



(12) **DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION**

(13) **A1**

(86) Date de dépôt PCT/PCT Filing Date: 2016/08/17
(87) Date publication PCT/PCT Publication Date: 2017/02/23
(85) Entrée phase nationale/National Entry: 2018/02/16
(86) N° demande PCT/PCT Application No.: US 2016/047398
(87) N° publication PCT/PCT Publication No.: 2017/031228
(30) Priorité/Priority: 2015/08/18 (CN201510509537.5)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01)
(71) Demandeur/Applicant:
ALIBABA GROUP HOLDING LIMITED, KY
(72) Inventeur/Inventor:
FU, YINGFANG, CN
(74) Agent: SMART & BIGGAR

(54) Titre : PROCEDE, APPAREIL ET SYSTEME D'AUTHENTIFICATION UTILISES DANS UN PROCESSUS DE DISTRIBUTION DE CLE QUANTIQUE
(54) Title: AUTHENTICATION METHOD, APPARATUS AND SYSTEM USED IN QUANTUM KEY DISTRIBUTION PROCESS

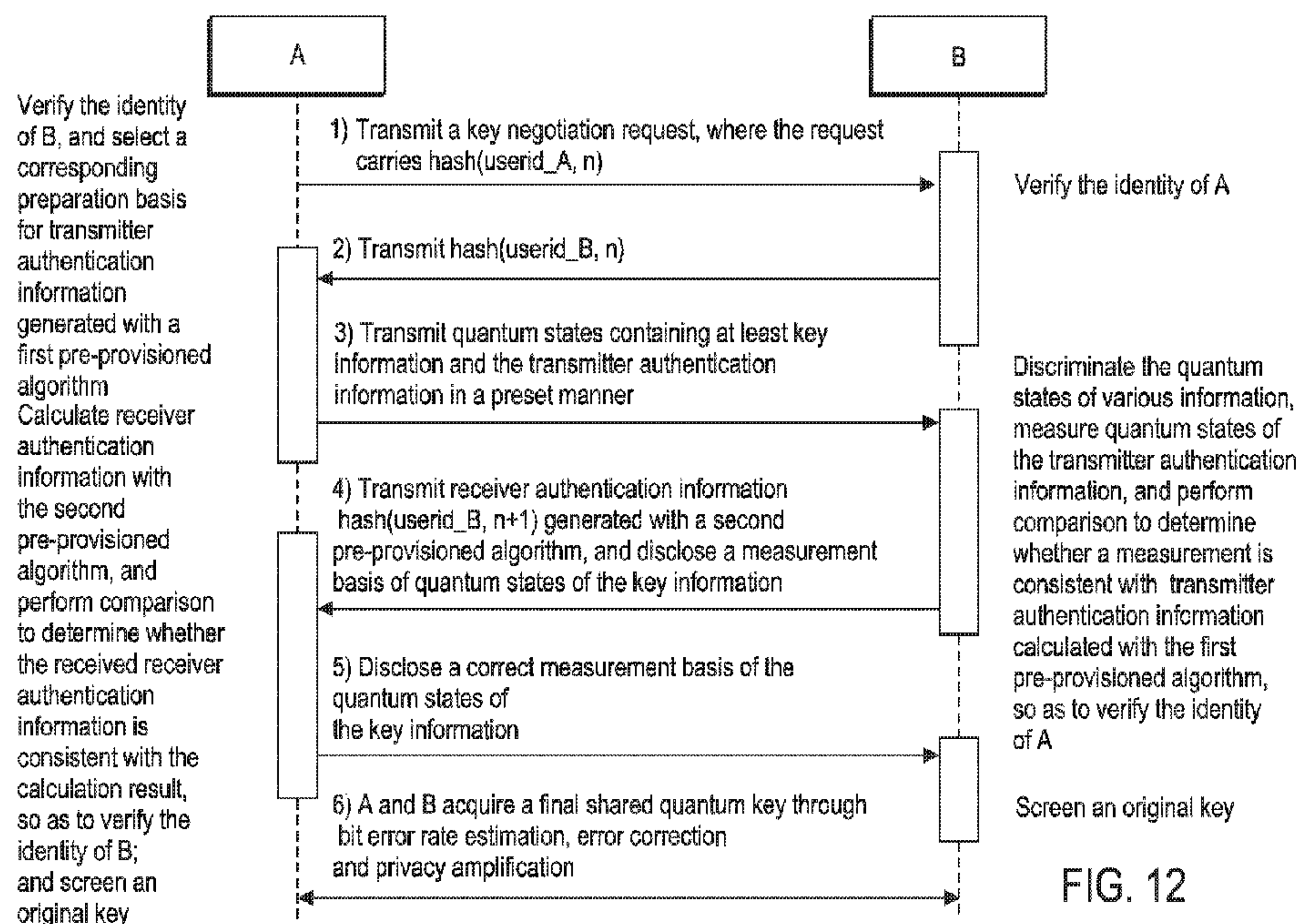


FIG. 12

(57) **Abrégé/Abstract:**

The present application discloses an authentication method used in a QKD process, and further discloses additional authentication methods and corresponding apparatuses, as well as an authentication system. The method comprises: selecting, by a transmitter according to a basis selection rule, a basis of preparation for transmitter authentication information that is generated with a first pre-provisioned algorithm and varies dynamically, and transmitting quantum states containing key information and the transmitter authentication information; and