embodied. It should not be seen as limiting the scope of the present disclosure to only the aforementioned system.

[0032] As used herein, the term “network device” refers to a node in a communication network via which a terminal device accesses the network and receives services therefrom. The network device may refer to a base station (BS) or an access point (AP), for example, a node B (NodeB or NB), an evolved NodeB (eNodeB or eNB), a NR NB (also referred to as a gNB), a Remote Radio Unit (RRU), a radio header (RH), a remote radio head (RRH), a relay, a low power node such as a femto, a pico, and so forth, depending on the applied terminology and technology.

[0033] The term “terminal device” refers to any end device that may be capable of wireless communication. By way of example rather than limitation, a terminal device may also be referred to as a communication device, user equipment (UE), a Subscriber Station (SS), a Portable Subscriber Station, a Mobile Station (MS), or an Access Terminal (AT). The terminal device may include, but not limited to, a mobile phone, a cellular phone, a smart phone, voice over IP (VoIP) phones, wireless local loop phones, a tablet, a wearable terminal device, a personal digital assistant (PDA), portable computers, desktop computer, image capture terminal devices such as digital cameras, gaming terminal devices, music storage and playback appliances, vehicle-mounted wireless terminal devices, wireless endpoints, mobile stations, laptop-embedded equipment (LEE), laptop-mounted equipment (LME), USB dongles, smart devices, wireless customer-premises equipment (CPE), an Internet of Things (IoT) device, a watch or other wearable, a head-mounted display (HMD), a vehicle, a drone, a medical device and applications (e.g., remote surgery), an industrial device and applications (e.g., a robot and/or other wireless devices operating in an industrial and/or an automated processing chain contexts), a consumer electronics device, a device operating on commercial and/or industrial wireless networks, and the like. In the following description, the terms “terminal device”, “communication device”, “terminal”, “user equipment” and

“UE” may be used interchangeably.

[0034] As mentioned, with the increasing computing power of cracking devices, the communication security in the 5G network is confronted with more and more challenges. In particular, the technology related to computing power is getting enhanced day by day, and thus the computing power is increasing such a way that an adversary may have huge computing power to crack existing cryptographic techniques based on mathematical solutions. As a result, security practitioners must revise the cryptographic algorithms using in the secure communication protocol stack. One recent such example is the removal of Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) key transport option from Transport Layer Security (TLS) 1.3 (Request For Comments, RFC, 8446).

[0035] On the other hand, today’s public key cryptography is still not proven to be secure against mathematical attacks. In a cryptographic attack scenario, an adversary can record all the secure data transmissions happening on a wire. Then, the adversary can take the data to his safe place, and later decrypt the data when enough computational power is available.

[0036] Another raising concern is related to the arrival of quantum computers. With the age of quantum computing drawing ever-closer, traditional encryption methods are at risk. Various governments and tech-giants are investing heavily on developing quantum computers. Quantum computers use the principles of quantum physics for its operations and are capable of performing mathematical calculation used for asymmetric cryptography in orders of magnitude more quickly than classical, electronic computers.

[0037] While brute force attacks can take months to break through security, quantum attacks can use more advanced techniques to break standard public key cryptography in a much shorter timeframe. This will create an alarming concern, because currently asymmetric cryptographic algorithms like RSA, Diffie Hellman and its variants are used primarily in existing internet cryptographic set up as vital authentication and key exchange primitives. Quantum computers can quickly crack these algorithms.

[0038] The National Institute of Standards and Technology (NIST) in the United States had already taken this concern seriously and they are evaluating possible cryptographic algorithms to handle threat from quantum computers. Among 69 submissions received by the NIST, around 26 algorithms are shortlisted and are considered as the strongest candidates

submitted to its Post-Quantum Cryptography Standardization. Again, these algorithms are based on complex mathematical calculations and according to the current studies it is suitable to handle threats from quantum computers. However, this does not mean that these algorithms cannot be broken, probably by an advanced computer in future.

5 [0039] In the 5G roaming architecture, a home Public Land Mobile Network (PLMN) and a visited PLMN can be connected through a Security Edge Protection Proxy (SEPP) for secure control plane connectivity. One of the key functions of the SEPP is to handle key management aspects that involve setting up required cryptographic keys needed for securing messages between two SEPPs. Due to the security concerns as discussed above, the current
10 design of SEPPs, based on cryptography and cipher suites of the current generation, cannot survive the computing power of Quantum computers that can easily break these algorithms and thus creating security vulnerabilities on the roaming interface between two operators of the two PLMNs.

[0040] In view of the above problems and other potential problems in the traditional
15 solutions, example embodiments of the present disclosure provide a solution for an encrypted communication based on a quantum key. In some example embodiments, there is proposed an approach to increase the security of communications between two devices (resistant to attacks generated by quantum computers) by associating the devices with a quantum key distribution (QKD) network (also termed as a QKD system). Some example
20 embodiments define how a device can fetch a quantum key from a key management device belonging to a QKD network. Then, the device can use the quantum key to increase the overall security of communication by combining the quantum key with a master key obtained from classical cryptography. Principles and implementations of example embodiments of the present disclosure will be described in detail below with reference to
25 the figures.

[0041] Fig. 1 illustrates a schematic diagram of a communication environment 100 in which some example embodiments of the present disclosure can be implemented. The communication environment 100 includes a first communication network 102 and a second communication network 104. In some example embodiments, the first and second
30 communication networks 102 and 104 may be two PLMNs. However, it is appreciated that the first and second communication networks 102 and 104 can be any other existing or future communication networks in which example embodiments of the present disclosure can be

implemented. In addition, although some example embodiments are described with reference to a scenario where there are two communication networks, it is understood that example embodiments of the present disclosure equally applicable to other scenarios where there is only one communication network or there are more than two communication networks.

[0042] As shown in Fig. 1, the first communication network 102 and the second communication network 104 include a first device 110 and a second device 120, respectively, which can communicate with each other. In some example embodiments, the first device 110 and the second device 120 can provide secure communications between the two communication networks 102 and 104. For example, the first network function 150 (for example, an Access and Mobility Management Function, AMF) in the first communication network 102 may intend to transmit data to a second network function 160 (for example, a Unified Data Management, UDM) in the second communication network 104. Then, the first network function 150 can send the data to the first device 110, which may encrypt the data and forward the encrypted data to the second device 120. Upon receiving the encrypted data, the second device 120 may decrypt the encrypted data and forward the decrypted data to the second network function 160. In this way, the first device 110 and the second device 120 provide safe communications between network functions in different communication networks.

[0043] In order to establish a secure communication, there may be two logically separate interfaces, namely a first interface 115 and a second interface 125, between the first device 110 and the second device 120. The first interface 115 can be used for transmitting data between the first device 110 and the second device 120. The second interface 125 may be used for establishing a secure connection between the first device 110 and the second device 120, so that the first network function 150 in the first communication network 102 can securely transmit data to the second network function 160 in the second communication network 104 through the first interface 115. That is, the first interface 115 may be controlled by the second interface 125. Although Fig. 1 shows two interfaces between the first device 110 and the second device 120, it is understood that there may be any suitable number of interfaces between the first device 110 and the second device 120. Example embodiments of the present disclosure are not limited in this regard.

[0044] In some example embodiments, the first device 110 can be a first SEPP of a first

PLMN, and the second device 110 can be a second SEPP of a second PLMN. The SEPP is an ambition of 5G network design to provide maximum security to the control plane signals during an inter-PLMN communication. In general, the SEPP is designed to handle requests from a network function (NF) in a PLMN (for example, the AMF in a Vodafone network) to communicate securely with another NF in another PLMN (for example, the UDM in an Airtel network). The SEPP is based on the 5G service-based architecture. Once a service-consumer NF (such as, the AMF) in a home PLMN sends a service request to a service-provider NF (such as, the UDM) in a visited PLMN, the SEPP in the home PLMN may encrypt the data and forward the encrypted data to the SEPP of the visited PLMN, which can decrypt the data, ensure that the data is received correctly, and then forward the data to the provider NF. In order to visualize easily, the function of the SEPP can be considered as a perimeter firewall in a secure PLMN, such as an enterprise network.

[0045] In the case that the first device 110 and the second device 120 are SEPPs, the interface between the two SEPPs may be called an N32 interface. The N32 interface can be logically considered as two separate interfaces, that is, an N32-f interface and an N32-c interface, which may be examples of the first interface 115 and the second interface 125, respectively. In general, the N32-c interface is for establishing a secure connection between the first SEPP and the second SEPP, so that an NF in the first PLMN can securely transmit data to another NF in the second PLMN through the N32-f interface. In other words, the N32-f interface is controlled by N32-c interface. The SEPPs can use the established N32-c connection to negotiate the N32-f specific associated security configuration parameters required to enforce Application Layer Security (ALS) on messages exchanged between SEPPs. The ALS in this case can be implemented by JavaScript Object Notation (JSON) Web Encryption (JWE).