measuring, by a receiver, quantum states of the transmitter authentication information according to the basis selection rule, and ending the QKD process if a measurement result is inconsistent with corresponding information calculated with the first pre-provisioned algorithm.

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

(19) World Intellectual Property

Organization

International Bureau

(43) International Publication Date
23 February 2017 (23.02.2017)

(10) International Publication Number

WO 2017/031228 A1

(51) International Patent Classification:

H04L 29/06 (2006.01)

(21) International Application Number:

PCT/US2016/047398

(22) International Filing Date:

17 August 2016 (17.08.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201510509537.5 18 August 2015 (18.08.2015)

CN

(71) Applicant: ALIBABA GROUP HOLDING LIMITED

[—/US]; Fourth Floor, One Capital Place, P.O. Box 847,
George Town, Grand Cayman (KY).

(72) Inventor: FU, Yingfang; Alibaba Broup Legal Depart-

ment, 5/f, Bulding 3, No. 969 West Wen Yi Road, Yu
Hang District, Hangzhou, 31121 (CN).

(74) Agent: MURABITO, Anthony, C.; Murabito Hao &

Barnes LLP, 2n. Market St., 3rd Floor, San Jose, CA
95113 (US).

(81) Designated States (unless otherwise indicated, for every

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

(84) Designated States (unless otherwise indicated, for every

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

Published:

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

(54) Title: AUTHENTICATION METHOD, APPARATUS AND SYSTEM USED IN QUANTUM KEY DISTRIBUTION PROCESS

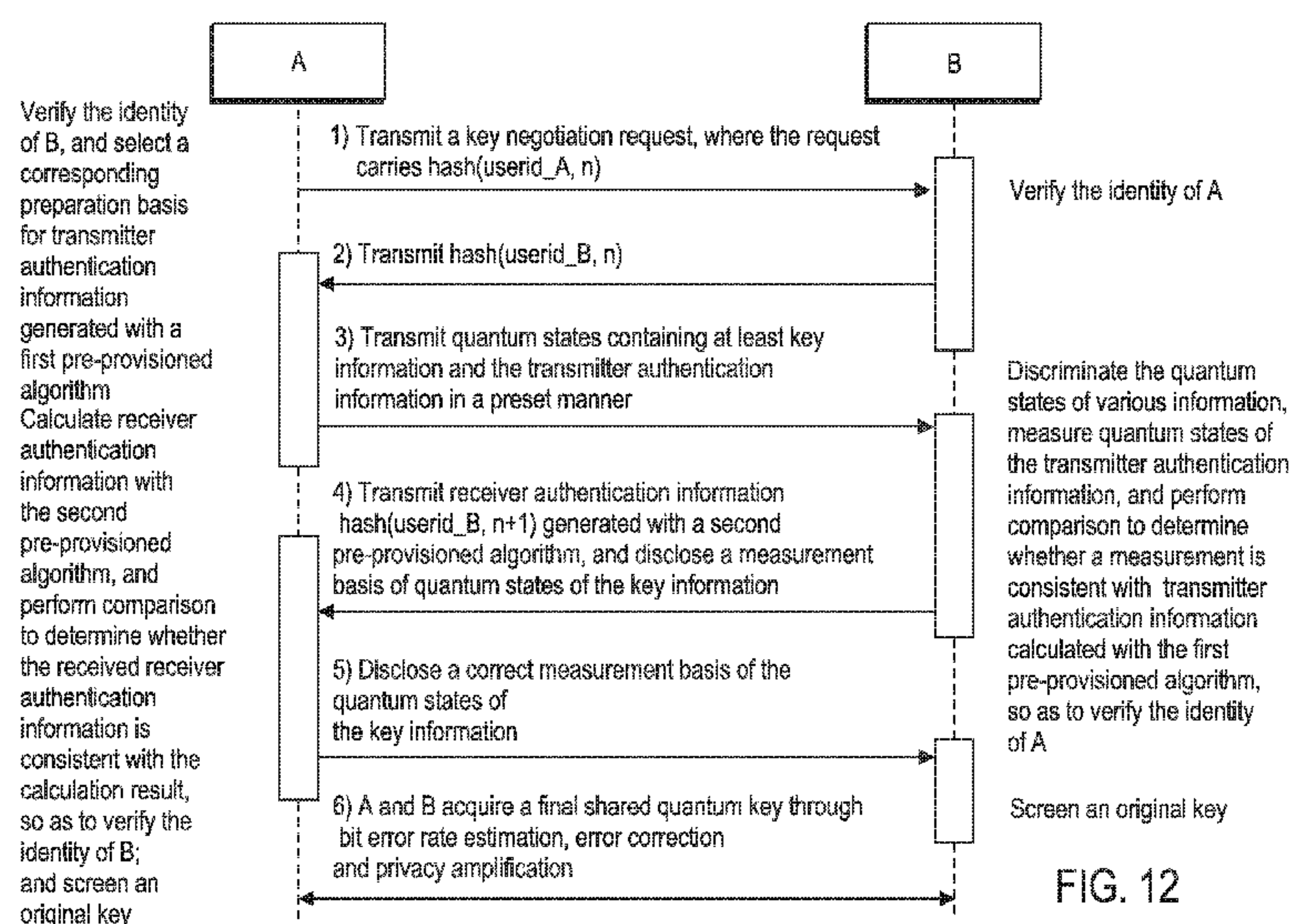


FIG. 12

(57) **Abstract:** The present application discloses an authentication method used in a QKD process, and further discloses additional authentication methods and corresponding apparatuses, as well as an authentication system. The method comprises: selecting, by a transmitter according to a basis selection rule, a basis of preparation for transmitter authentication information that is generated with a first pre-provisioned algorithm and varies dynamically, and transmitting quantum states containing key information and the transmitter authentication information; and measuring, by a receiver, quantum states of the transmitter authentication information according to the basis selection rule, and ending the QKD process if a measurement result is inconsistent with corresponding information calculated with the first pre-provisioned algorithm.

WO 2017/031228 A1

AUTHENTICATION METHOD, APPARATUS AND SYSTEM USED IN QUANTUM KEY DISTRIBUTION PROCESS

Claim of Priority

[0001] The present application claims the benefit of Chinese Patent Application No. 201510509537.5 filed August 18, 2015 to Fu, Yingfang, which is incorporated by reference and in its entirety.

Technical Field

[0002] The present application relates to the technical field of authentication, in particular to an authentication method for a quantum key distribution (QKD) process. The present invention further relates to an authentication system for the QKD process.

Background

[0003] Authentication is an important part of ensuring network security; effective authentication can guarantee the authenticity of two communication parties, the integrity of a message and the reliability of a source, and can also protect information from attacks by illegal parties through such means as forgery, modification, and delay. Both private key cryptography mechanisms and public key cryptography mechanisms are commonly used in cryptography to ensure the security, integrity, and non-repudiation of identity information in communications, and to resist identity spoofing attacks. Quantum cryptography is a joint product of quantum mechanics and cryptography, and has proven to provide increased security and eavesdropper detectability. Quantum cryptography employs the fundamentals of quantum mechanics and is irrespective of the computing power and storage capacity of attackers. However, conventional QKD protocols do not provide an effective authentication mechanism, so a QKD process may still be subject to spoofing attacks, man-in-the-middle attacks or distributed denial of service (DDoS) attacks.