[0046] In some example embodiments, the first device 110 and the second device 120 may not directly communicate with each other, but through one or more relays. For example, in the event that the first device 110 and the second device 120 are SEPPs. There may be another network element in an inter-PLMN scenario, that is, an interconnection provider or Internetwork Packet Exchange (IPX). In actual deployment scenario, a home PLMN may not have a roaming relationship between all other PLMNs it desires to connect. Instead, the home PLMN may have a tie up with an IPX and the IPX can in turn connect to different roaming PLMNs. In such a scenario, the first SEPP may not be connected to the second

SEPP directly, but can be connected via their respective IPXs. The IPX can offer services that require modifications of the messages transported over the interconnection (such as, the N32) interface. These modifications can be appended to the messages as digitally signed JWS objects which contain the desired changes.

5 [0047] In some example embodiments, the encryption methods supported by the JWE are Authenticated Encryption with Associated Data (AEAD) methods, namely, methods that provide encryption and integrity protection in one single operation and can additionally provide integrity protection to additional data. Therefore, the first device 110 in the first communication network 102, while sending the secure data to the second device 120 in the
10 second communication network 104, can send data blocks with both ciphered protection and integrity protection, and some data blocks with only integrity protection. The data with only integrity protection can be read by the IPX and makes necessary modifications according to the requirements.

[0048] It can be seen that the security of the data transmitted between the first device 110
15 and the second device 120 depends on the encryption and integrity check techniques used between them. Again, the strength of the encryption and integrity check algorithms is having direct dependency on the strength of the shared keys (such as, session keys) used between the two devices and how safely the keys are distributed between the two devices without any eavesdropping. Accordingly, in order to ensure a secure communication
20 between the first device 110 and the second device 120, the first device 110 and the second device 120 may need to determine a master key 170 to be used in the encrypted communication between them.

[0049] Further, in addition to the master key 170, the first device 110 can obtain a quantum key 180 and a key identifier 185 of the quantum key 180 from a first key management device
25 130 associated with the first device 110. Then, the first device 110 may inform the second device 120 of the key identifier 185, so that the second device 120 can obtain the quantum key 180 from a second key management device 140 associated with the second device 120. The first key management device 130 and the second key management device 140 can share the quantum key 180 and the key identifier 185 based on a QKD protocol, which means that
30 the quantum key 180 and the key identifier 185 shared between the first key management device 130 and the second key management device 140 can be information theoretically secure.

[0050] In some example embodiments, the first key management device 130 and the second key management device 140 may belong to a same QKD network. The QKD network can consist of a single link (also termed as a QKD link) between a single QKD transmitter and a single QKD receiver, or it can be an extended network involving many such QKD links. Similarly, the first key management device 130 and the second key management device 140 may be either connected by a direct QKD link or a QKD network comprising multiple QKD links. Thus, the first key management device 130 and the second key management device 140 can share the quantum key 180 and the key identifier 185 via a QKD link between them. In other words, the first key management device 130 and the second key management device 140 can exchange and store quantum keys and each quantum key delivered can be assigned a universally unique identifier.

[0051] As used herein, a QKD protocol may refer to a communication protocol and data format for a QKD network to supply cryptographic keys to an application, such as the BB84 protocol, the BBM92 protocol, the Ekert91 protocol, the Measurement Device Independent (MDI)-QKD protocol, the decoy state QKD protocol, the European Telecommunications Standards Institute (ETSI) Group Specification (GS) QKD standards, and other existing or future QKD protocols. More generally, a QKD protocol can refer to any protocol for implementing a QKD technology.

[0052] The QKD protocol can ensure the exchange of a cryptographic key between two remote parties with proven security, guaranteed by the fundamental laws of physics. Accordingly, the QKD network may deliver common shared quantum keys to devices in different PLMNs. In this way, quantum keys can be generated and shared securely with QKD technology by the first key management device 130 and the second key management device 140. In some example embodiments, each of the first key management device 130 and the second key management device 140 can have a unique identifier in the QKD network.

[0053] The QKD link between the first key management device 130 and the second key management device 140 can be constituted by the combination of a classical channel 135 and a quantum channel 145. The first key management device 130 may generate a random stream of classical bits and encode them into a sequence of non-orthogonal quantum states of light, sent over the quantum channel 145. Upon reception of those quantum states, the second key management device 140 can perform some appropriate measurements leading it to share some classical data correlated with the bit stream of the first key management device

130.

[0054] The classical channel 135 may then be used to test these correlations. If the correlations are high enough, this statistically implies that no significant eavesdropping has taken place on the quantum channel 145 and thus that with very high probability, a perfectly secure symmetric key can be distilled from the correlated data shared by the first key management device 130 and the second key management device 140. In the opposite case, the key generation process has to be aborted and started again.

[0055] In some example embodiments, each of the first key management device 130 and the second key management device 140 may include a Key Management Entity (KME) and a QKD transceiver. The KME may deal with the generation, exchange, use, destruction and replacement of keys, such as quantum keys. The QKD transceiver can implement the QKD technology by transmitting and receiving information via a QKD link. In these example embodiments, the first device 110 and the second device 120 can receive quantum keys from a QKD setup by associating with an external KME, which is already associated with a QKD system.

[0056] In some example embodiments, each of the first key management device 130 and the second key management device 140 may have a quantum random number generator (QRNG), which can be used by the first key management device 130 and the second key management device 140 to supply true random keys to the first device 110 and the second device 120, respectively.

[0057] In case the two communication networks 102 and 104 are PLMNs, one or more trusted optical fiber paths may be defined between the two PLMNs to carry both the QKD data and the general traffic. One option is to use a same optical fiber cable with Wave Division Multiplexing (WDM) enabled to send both the QKD traffic and the classical data. A more precise option to avoid error while transmission is to use a dedicated fiber for the QKD system. Although the optical fiber is used herein as an example communication medium between the two networks 102 and 104, it is appreciated that the first device 110 and the second device 120 can communicate with each other through any suitable wired or wireless communication medium. Analogously, the first key management device 130 and the second key management device 140 can communicate with each other through any suitable wired or wireless communication medium.

[0058] It is to be understood that the number of communication networks, the number of devices, the number of channels, and the number of other elements are only for the purpose of illustration without suggesting any limitations. The communication environment 100 may include any suitable number of communication networks, any suitable number of devices, any suitable number of channels, and any suitable number of other elements adapted for implementing example embodiments of the present disclosure. Although not shown, it would be appreciated that all the devices and other function entities may belong to and be located in the same communication network.

[0059] Communications in the communication environment 100 may be implemented according to any proper communication protocol(s), comprising, but not limited to, cellular communication protocols of the first generation (1G), the second generation (2G), the third generation (3G), the fourth generation (4G) and the fifth generation (5G) and on the like, wireless local network communication protocols such as Institute for Electrical and Electronics Engineers (IEEE) 802.11 and the like, and/or any other protocols currently known or to be developed in the future. Moreover, the communication may utilize any proper wireless communication technology, comprising but not limited to: Code Division Multiple Access (CDMA), Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Frequency Division Duplex (FDD), Time Division Duplex (TDD), Multiple-Input Multiple-Output (MIMO), Orthogonal Frequency Division Multiple (OFDM), Discrete Fourier Transform spread OFDM (DFT-s-OFDM) and/or any other technologies currently known or to be developed in the future.

[0060] Reference is now made to Fig. 2, which illustrates an example communication process 200 among the first device 110, the second device 120, the first key management device 130, and the second key management device 140 in accordance with some example embodiments of the present disclosure. For the purpose of discussion, the process 200 will be described with reference to Fig. 1. However, it would be appreciated that the process 200 may be equally applicable to other communication scenarios where a quantum key is used for an encrypted communication between two devices.

[0061] It would also be appreciated that although the process 200 is discussed in the case that the first device 110 and the first key management device 130 are within the first communication network 102 and the second device 120 and the second key management device 140 are within the second communication network 104, the process 200 may be

equally applicable to the case that the first device 110, the second device 120, the first key management device 130, and the second key management device 140 are within a same communication network.

[0062] As shown in Fig. 2, the first device 110 determines 205 the master key 170 with the second device 120 for an encrypted communication between the first device 110 and the second device 120. For example, this encrypted communication may be used to implement a secure communication between the first network function 150 in the first communication network 102 and the second network function 160 in the second communication network 104. Since the determination 205 of the master key 170 is performed by the first device 110 together with the second device 120, from a perspective of the second device 120, it can be that the second device 120 determines 205 the master key 170 with the first device 110 for the encrypted communication. In some example embodiments, the determination 205 of the master key 170 may involve some interactions between the first device 110 and the second device 120 for negotiating the master key 170.

[0063] For example, if the first device 110 is a first SEPP of a first (home) PLMN and the second device 120 is a second SEPP of a second (visited) PLMN, the first device 110 and the second device 120 may perform mutual authentication and negotiation of cipher suites. In addition, each of the first device 110 and the second device 120 may handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the interfaces (such as, the N32 interface) between the two devices.