[0004] In view of the foregoing problems, the prior art provides the following two solutions:

i. M.Dusek et al. is one solution that is characterized by a belief that it is unnecessary to authenticate all pre-determined information in a quantum communication process. According

to M.Dusek, only pre-determined information that affects the correct determination of the error rate of quantum states should be authenticated, and all other pre-determined information does not need to be authenticated. As a result, M.Dusek proposes a quantum authentication protocol in combination with a pre-determined message authentication algorithm, and the essence of the protocol is to authenticate as few pre-determined messages as possible with a pre-determined authentication algorithm.

ii. Another proposed solution combines the BB84 protocol with authentication. This protocol is different from the original BB84 protocol in that some bits in a randomly sent quantum bit string are set as specific authentication bits, the specific positions of the authentication bits are determined by an authentication key, authentication between two communication parties is achieved with measurement bases and polarization states of photons represented by bits of the authentication bits, and quantum states information of the authentication bits cannot be randomly sent and should be determined by an authentication key shared between the two parties according to a specific rule. A transmitter and a receiver set a portion of the shared quantum key acquired by each negotiation as an authentication key so as to realize the dynamic update of the authentication key.

[0005] The foregoing two solutions can improve the security of a QKD process to some extent because both adopt an authentication mechanism, however, they each have certain defects:

i. For the M.Dusek solution, the number of authentication keys pre-provisioned between two communication parties is limited, and the solution still adopts a pre-determined authentication technology without taking full advantage of quantum technology, so the solution inherits the risk of hacking and is vulnerable to spoofing attacks, man-in-the-middle attacks and DDoS attacks.

ii. For the BB84 protocol with authentication, although authentication information is sent in the form of quantum states to improve the security of key distribution, as this technical solution requires choosing a portion of the shared quantum key acquired by each negotiation as the authentication key, that portion of the shared quantum key can no longer be used for service data encryption, and quantum key resources are wasted.

Summary

[0006] Embodiments of the present application provide an authentication method used in a QKD process, which not only provides a new idea for performing dynamic authentication in a QKD process, but can also effectively solve the issues of vulnerability and quantum key resource waste. The embodiments of the present application further provide another two authentication methods and corresponding apparatuses used in a QKD process, and an authentication system used in a QKD process.

[0007] The present application provides an authentication method used in a QKD process, where the method is implemented on a quantum communication transmitter device and a quantum communication receiver device participating in a QKD process. In an embodiment, the method comprises:

selecting, by the transmitter, a basis of preparation for authenticating the transmitter identity information according to a basis selection rule agreed upon with the receiver, and transmitting quantum states containing at least key information and the transmitter authentication information in a preset manner, wherein the transmitter authentication information is generated with a first pre-provisioned algorithm; and

filtering (or differentiating), by the receiver, the received quantum states of various information in the preset manner, and measuring the received quantum states of the transmitter authentication information according to the basis selection rule, and, if the measurement result is consistent with the transmitter authentication information calculated following the first pre-provisioned algorithm, determining that the transmitter is authenticated; otherwise, determining that the transmitter is not authenticated and ending the QKD process; wherein

the transmitter authentication information generated with the first pre-provisioned algorithm varies dynamically in different QKD processes initiated towards the receiver.

In an embodiment, the following operations are performed after determining (in the receiver) that the transmitter is authenticated:

generating, by the receiver, receiver authentication information with a second pre-provisioned algorithm, and transmitting the receiver authentication information; and

calculating, in the transmitter, receiver authentication information with the second

pre-provisioned algorithm, and, when the received receiver authentication information is consistent with the calculation result, determining that the receiver is authenticated; otherwise, determining that the receiver is not authenticated and ending the QKD process.

[0008] In an embodiment, the receiver further performs the following operations after determining that the transmitter is authenticated:

randomly selecting a measurement basis to measure the received quantum states of the key information, and disclosing the measurement basis through a pre-determined channel; and

correspondingly, after determining that the receiver is authenticated, the transmitter performs the following operations:

determining a correct measurement basis of the quantum states of the key information, and screening an original key; and

disclosing the correct measurement basis of the quantum states of the key information through the pre-determined channel; and

correspondingly, after the step of disclosing, by the transmitter, the correct measurement basis of the quantum states of the key information, the following operations are performed:

screening, by the receiver, an original key; and

acquiring, by the transmitter and the receiver, a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0009] In an embodiment, the first pre-provisioned algorithm comprises: calculating the transmitter authentication information according to transmitter identification information and a synchronously changing parameter according to a preset policy by both the transmitter and the receiver; and wherein the transmitter identification information on the receiver side is pre-provisioned or sent to the receiver by the transmitter through a pre-determined channel.

[0010] In an embodiment, before selecting, by a transmitter, a basis of preparation for transmitter authentication information according to the basis selection rule agreed upon with a receiver, the following operation is performed:

performing, by both the transmitter and the receiver, authentication for the peer device of the other party with the synchronously changing parameter according to the preset policy during a request initiating interaction carried out through the pre-determined channel, and not

initiating the QKD process if either device fails the authentication.

[0011] In an embodiment, the second pre-provisioned algorithm comprises: calculating the receiver authentication information according to receiver identification information and a variant of the synchronously changing parameter according to a preset policy by both the transmitter and the receiver; wherein the receiver identification information on the transmitter side is pre-provisioned or sent to the transmitter by the receiver through a pre-determined channel.

[0012] In an embodiment, the variant of the synchronously changing parameter according to the preset policy comprises the parameter itself, or a result obtained from processing the parameter with a preset mathematical transformation method.

[0013] In an embodiment, the synchronously changing parameter according to the preset policy of both the transmitter and the receiver comprises the number of times the transmitter and the receiver perform the QKD processes.

[0014] In an embodiment, calculating the authentication information comprises calculating the corresponding authentication information with a hash function.

[0015] In an embodiment, transmitting quantum states containing at least key information and the transmitter authentication information in a preset manner comprises transmitting quantum states of control information and data information with respectively different wavelengths in a preset information format, wherein the data information comprises the key information and the transmitter authentication information.

[0016] In an embodiment, the preset information is formatted such that the authentication information and the key information use respective control information as prefixes.

[0017] In an embodiment, a wavelength carrying quantum states of the control information used as the prefix of the authentication information is different from a wavelength carrying quantum states of the control information used as the prefix of the key information.

[0018] In an embodiment, the preset information is formatted such that the control information used as the prefix of the authentication information and the control information used as the prefix of the key information use different codes, respectively; the different codes are preset by the transmitter and the receiver or determined via negotiation through a pre-determined channel; and a basis for preparing or measuring quantum states of control information is preset by the

transmitter and the receiver or determined via negotiation through the pre-determined channel.

[0019] In an embodiment, the preset information is formatted so that the authentication information and the key information use common control information as a prefix, and the length of the authentication information between the control information and the key information is preset by the transmitter and the receiver or determined via negotiation through a pre-determined channel.

[0020] In addition, the present application further provides an authentication method used in a QKD process, wherein the method is implemented on a quantum communication transmitter device participating in a QKD process, with the method comprising:

- generating transmitter authentication information with a first pre-provisioned algorithm;

- selecting a basis of preparation for the transmitter authentication information according to a basis selection rule agreed upon with a peer device participating in the QKD process; and

- transmitting quantum states containing at least key information and the transmitter authentication information to the peer device in a preset manner; wherein

- the transmitter authentication information generated with the first pre-provisioned algorithm varies dynamically in different QKD processes initiated towards the peer device.

[0021] In an embodiment, after transmitting quantum states containing at least key information and the transmitter authentication information to the peer device participating in the QKD process in a preset manner, the following operations are performed:

- receiving information returned by the peer device, wherein the information comprises at least receiver authentication information;

- calculating receiver authentication information with a second pre-provisioned algorithm; and

- determining whether the receiver authentication information received is consistent with the calculation result, and if so, then determining that the receiver is authenticated; otherwise, determining that the receiver is not authenticated and ending the QKD process.

[0022] In an embodiment, the information returned by the peer device not only comprises the receiver authentication information, but also comprises a measurement basis used for measuring quantum states of the key information; and

correspondingly, after determining that a receiver is authenticated, the following operations are performed:

determining a correct measurement basis of the quantum states of the key information, and screening an original key;

disclosing the correct measurement basis of the quantum states of the key information through a pre-determined channel; and

acquiring a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0023] In an embodiment, the first pre-provisioned algorithm comprises calculating the transmitter authentication information according to identification information of a host device and a synchronously changing parameter of the peer device according to a preset policy.

[0024] In an embodiment, the second pre-provisioned algorithm comprises calculating the receiver authentication information according to identification information of the peer device and a variant of a synchronously changing parameter of the peer device according to a preset policy.