[0064] In this scenario, the first device 110 and the second device 120 may independently export a key material associated with the first connection (such as, an N32-c connection) between them and use it as a pre-master secret (or pre-master key) for generating a shared master secret (master key) 170. In some example embodiments, the master key 170 can be obtained from a TLS exporter and may be used to derive session keys and possibly other encryption parameters (such as, IV salts) for the N32-f context and use it for enforcing application layer security (JWE).

[0065] Continuing with reference to Fig. 2, the first device 110 obtains 210 the quantum key 180 and a key identifier 185 of the quantum key 180 from the first key management device 130 associated with the first device 110. As described with reference to Fig. 1, the quantum key 180 and the key identifier 185 are shared between the first key management device 130 and the second key management device 140 associated with the second device

120 based on a QKD protocol, which means that the sharing of quantum key 180 and the key identifier 185 between the first key management device 130 and the second key management device 140 can be information theoretically secure.

[0066] There may be various possible manners for the first device 110 to obtain the quantum key 180 and the key identifier 185 from the first key management device 130. For example, the first key management device 130 may be configured to generate a quantum key and a related key identifier for the first device 110 periodically, such that the first device 110 can use the periodical quantum key in an encrypted communication with other devices. In some other example embodiments, the first device 110 can use a request-response manner to obtain the quantum key 180 and the key identifier 185 from the first key management device 130. In this way, the quantum keys can be generated for the first device 110 as needed, so that the computing resources, transmission resources, and/or other resources related to the generation and distribution of the quantum keys can be conserved. This request-response manner will be detailed below with reference to Fig. 3.

[0067] Fig. 3 illustrates an example communication process 300 between the first device 110 and the first key management device 130 in accordance with some example embodiments of the present disclosure. As shown in Fig. 3, in order to obtain the quantum key 180 and the key identifier 185, the first device 110 may transmit 305 a request to the first key management device 130 for requesting the quantum key 180. The request can include a device identifier of the second device 120, so that the first key management device 130 may associate the generated quantum key 180 with the first device 110 and the second device 120.

[0068] Upon receiving the request from the first device 110, the first key management device 130 can generate the quantum key 180 for the encrypted communication between the first device 110 and the second device 120, and then transmit 310 the quantum key 180 along with the key identifier 185 to the first device 110. Accordingly, the first device 110 can receive 310 the quantum key 180 and the key identifier 185 from the first key management device 130.

[0069] In some example embodiments, the first device 110 can use a key delivery Application Programming Interface (API) to fetch the quantum key 180 from the first key management device 130. For example, the key delivery API may be a Representational State Transfer (REST)-based API. In this event, the first device 110 can send a Hypertext

Transfer Protocol Secure (HTTPS) request to the first key management device 130 to get the quantum key 180, the key identifier 185, and possibly other related status information. As non-limiting examples, such a HTTPS request may include but not limited to “Get key,” “Get key with key IDs,” “Key ID notification,” and the like.

5 [0070] As used herein, the device sending an initial “Get key” request can be referred to as a master device for the returned quantum key(s), whereas the device sending a subsequent “Get key with key IDs” request may be called as a slave device for the returned quantum key(s). That is, in some example embodiments, the first device 110 may call the key delivery API “Get key” with the device identifier of the slave device (the second device 120)
10 to get one or more quantum key from the first key management device 130, which may then deliver to the first device 110 one or more key materials with the associated key identifiers that are (to be) shared with the second key management device 140.

[0071] Referring back to Fig. 2, subsequent to obtaining 210 the quantum key 180 and the key identifier 185 from the first key management device 130, the first device 110 transmits
15 215 the key identifier 185 to the second device 120. From the perspective of the second device 120, the second device 120 receives 215 the key identifier 185 from the first device 110. With the key identifier 185, the second device 120 can obtain the quantum key 180 from the second key management device 140 associated with the second device 120.

[0072] In some example embodiments, the first device 110 may transmit the key identifier
20 185 as part of a key agreement and parameter exchange procedure between the first device 110 and the second device 120. Accordingly, the second device 120 may receive the key identifier 185 as part of the key agreement and parameter exchange procedure. In this way, the existing key agreement and parameter exchange procedure (which, for example, can be used to protect NF service related signaling over the N32-f interface) between the first device
25 110 and the second device 120 (such as two SEPPs) can be reused, and thus there is no need to add new signaling for transmitting the key identifier 185. In case the first device 110 and the second device 120 are SEPPs, the notification of the key identifier 185 can be sent across the N32-c interface between them.

[0073] In some example embodiments, the quantum key 180 may comprise a true random
30 number generated by a QRNG. By using a true random number generator to create a highly secure quantum key 180 and combining this quantum key 180 with the master key 170 to generate a shared session key can enhance the security of the secured data transmission.

For example, a QRNG can use a quantum source to create a true random number, and thus it is a special true random number generator where the randomness is due to the unpredictable nature of the outcome of quantum measurements.

[0074] Continuing with reference to Fig. 2, after receiving 215 the key identifier 185 from the first device 110, the second device 120 obtains 220 the quantum key 180 from the second key management device 140 based on the key identifier 185. As mentioned, the quantum key 180 and the key identifier 185 are shared between the first key management device 130 and the second key management device 140 based on a QKD protocol. Therefore, upon the first key management device 130 generates the quantum key 180 for the first device 110 and the second device 120, the first key management device 130 may share the quantum key 180 and the key identifier 185 with the second key management device 140 associated with the second device 120, based on the QKD protocol and via the QKD link. Accordingly, the second key management device 140 can obtain the quantum key 180 and provide it to the second device 120.

[0075] There are various possible manners for the second device 120 to obtain the quantum key 180 from the second key management device 140. For example, the second key management device 140 may be configured to transmit the quantum key 180 to the second device 120 autonomously, since the second key management device 140 can determine that the quantum key 180 is for use in the encrypted communication between the second device 120 and the first device 110. In some other example embodiments, the second device 120 can use a request-response manner to obtain the quantum key 180 from the second key management device 140. In this way, the quantum keys can be generated for the second device 120 as needed, so that the computing resources, transmission resources, and/or other resources related to the generation and distribution of the quantum keys can be conserved. This request-response manner will be detailed below with reference to Fig. 4.

[0076] Fig. 4 illustrates an example communication process 400 between the second device 120 and the second key management device 140 in accordance with some example embodiments of the present disclosure. As shown in Fig. 4, in order to obtain the quantum key 180, the second device 120 may transmit 405 a request to the second key management device 140 for requesting the quantum key 180. The request can comprise the key identifier 185 and a device identifier of the first device.

[0077] Upon receiving the request from the second device 120, the second key

management device 140 can uniquely identify the quantum key 180 for the first device 110 and the second device 120, based on the key identifier 185 and the device identifier of the first device 110, even if the key identifier 185 may not be globally unique. Then, the second key management device 140 can transmit 410 the key identifier 185 to the second device
5 120, and thus the second device 120 may receive 410 the quantum key 180 from the second key management device 140.

[0078] In some example embodiments, the second device 120 may call the key delivery API “Get key with key IDs” with the device identifier of the first device 110 (the master device) and one or more notified key identifiers to get one or more identical quantum keys
10 from the second key management device 140, which then delivers to the second device 120 one or more identical key materials with the identical associated key identifiers that are shared with the first key management device 130.

[0079] Referring back to Fig. 2, upon determining the master key 170 and obtaining the quantum key 180, the first device 110 and the second device 120 can perform 225 the
15 encrypted communication using the master key 170 and the quantum key 180. In other words, both the master key 170 and the quantum key 180 may be used in the encrypted communication. As used herein, this dual key scheme may be termed as a dual secret key agreement. In particular, the first device 110 or the second device 120 can receive the quantum key 180 from a QKD system and combine it with the master key 170 derived from
20 an N32-c initial handshake. In other words, the first device 110 or the second device 120 may obtain a quantum enhanced master key (also referred to as a target key hereinafter) based on the master key 170 and the quantum key 180. Then, the first device 110 or the second device 120 is able to provide the quantum enhanced master key, an information theoretically secure key (unconditionally secure key), to the interface between them (such
25 as, the N32-f interface) for encrypting the transaction between an NF in one PLMN to another NF in another PLMN, for example.

[0080] The idea of such a cascaded cipher is to compose several encryption primitives by applying them sequentially on a same clear text. This idea of cascaded cipher can straightforwardly be applied to a secret key agreement. For example, two keys of the same
30 length may be established through two different secret key agreement schemes (relying on either the same primitive or on different ones) and a final key (also termed as a target key or an enhanced master key) can be obtained based on the two keys, such as, by performing an

exclusive OR (XOR) operation on these two keys. Then, the first device 110 or the second device 120 may perform the encrypted communication between them using the target key. It is to be understood that the XOR operation on the two keys is only an example for obtaining the target key by mathematically combining the two keys. The target key can be
5 obtained in various other mathematical combining manners in other example embodiments. Additionally or alternatively, the target key may be obtained from a hash function with the two keys as input parameters.