[0025] In an embodiment, synchronously changing parameter of the peer device according to the preset policy comprises the number of times the QKD process is performed with the peer device.

[0026] In an embodiment, calculating the authentication information comprises calculating the corresponding authentication information with a hash function.

[0027] In an embodiment, transmitting quantum states containing at least key information and the transmitter authentication information in a preset manner comprises transmitting quantum states of control information and data information with respectively different wavelengths in a preset information format, wherein the data information comprises the key information and the transmitter authentication information.

[0028] In an embodiment, the preset information is formatted so that the authentication information and the key information use respective control information as prefixes.

[0029] In an embodiment, the preset information is formatted so that the authentication information and the key information use common control information as a prefix, and the length of the authentication information between the control information and the key

information is preset or determined via negotiation with the peer device through a pre-determined channel.

[0030] Correspondingly, the present application further provides an authentication apparatus used in a QKD process, wherein the apparatus is deployed on a quantum communication transmitter device participating in a QKD process, and the apparatus comprises:

a transmitter identity information generating unit, configured to generate transmitter authentication information with a first pre-provisioned algorithm, wherein the transmitter authentication information varies dynamically in different QKD processes initiated with a receiver;

a basis of preparation selection unit, configured to select a basis of preparation for the transmitter authentication information according to a basis selection rule agreed upon with a peer device participating in the QKD process; and

a quantum states transmitting unit, configured to transmit quantum states containing at least key information and the transmitter authentication information to the peer device in a preset manner.

[0031] In an embodiment, the apparatus further comprises:

a receiver identity information receiving unit, configured to receive information returned by the peer device after the quantum states transmitting unit completes the quantum states transmitting operation, wherein the information comprises at least receiver authentication information;

a receiver identity information calculation unit, configured to calculate receiver authentication information with a second pre-provisioned algorithm; and

a receiver authentication unit, configured to determine whether the receiver authentication information received is consistent with the calculation result, and if so, determine that the receiver is authenticated; otherwise, determine that the receiver is not authenticated and end the QKD process.

[0032] In an embodiment, the information received by the receiver identity information receiving unit not only comprises the receiver authentication information, but also comprises a measurement basis used by the peer device for measuring quantum states of the key information. According to these embodiments, the apparatus comprises:

an original key screening unit, configured to determine a correct measurement basis for the quantum states of the key information and to screen the original key after the receiver authentication unit determines that the receiver is authenticated;

a correct measurement basis disclosing unit, configured to disclose the correct measurement basis for the quantum states of the key information through a pre-determined channel; and

a shared quantum key generating unit, configured to acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0033] In an embodiment, the first pre-provisioned algorithm used by the transmitter identity information generating unit comprises calculating the transmitter authentication information according to identification information of a host device and a synchronously changing parameter of the peer device according to a preset policy.

[0034] In an embodiment, the second pre-provisioned algorithm used by the receiver identity information calculation unit comprises calculating the receiver authentication information according to identification information of the peer device and a variant of a synchronously changing parameter of the peer device according to a preset policy.

[0035] In an embodiment, the synchronously changing parameter that is used by the transmitter identity information generating unit and the receiver identity information calculation unit for calculation according to the preset policy comprises the number of times the QKD process is performed with the peer device.

[0036] In an embodiment, the transmitter identity information generating unit or the receiver identity information calculation unit is specifically configured to calculate the corresponding authentication information with a hash function.

[0037] In an embodiment, the quantum states transmitting unit is specifically configured to transmit quantum states of control information and data information with respectively different wavelengths in a preset information format, and the data information comprises the key information and the transmitter authentication information.

[0038] In an embodiment, the preset information format used by the quantum states transmitting unit is such that the authentication information and the key information use respective control information as prefixes.

[0039] In an embodiment, the preset information format used by the quantum states transmitting unit is such that the authentication information and the key information use common control information as a prefix, and the length of the authentication information between the control

information and the key information is preset or determined via negotiation with the peer device through a pre-determined channel.