[0081] Adopting QKD using a dual key agreement scheme can provide some technical advantages. For example, the approach of a dual secret key agreement could allow
10 certifying a system according to already existing security standards in classical cryptography. This is an easy way to associate a QKD system with a device (such as, a SEPP) without any change in standards. In addition, the approach provides a redundant layer of security to existing keys used in a device (such as, a SEPP). The final security of the exchanged data over a transmission link cannot be stronger than the security of the encryption scheme. If
15 the security of the QKD fails, the dual secret key agreement procedure can guarantee that the security based on the classical cryptography still works and vice versa. An example of a SEPP using the dual secret key agreement will now be described with reference to Fig. 5.

[0082] Fig. 5 illustrates a schematic diagram of an example dual key agreement 500 according to some example embodiments of the present disclosure. In particular, Fig. 5
20 shows the example dual key agreement 500 where the first device 110 and the second device 120 are SEPPs in different PLMNs. As shown, at each of the two SEPPs, the master key 170 can be obtained from an N32-c initial handshake 510 between the two SEPPs. The quantum key 180 can be obtained from quantum key distribution 520, for example, provided by the KMEs of the first key management device 130 and the second key management device
25 140.

[0083] Then, the master key 170 and the quantum key 180 can be input into a generator 530 to generate a target key 535. In other words, the target key 535 may be generated based on the master key 170 and the quantum key 180. As mentioned, the generation of the target key 535 may employ any manner among various manners. For example, the target key 535
30 may be generated by performing an XOR operation between the master key 170 and the quantum key 180. As another example, the target key 535 may be generated from a hash function with the master key 170 and the quantum key 180 as input parameters. More

generally, any suitable generating manner can be used to combine the master key 170 and the quantum key 180 to generate the target key 535. Afterwards, the target key 535 can be forwarded by a TLS forwarder 540 to perform an N32-f ALS session key agreement 550 between the two SEPPs, so as to determine a session key 555. Subsequently, the session key 555 can be used by an encryptor 560 to encrypt plain data 570, resulting in the encrypted data 580 to be transmitted.

[0084] In other words, a SEPP can perform a generation operation using the master key 170 and the quantum key 180 to generate a “super master” key, which can guarantee forward secrecy and eavesdropping protection. For example, the quantum key 180 can be renewed every second and then be combined with the master key 170 obtained from classical cryptography to generate a new quantum-safe session key.

[0085] The example embodiments of the present disclosure can achieve technical benefits as follows. The security of a QKD based cryptographic solution is based on fundamental physical principles instead of computational hardness, and thus the security provided by a QKD based device can improve security against attack of quantum computers, new mathematical discoveries to break classical crypto algorithms, and massive parallel computing networks. In addition, the QKD is the only existing and practically implementable scheme that can offer secret key sharing in an information theoretic security. This can ensure long-term security guarantee of the keys used by a SEPP in a 5G network.

[0086] Moreover, the QKD can assure forward secrecy to a device, such as a SEPP. In particular, the QKD is able to provide immediate protection to data in the face of today’s brute force attacks, ensure that data with a long shelf life is protected against future attacks, and safeguard high-value data in a post-quantum computing world. Furthermore, with the QKD mechanism, two devices (such as, two SEPPs) can continuously refresh a shared secret (or key) between them, by distribution of a shared key encoding information in quantum states, which blocks a third party from eavesdropping.

[0087] Fig. 6 illustrates a flowchart of an example method 600 in accordance with some example embodiments of the present disclosure. In some example embodiments, the method 600 can be implemented at a device in a communication network, such as the first device 110 as shown in Fig. 1. Additionally or alternatively, the method 600 can also be implemented at other devices shown in Fig. 1, for example, at the second device 120. In some other example embodiments, the method 600 may be implemented at devices not

shown in Fig. 1. For the purpose of discussion, the method 600 will be described with reference to Fig. 1 as performed by the first device 110 without loss of generality.

[0088] At block 610, the first device 110 determines a master key with a second device 120 for an encrypted communication between the first device 110 and the second device 120.

5 At block 620, the first device 110 obtains a quantum key and a key identifier of the quantum key from a first key management device associated with the first device 110. The quantum key and the key identifier are shared between the first key management device and a second key management device associated with the second device 120 based on a quantum key distribution protocol. At block 630, the first device 110 transmits the key identifier to the
10 second device 120, for performing the encrypted communication with the second device 120 using the master key and the quantum key.

[0089] In some example embodiments, obtaining the quantum key and the key identifier comprises: transmitting a request to the first key management device for requesting the quantum key, the request comprising a device identifier of the second device 120; and
15 receiving the quantum key and the key identifier from the first key management device.

[0090] In some example embodiments, transmitting the key identifier to the second device 120 comprises: transmitting the key identifier as part of a key agreement and parameter exchange procedure between the first device 110 and the second device 120.

[0091] In some example embodiments, performing the encrypted communication
20 comprises: obtaining a target key based on the master key and the quantum key; and performing the encrypted communication using the target key.

[0092] In some example embodiments, obtaining the target key comprises at least one of: combining the master key and the quantum key mathematically; and performing a hash function with the master key and the quantum key as input parameters.

25 [0093] In some example embodiments, the first device 110 comprises a first SEPP for a first public land mobile network, the second device 120 comprises a second SEPP for a second public land mobile network, and the key identifier is transmitted across a N32-c interface between the first SEPP and the second SEPP.

[0094] In some example embodiments, the quantum key comprises a true random number
30 generated by a quantum random number generator.

[0095] Fig. 7 illustrates a flowchart of another example method 700 in accordance with

some example embodiments of the present disclosure. In some example embodiments, the method 700 can be implemented at a device in a communication network, such as the second device 120 as shown in Fig. 1. Additionally or alternatively, the method 700 can also be implemented at other devices shown in Fig. 1, for example, at the first device 110. In some
5 other example embodiments, the method 700 may be implemented at devices not shown in Fig. 1. For the purpose of discussion, the method 700 will be described with reference to Fig. 1 as performed by the second device 120 without loss of generality.

[0096] At block 710, the second device 120 determines a master key with a first device 110 for an encrypted communication between the first device 110 and the second device 120.

10 At block 720, the second device 120 receives a key identifier of a quantum key from the first device 110. The quantum key and the key identifier being shared between a first key management device associated with the first device 110 and a second key management device associated with the second device 120 based on a quantum key distribution protocol. At block 730, the second device 120 obtains the quantum key from the second key
15 management device based on the key identifier, for performing the encrypted communication with the first device 110 using the master key and the quantum key.

[0097] In some example embodiments, obtaining the quantum key comprises: transmitting a request to the second key management device for requesting the quantum key, the request comprising the key identifier and a device identifier of the first device 110; and receiving
20 the quantum key from the second key management device.

[0098] In some example embodiments, receiving the key identifier from the first device 110 comprises: receiving the key identifier as part of a key agreement and parameter exchange procedure between the first device 110 and the second device 120.

[0099] In some example embodiments, performing the encrypted communication
25 comprises: obtaining a target key based on the master key and the quantum key; and performing the encrypted communication using the target key.

[00100] In some example embodiments, obtaining the target key comprises at least one of: combining the master key and the quantum key mathematically; and performing a hash function with the master key and the quantum key as input parameters.

30 [00101] In some example embodiments, the first device 110 comprises a first SEPP for a first public land mobile network, the second device 120 comprises a second SEPP for a

second public land mobile network, and the key identifier is received across a N32-c interface between the first SEPP and the second SEPP.

[00102] In some example embodiments, the quantum key comprises a true random number generated by a quantum random number generator.

- 5 [00103] In some example embodiments, an apparatus capable of performing any of the method 600 (for example, the first device 110) may comprise means for performing the respective steps of the method 600. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

- 10 [00104] In some example embodiments, the apparatus comprises means for determining, at a first device, a master key with a second device for an encrypted communication between the first device and the second device; means for obtaining a quantum key and a key identifier of the quantum key from a first key management device associated with the first device, the quantum key and the key identifier being shared between the first key management device and a second key management device associated with the second device
15 based on a quantum key distribution protocol; and means for transmitting the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

- [00105] In some example embodiments, the means for obtaining the quantum key and the key identifier comprises: means for transmitting a request to the first key management device
20 for requesting the quantum key, the request comprising a device identifier of the second device; and means for receiving the quantum key and the key identifier from the first key management device.

- [00106] In some example embodiments, the means for transmitting the key identifier to the second device comprises: means for transmitting the key identifier as part of a key agreement
25 and parameter exchange procedure between the first device and the second device.

[00107] In some example embodiments, performing the encrypted communication comprises: obtaining a target key based on the master key and the quantum key; and performing the encrypted communication using the target key.

- [00108] In some example embodiments, obtaining the target key comprises at least one of:
30 combining the master key and the quantum key mathematically; and performing a hash function with the master key and the quantum key as input parameters.

[00109] In some example embodiments, the first device comprises a first security edge protection proxy for a first public land mobile network, the second device comprises a second security edge protection proxy for a second public land mobile network, and the key identifier is transmitted across a N32-c interface between the first security edge protection proxy and the second security edge protection proxy.

[00110] In some example embodiments, the quantum key comprises a true random number generated by a quantum random number generator.

[00111] In some example embodiments, an apparatus capable of performing any of the method 700 (for example, the second device 120) may comprise means for performing the respective steps of the method 700. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[00112] In some example embodiments, the apparatus comprises: means for determining, at a second device, a master key with a first device for an encrypted communication between the first device and the second device; means for receiving a key identifier of a quantum key from the first device, the quantum key and the key identifier being shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol; and means for obtaining the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

[00113] In some example embodiments, the means for obtaining the quantum key comprises: means for transmitting a request to the second key management device for requesting the quantum key, the request comprising the key identifier and a device identifier of the first device; and means for receiving the quantum key from the second key management device.

[00114] In some example embodiments, the means for receiving the key identifier from the first device comprises: means for receiving the key identifier as part of a key agreement and parameter exchange procedure between the first device and the second device.

[00115] In some example embodiments, performing the encrypted communication comprises: obtaining a target key based on the master key and the quantum key; and performing the encrypted communication using the target key.

[00116] In some example embodiments, obtaining the target key comprises at least one of:

combining the master key and the quantum key mathematically; and performing a hash function with the master key and the quantum key as input parameters.

[00117] In some example embodiments, the first device comprises a first security edge protection proxy for a first public land mobile network, the second device comprises a second security edge protection proxy for a second public land mobile network, and the key identifier is received across a N32-c interface between the first security edge protection proxy and the second security edge protection proxy.

[00118] In some example embodiments, the quantum key comprises a true random number generated by a quantum random number generator.

[00119] Fig. 8 is a simplified block diagram of a device 800 that is suitable for implementing example embodiments of the present disclosure. The device 800 may be provided to implement the communication device, for example the first device 110, the second device 120, the first key management device 130, the second key management device 140, the first network function 150, and the second network function 160 as shown in Fig. 1. As shown, the device 800 includes one or more processors 810, one or more memories 820 coupled to the processor 810, and one or more communication modules 840 coupled to the processor 810.

[00120] The communication module 840 is for bidirectional communications. The communication module 840 has at least one antenna to facilitate communication. The communication interface may represent any interface that is necessary for communication with other network elements.

[00121] The processor 810 may be of any type suitable to the local technical network and may include one or more of the following: general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multicore processor architecture, as non-limiting examples. The device 800 may have multiple processors, such as an application specific integrated circuit chip that is slaved in time to a clock which synchronizes the main processor.

[00122] The memory 820 may include one or more non-volatile memories and one or more volatile memories. Examples of the non-volatile memories include, but are not limited to, a Read Only Memory (ROM) 824, an electrically programmable read only memory (EPROM), a flash memory, a hard disk, a compact disc (CD), a digital video disk (DVD),

and other magnetic storage and/or optical storage. Examples of the volatile memories include, but are not limited to, a random access memory (RAM) 822 and other volatile memories that will not last in the power-down duration.

[00123] A computer program 830 includes computer executable instructions that are executed by the associated processor 810. The program 830 may be stored in the ROM 824. The processor 810 may perform any suitable actions and processing by loading the program 830 into the RAM 822.

[00124] The example embodiments of the present disclosure may be implemented by means of the program 830 so that the device 800 may perform any process of the disclosure as discussed with reference to Figs. 2 to 7. The example embodiments of the present disclosure may also be implemented by hardware or by a combination of software and hardware.

[00125] In some example embodiments, the program 830 may be tangibly contained in a computer readable medium which may be included in the device 800 (such as in the memory 820) or other storage devices that are accessible by the device 800. The device 800 may load the program 830 from the computer readable medium to the RAM 822 for execution. The computer readable medium may include any types of tangible non-volatile storage, such as ROM, EPROM, a flash memory, a hard disk, CD, DVD, and the like. Fig. 9 shows an example of the computer readable medium 900 in form of CD or DVD. The computer readable medium has the program 830 stored thereon.

[00126] Generally, various example embodiments of the present disclosure may be implemented in hardware or special purpose circuits, software, logic or any combination thereof. Some aspects may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device. While various aspects of example embodiments of the present disclosure are illustrated and described as block diagrams, flowcharts, or using some other pictorial representations, it is to be understood that the block, apparatus, system, technique or method described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

[00127] The present disclosure also provides at least one computer program product tangibly

stored on a non-transitory computer readable storage medium. The computer program product includes computer-executable instructions, such as those included in program modules, being executed in a device on a target real or virtual processor, to carry out the method 800 as described above with reference to Figs. 2-7. Generally, program modules
5 include routines, programs, libraries, objects, classes, components, data structures, or the like that perform particular tasks or implement particular abstract data types. The functionality of the program modules may be combined or split between program modules as desired in various example embodiments. Machine-executable instructions for program modules may be executed within a local or distributed device. In a distributed device,
10 program modules may be located in both local and remote storage media.

[00128] Program code for carrying out methods of the present disclosure may be written in any combination of one or more programming languages. These program codes may be provided to a processor or controller of a general purpose computer, special purpose computer, or other programmable data processing apparatus, such that the program codes,
15 when executed by the processor or controller, cause the functions/operations specified in the flowcharts and/or block diagrams to be implemented. The program code may execute entirely on a machine, partly on the machine, as a stand-alone software package, partly on the machine and partly on a remote machine or entirely on the remote machine or server.

[00129] In the context of the present disclosure, the computer program codes or related data
20 may be carried by any suitable carrier to enable the device, apparatus or processor to perform various processes and operations as described above. Examples of the carrier include a signal, computer readable medium, and the like.

[00130] The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable medium may include but not
25 limited to an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples of the computer readable storage medium would include an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory
30 (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing.

[00131] Further, while operations are depicted in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous.

5 Likewise, while several specific implementation details are contained in the above discussions, these should not be construed as limitations on the scope of the present disclosure, but rather as descriptions of features that may be specific to particular example embodiments. Certain features that are described in the context of separate embodiments may also be implemented in combination in a single example embodiment. Conversely,
10 various features that are described in the context of a single example embodiment may also be implemented in multiple example embodiments separately or in any suitable sub-combination.

[00132] Although the present disclosure has been described in languages specific to structural features and/or methodological acts, it is to be understood that the present
15 disclosure defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

I/We Claim:

1. A first device, comprising:

at least one processor; and

at least one memory storing computer program codes;

5 the at least one memory and the computer program codes are configured to, with the at least one processor, cause the first device to:

determine a master key with a second device for an encrypted communication between the first device and the second device;

10 obtain a quantum key and a key identifier of the quantum key from a first key management device associated with the first device, the quantum key and the key identifier being shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol; and

transmit the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

15

2. The first device of claim 1, wherein the first device is caused to obtain the quantum key and the key identifier by:

transmitting a request to the first key management device for requesting the quantum key, the request comprising a device identifier of the second device; and

20 receiving the quantum key and the key identifier from the first key management device.

3. The first device of claim 1, wherein the first device is caused to transmit the key identifier to the second device by:

25 transmitting the key identifier as part of a key agreement and parameter exchange procedure between the first device and the second device.

4. The first device of claim 1, wherein the first device is caused to perform the encrypted communication by:

30 obtaining a target key based on the master key and the quantum key; and performing the encrypted communication using the target key.

5. The first device of claim 4, wherein the first device is caused to obtain the target key by at least one of:

combining the master key and the quantum key mathematically; and

performing a hash function with the master key and the quantum key as input parameters.

6. The first device of claim 1, wherein:

the first device comprises a first security edge protection proxy for a first public land mobile network,

the second device comprises a second security edge protection proxy for a second public land mobile network, and

the key identifier is transmitted across a N32-c interface between the first security edge protection proxy and the second security edge protection proxy.

7. The first device of claim 1, wherein the quantum key comprises a true random number generated by a quantum random number generator.

8. A second device, comprising:

at least one processor; and

at least one memory storing computer program codes;

the at least one memory and the computer program codes are configured to, with the at least one processor, cause the second device to:

determine a master key with a first device for an encrypted communication between the first device and the second device;

receive a key identifier of a quantum key from the first device, the quantum key and the key identifier being shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol; and

obtain the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

9. The second device of claim 8, wherein the second device is caused to obtain

the quantum key by:

transmitting a request to the second key management device for requesting the quantum key, the request comprising the key identifier and a device identifier of the first device; and

5 receiving the quantum key from the second key management device.

10. The second device of claim 8, wherein the second device is caused to receive the key identifier from the first device by:

receiving the key identifier as part of a key agreement and parameter exchange
10 procedure between the first device and the second device.