[0040] In addition, the present application further provides an authentication method used in a QKD process, wherein the method is implemented on a quantum communication receiver device participating in a QKD process, with the method comprising:

receiving quantum states sent by a peer device participating in the QKD process, and differentiating the received quantum states of various information in the same preset manner as that of the peer device;

calculating transmitter authentication information with the same first pre-provisioned algorithm as that of the peer device;

selecting a measurement basis according to the same basis selection rule as that of the peer device, and measuring the received quantum states of transmitter authentication information; and

determining whether a measurement result is consistent with the calculated transmitter authentication information, and if so, determining that a transmitter is authenticated; otherwise, determining that the transmitter is not authenticated and ending the QKD process.

[0041] In an embodiment, the following operations may be performed after determining that a transmitter is authenticated:

generating receiver authentication information with the same second pre-provisioned algorithm as that of the peer device; and

transmitting the receiver authentication information to the peer device.

[0042] In an embodiment, the following operations may be performed after determining that a transmitter is authenticated:

randomly selecting a measurement basis to measure received quantum states of the key information, and disclosing the measurement basis through a pre-determined channel;

receiving a correct measurement basis of the quantum states of the key information sent by the peer device through the pre-determined channel; and

screening an original key, and acquiring a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0043] Correspondingly, the present application further provides an authentication apparatus

used in a QKD process, wherein the apparatus is deployed on a quantum communication receiver device participating in a QKD process, with the apparatus comprising:

a quantum states receiving and differentiating unit, configured to receive quantum states sent by a peer device participating in the QKD process, and to filter or differentiate the received quantum states of various information in the same preset manner as that of the peer device;

a transmitter identity information calculation unit, configured to calculate transmitter authentication information with the same first pre-provisioned algorithm as that of the peer device;

an identity information quantum states measurement unit, configured to select a measurement basis according to the same basis selection rule as that of the peer device, and measure received quantum states of transmitter authentication information; and

a transmitter authentication unit, configured to determine whether a measurement result is consistent with the calculated transmitter authentication information, and if so, determine that a transmitter is authenticated; and to determine that the transmitter is not authenticated and end the QKD process otherwise.

[0044] In an embodiment, the apparatus further comprises:

a receiver identity information generating unit, configured to generate receiver authentication information with the same second pre-provisioned algorithm as that of the peer device after the transmitter authentication unit determines that the transmitter is authenticated; and

a receiver identity information transmitting unit, configured to transmit the receiver authentication information to the peer device.

[0045] In an embodiment, the apparatus further comprises:

a key information quantum states measurement basis disclosing unit, configured to randomly select a measurement basis to measure received quantum states of key information, and disclose the measurement basis through a pre-determined channel after the transmitter authentication unit determines that the transmitter is authenticated;

a correct measurement basis receiving unit, configured to receive a correct measurement basis of the quantum states of the key information sent by the peer device through the pre-determined channel;

and

a screening and shared quantum key generating unit, configured to screen an original key and acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0046] In addition, the present application further provides an authentication system used in a QKD process, which comprises the authentication apparatus being deployed on a quantum communication transmitter device according to any of the foregoing parts, and the authentication apparatus being deployed on a quantum communication receiver device according to any of the foregoing parts.

[0047] Compared with the prior art, the present application has the following advantages:

According to the authentication method used in the QKD process provided in the present application, a transmitter selects, according to a basis selection rule agreed upon with a receiver, a basis of preparation of transmitter authentication information that is generated with a first pre-provisioned algorithm, and transmits quantum states containing at least key information and the transmitter authentication information in a preset manner; the receiver differentiates (filters) the received quantum states of various information in the preset manner, and measures the received quantum states of the transmitter authentication information according to the basis selection rule, and if a measurement result is consistent with transmitter authentication information calculated with the first pre-provisioned algorithm, determines that the transmitter is authenticated; and determines that the transmitter is not authenticated and ends the QKD process otherwise. In the above technical solution, the transmitter authentication information, which is sent by the transmitter in the form of quantum states and generated with the first pre-provisioned algorithm, varies dynamically in different QKD processes initiated towards the receiver, and the receiver verifies the received authentication information with the same pre-provisioned algorithm, so that dynamic authentication of a requestor is achieved in a QKD process, an effective defense can be provided against spoofing attacks, man-in-the-middle attacks and distributed denial of service (DDoS) attacks on the receiver, and the security of the QKD process is improved; furthermore, a waste of quantum key resources can be avoided as authentication information is dynamically generated with an algorithm.