11. The second device of claim 8, wherein the second device is caused to perform the encrypted communication by:

obtaining a target key based on the master key and the quantum key; and
15 performing the encrypted communication using the target key.

12. The second device of claim 11, wherein the second device is caused to obtain the target key by at least one of:

combining the master key and the quantum key mathematically; and
20 performing a hash function with the master key and the quantum key as input parameters.

13. The second device of claim 8, wherein:

the first device comprises a first security edge protection proxy for a first public land
25 mobile network,

the second device comprises a second security edge protection proxy for a second public land mobile network, and

the key identifier is received across a N32-c interface between the first security edge protection proxy and the second security edge protection proxy.

30

14. The second device of claim 8, wherein the quantum key comprises a true random number generated by a quantum random number generator.

15. A method, comprising:

determining, at a first device, a master key with a second device for an encrypted communication between the first device and the second device;

obtaining a quantum key and a key identifier of the quantum key from a first key management device associated with the first device, the quantum key and the key identifier being shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol; and

transmitting the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

10

16. The method of claim 15, wherein obtaining the quantum key and the key identifier comprises:

transmitting a request to the first key management device for requesting the quantum key, the request comprising a device identifier of the second device; and

receiving the quantum key and the key identifier from the first key management device.

15

17. The method of claim 15, wherein transmitting the key identifier to the second device comprises:

transmitting the key identifier as part of a key agreement and parameter exchange procedure between the first device and the second device.

20

18. The method of claim 15, wherein performing the encrypted communication comprises:

obtaining a target key based on the master key and the quantum key; and performing the encrypted communication using the target key.

25

19. The method of claim 18, wherein obtaining the target key comprises at least one of:

combining the master key and the quantum key mathematically; and

30

performing a hash function with the master key and the quantum key as input parameters.

20. The method of claim 15, wherein:

the first device comprises a first security edge protection proxy for a first public land mobile network,

5 the second device comprises a second security edge protection proxy for a second public land mobile network, and

the key identifier is transmitted across a N32-c interface between the first security edge protection proxy and the second security edge protection proxy.

10 21. The method of claim 15, wherein the quantum key comprises a true random number generated by a quantum random number generator.

22. A method, comprising:

determining, at a second device, a master key with a first device for an encrypted communication between the first device and the second device;

15 receiving a key identifier of a quantum key from the first device, the quantum key and the key identifier being shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol; and

20 obtaining the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

23. The method of claim 22, wherein obtaining the quantum key comprises:

25 transmitting a request to the second key management device for requesting the quantum key, the request comprising the key identifier and a device identifier of the first device; and

receiving the quantum key from the second key management device.

30 24. The method of claim 22, wherein receiving the key identifier from the first device comprises:

receiving the key identifier as part of a key agreement and parameter exchange procedure between the first device and the second device.

25. The method of claim 22, wherein performing the encrypted communication comprises:

obtaining a target key based on the master key and the quantum key; and
performing the encrypted communication using the target key.

5

26. The method of claim 25, wherein obtaining the target key comprises at least one of:

combining the master key and the quantum key mathematically; and
performing a hash function with the master key and the quantum key as input
parameters.

10

27. The method of claim 22, wherein:

the first device comprises a first security edge protection proxy for a first public land mobile network,

15

the second device comprises a second security edge protection proxy for a second public land mobile network, and

the key identifier is received across a N32-c interface between the first security edge protection proxy and the second security edge protection proxy.

20

28. The method of claim 22, wherein the quantum key comprises a true random number generated by a quantum random number generator.

29. An apparatus, comprising:

means for determining, at a first device, a master key with a second device for an encrypted communication between the first device and the second device;

25

means for obtaining a quantum key and a key identifier of the quantum key from a first key management device associated with the first device, the quantum key and the key identifier being shared between the first key management device and a second key management device associated with the second device based on a quantum key distribution protocol; and

30

means for transmitting the key identifier to the second device, for performing the encrypted communication with the second device using the master key and the quantum key.

30. An apparatus, comprising:

means for determining, at a second device, a master key with a first device for an encrypted communication between the first device and the second device;

5 means for receiving a key identifier of a quantum key from the first device, the quantum key and the key identifier being shared between a first key management device associated with the first device and a second key management device associated with the second device based on a quantum key distribution protocol; and

10 means for obtaining the quantum key from the second key management device based on the key identifier, for performing the encrypted communication with the first device using the master key and the quantum key.

31. A non-transitory computer readable medium storing program instructions for causing an apparatus to perform at least the method of any of claims 15-21 and 22-28.

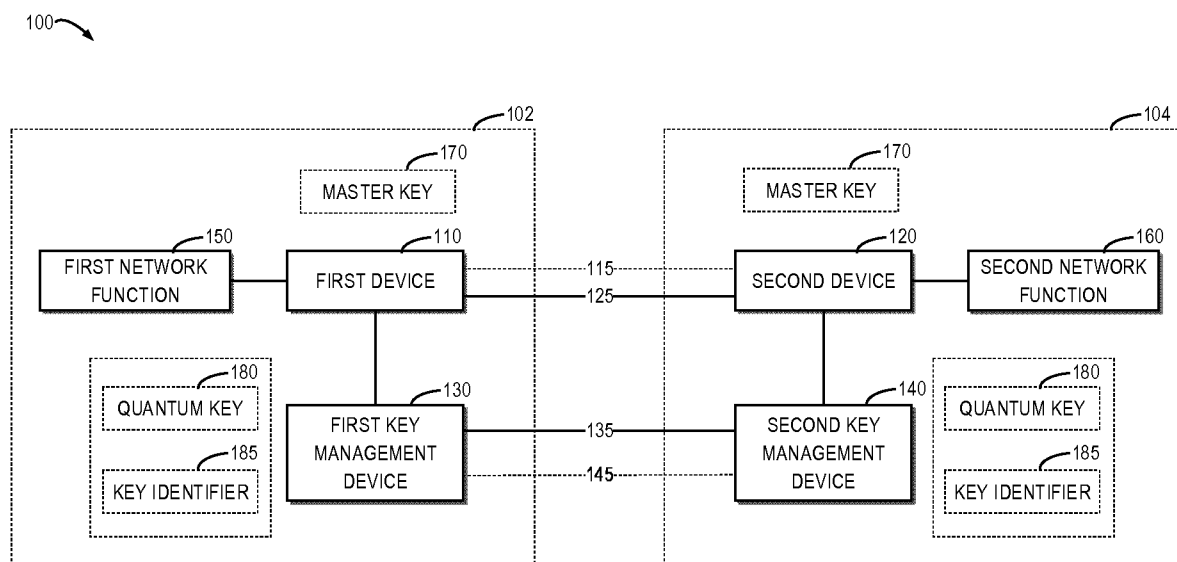


FIG. 1

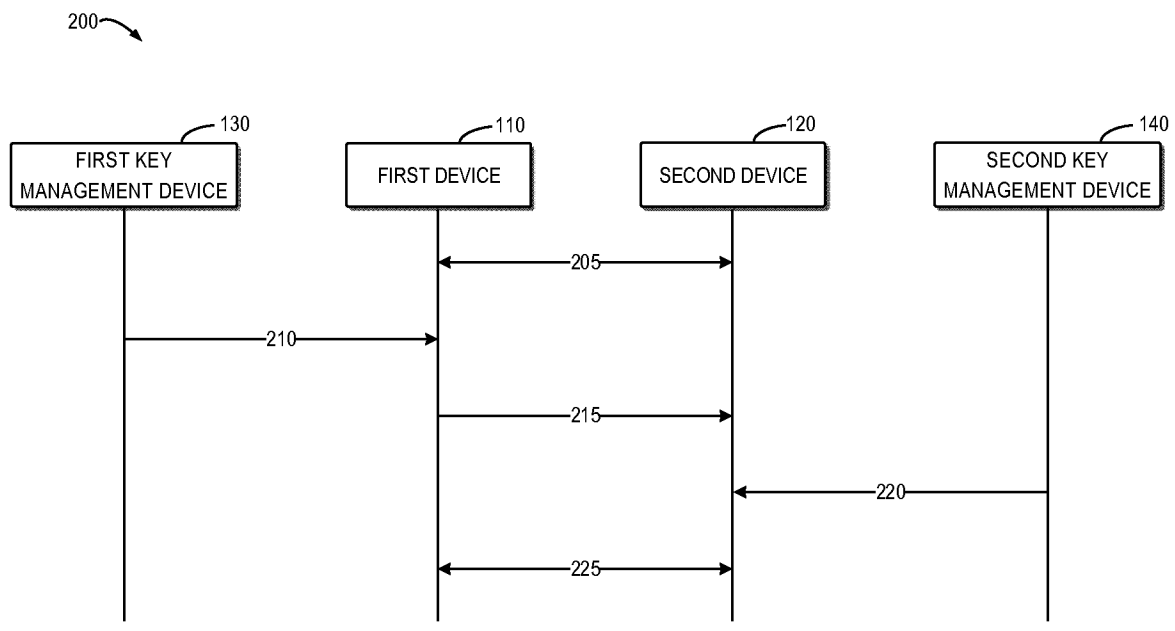


FIG. 2

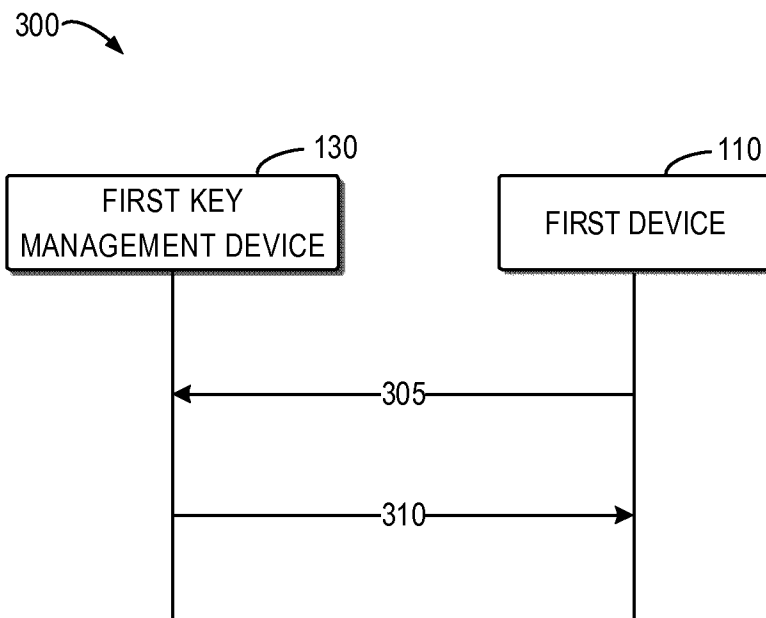


FIG. 3

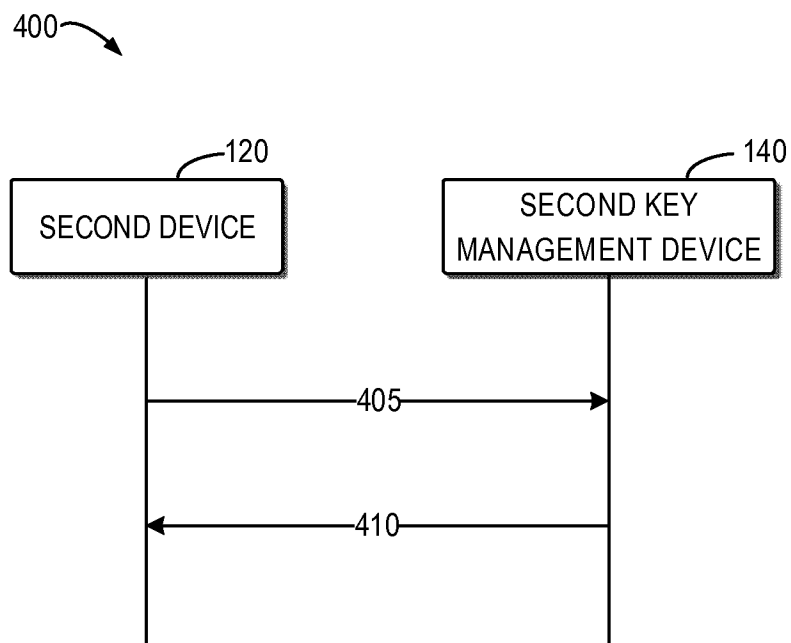


FIG. 4

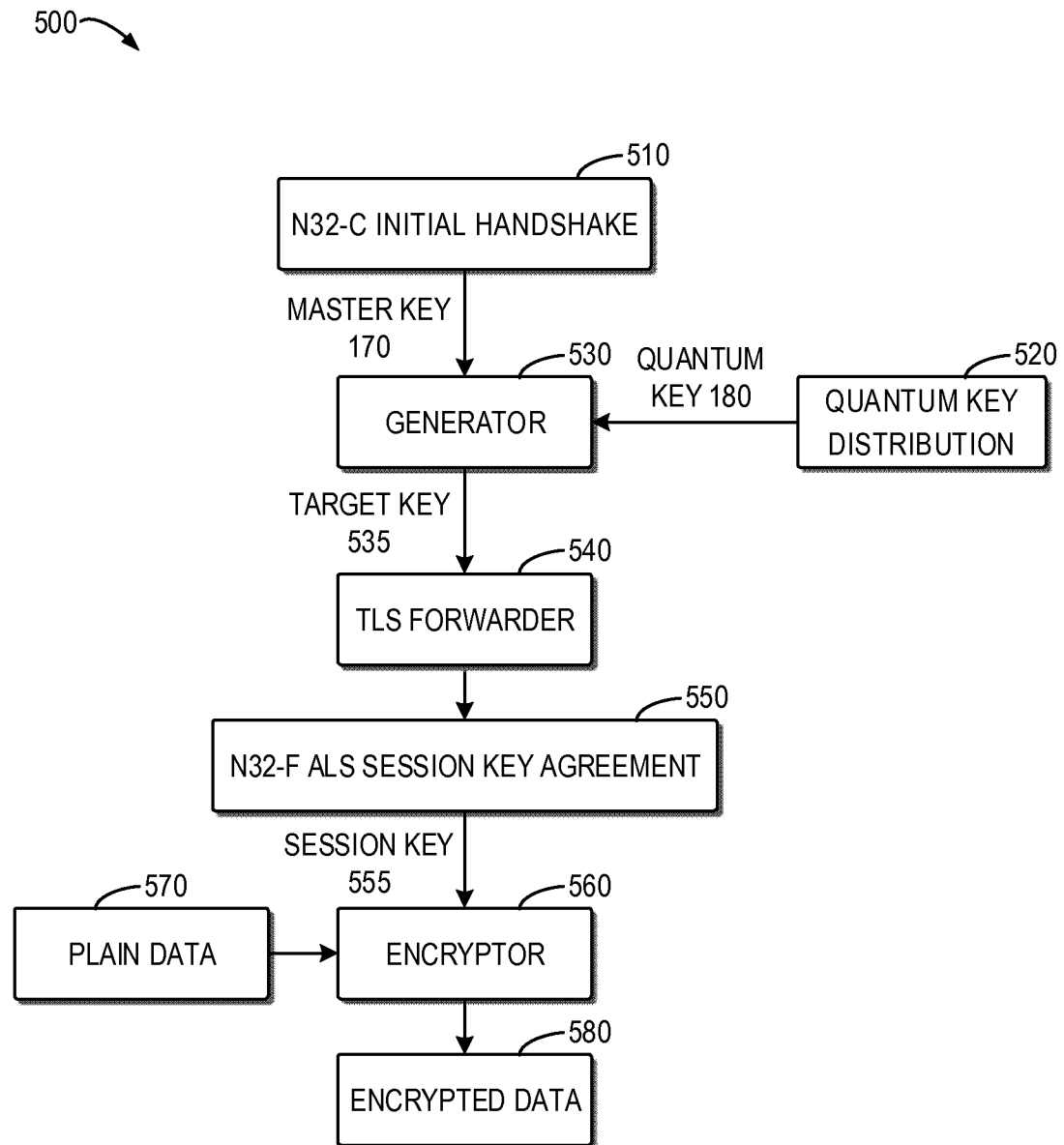


FIG. 5

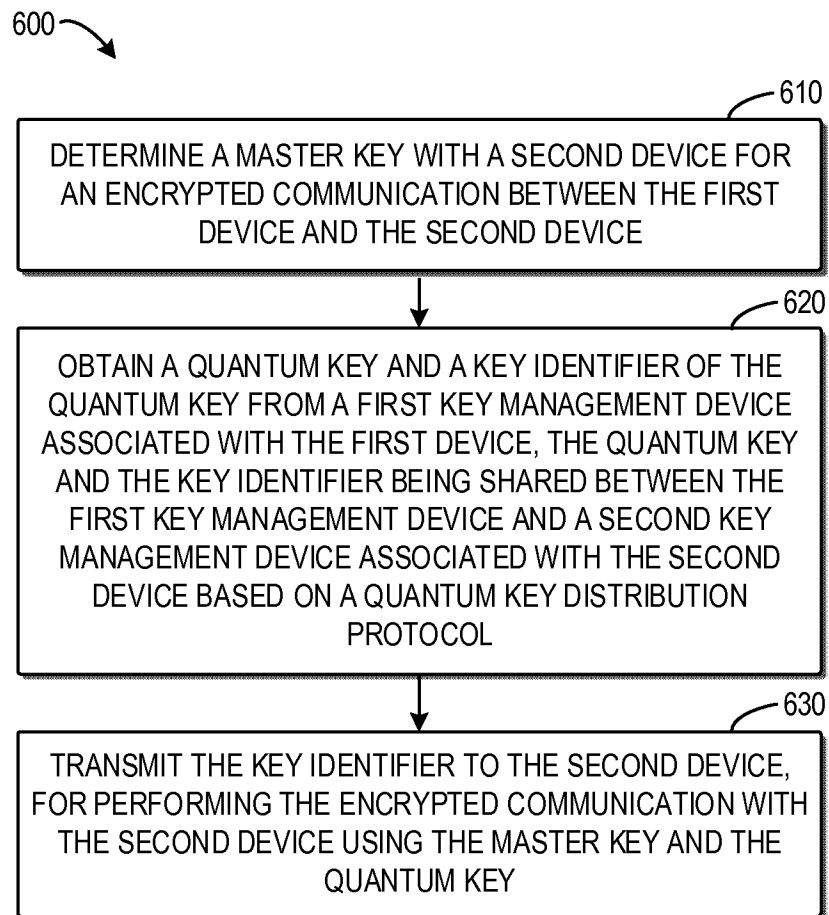


FIG. 6

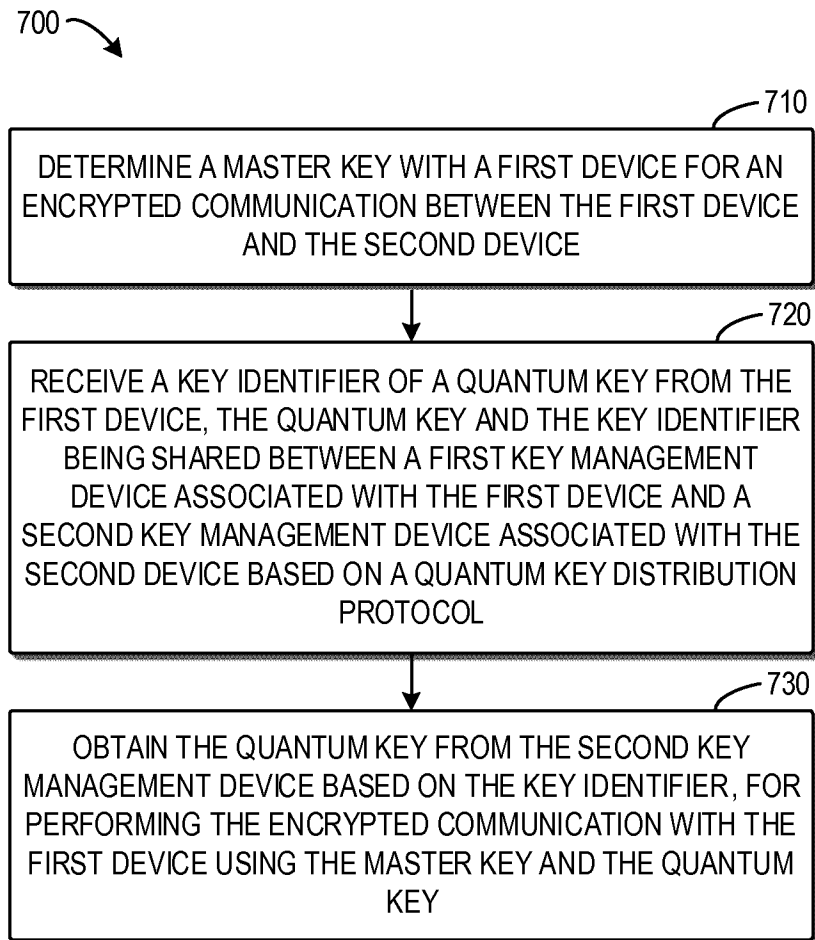


FIG. 7

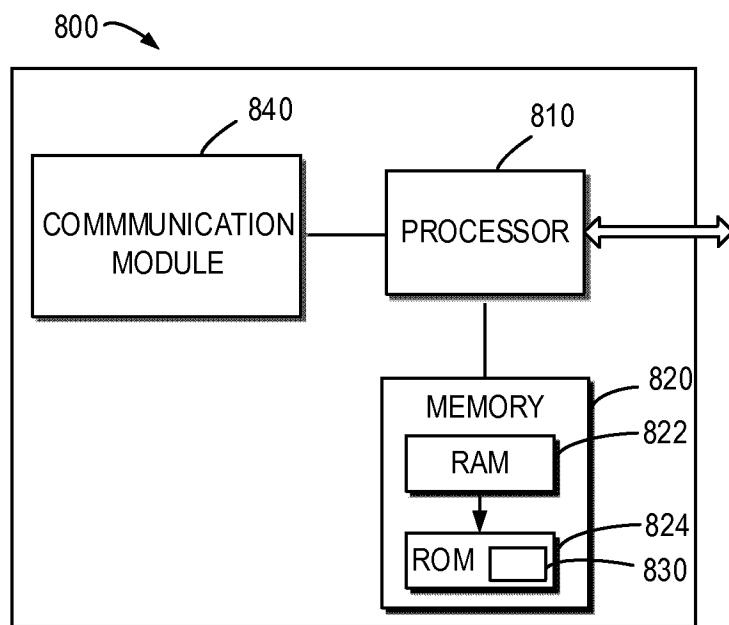


FIG. 8

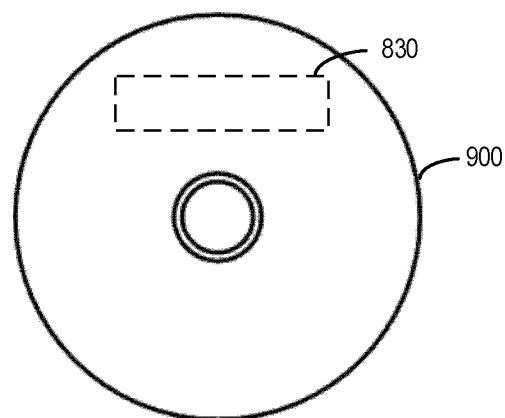


FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2020/050282

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base, and, where practicable, search terms used)

WPIAP, EPODOC, EPO-Internal full-text databases, Full-text translation databases from Asian languages, XP3GPP, XPAIP, XPCPVO, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPTK, COMPD, INSPEC, NPL, PRH-Internal, Internet, IEEE Xplore, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 3432509 A1 (ID QUANTIQUE S A [CH]) 23 January 2019 (23.01.2019) abstract; Fig. 2; paragraphs [0047]-[0056]	1-31
Y	US 2014331050 A1 (ARMSTRONG WARREN [AU] et al.) 06 November 2014 (06.11.2014) abstract; Fig. 1; paragraphs [0013]-[0018], [0021]-[0028]; claim 1	1-31
Y	US 2014219443 A1 (BRAINIS EDOUARD [BE] et al.) 07 August 2014 (07.08.2014) abstract; Figs. 2, 2a; paragraphs [0004], [0037], [0044]-[0050]	1-31
A	US 2017230173 A1 (CHOI JEONGWOON [KR]) 10 August 2017 (10.08.2017) the whole document	1-31

☒ Further documents are listed in the continuation of Box C.
☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"D" document cited by the applicant in the international application	"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
"E" earlier application or patent but published on or after the international filing date	"&" document member of the same patent family
"L" document which may throw doubts on priority claim(s) or which 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	

Date of the actual completion of the international search 13 October 2020 (13.10.2020)	Date of mailing of the international search report 15 October 2020 (15.10.2020)
Name and mailing address of the ISA/FI Finnish Patent and Registration Office FI-00091 PRH, FINLAND Facsimile No. +358 29 509 5328	Authorized officer Timo Laakso phone No. +358 29 509 5000

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2020/050282

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ETSI TS 133 501, V15.4.0. 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15) [online], May 2019, [retrieved on 2020-09-23]. Retrieved from < https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf > the whole document, in particular Sections 4.2, 13.2.2	1-31
A	DRAFT RECOMMENDATION ITU-T X.5GSEC-Q Security guidelines for applying quantum-safe algorithms in 5G systems [online], 2019-04-23, [retrieved on 2020-10-13]. Retrieved from < https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_95_Reno/Docs/S3-191159.zip > the whole document, in particular Appendix B.2	1-31

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2020/050282

EP 3432509 A1 23/01/2019 None

.....

US 2014331050 A1	06/11/2014	US 9698979 B2	04/07/2017
		EP 2697931 A1	19/02/2014
		EP 2697931 B1	13/12/2017
		WO 2012139174 A1	18/10/2012

.....

US 2014219443 A1 07/08/2014 US 9246674 B2 26/01/2016

		GB 201110290 D0	03/08/2011
		GB 2491896 A	19/12/2012
		WO 2012172080 A1	20/12/2012

.....

US 2017230173 A1 10/08/2017 US 10382198 B2 13/08/2019

		CN 107113166 A	29/08/2017
		CN 107113166 B	21/08/2020
		KR 20160051994 A	12/05/2016
		KR 101776137 B1	19/09/2017
		WO 2016068508 A1	06/05/2016

.....

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2020/050282

CLASSIFICATION OF SUBJECT MATTER

IPC
H04L 9/08 (2006.01)