Brief Description of the Drawings

[0048] FIG. 1 is a flow diagram of an embodiment of an authentication method used in a QKD process as provided in the present application;

[0049] FIG. 2 is a process flow diagram depicting a transmitter transmitting quantum states containing authentication information and key information as provided in the embodiment of the present application;

[0050] FIG. 3 is a schematic diagram of a first information format as provided in the embodiment of the present application;

[0051] FIG. 4 is a schematic diagram of a second information format as provided in the embodiment of the present application;

[0052] FIG. 5 is a schematic diagram of a third information format as provided in the embodiment of the present application;

[0053] FIG. 6 is a process flow diagram depicting a receiver performing an authentication operation as provided in the embodiment of the present application;

[0054] FIG. 7 is a flow diagram of an embodiment of another authentication method used in a QKD process as provided in the present application;

[0055] FIG. 8 is a schematic diagram of an embodiment of an authentication apparatus used in a QKD process as provided in the present application;

[0056] FIG. 9 is a flow diagram of an embodiment of a third authentication method used in a QKD process as provided in the present application;

[0057] FIG. 10 is a schematic diagram of an embodiment of an authentication apparatus used in a QKD process as provided in the present application;

[0058] FIG. 11 is a schematic diagram of an embodiment of an authentication system used in a QKD process as provided in the present application; and

[0059] FIG. 12 is a schematic diagram illustrating an interactive processing flow of the authentication system as provided in the embodiment of the present application.

Detailed Description of the Embodiments

[0060] Many specific details are elaborated in the following description to facilitate a thorough understanding of the present application. However, the present application can be implemented in other manners different from what is described herein, and those skilled in the art can make similar extensions without deviating from the spirit of the present application. It is to be understood that the present application is not limited to the specific embodiments disclosed below.

[0061] The present application provides an authentication method, and additional two other authentication methods and corresponding apparatuses, and an authentication system used in a QKD process, which are described respectively in detail in the following embodiments.

[0062] FIG. 1 illustrates a flow diagram of an embodiment of an authentication method used in a QKD process following the application. The method is implemented on a quantum communication transmitter device and a quantum communication receiver device participating in a QKD process. Before the specific steps of this embodiment are described in detail, the quantum communication transmitter device and the quantum communication receiver device involved in this embodiment are described briefly.

[0063] In this embodiment, identities of quantum communication devices participating in a QKD process are dynamically authenticated in the distribution process. Specifically, a first device that selects a basis of preparation and transmits quantum states to a peer device. This device (also called an initiator or a requestor of a QKD process) is defined as a quantum communication transmitter device, or a transmitter for short within this technical solution. A second device that selects a measurement basis to measure received quantum states is defined as a quantum communication receiver device, or a receiver for short within this technical solution.

[0064] According to one or more embodiments, the QKD process comprises the following stages: transmitting quantum states by a transmitter, measuring quantum states by a receiver, comparing a measurement basis by the transmitter and the receiver, screening an original key, estimating bit error rate, correcting error and amplifying privacy. Dynamic authentication is achieved in the above process according to this technical solution. In particular, after the transmitter transmits quantum states containing key information and authentication information, the receiver may verify the identity of the transmitter by measuring quantum states of the authentication information, so as to avoid spoofing attacks, man-in-the-middle attacks or DDoS

attacks. In addition to the foregoing one-way authentication, the transmitter may also verify the identity of the receiver according to authentication information provided by the receiver, so as to avoid "phishing attacks," thereby achieving a more secure two-way authentication.

[0065] Following examples will focus on describing this two-way authentication. It should be noted that In one or more implementations of this technical solution, one-way authentication by the receiver on the transmitter may be performed alone, which can also achieve the beneficial effects of improving security and avoiding wasted quantum key resources.

[0066] In addition, In one or more implementations of this technical solution, the subsequent stages such as measuring quantum states of the key information and comparing the measurement basis may be proceeded after authentication is completed. The mutual authentication may also be accomplished at and interleaved with various stages. The second implementation can simplify the interaction process and improve execution efficiency. As such, the following embodiments are described using these implementations. This embodiment is described in detail below.

[0067] The authentication method used in a QKD process comprises the following steps:

Step 101: A transmitter selects a preparation basis of transmitter authentication information according to a basis selection rule agreed upon with a receiver, and transmits quantum states containing at least key information and the transmitter authentication information in a preset manner, where the transmitter authentication information is generated with a first pre-provisioned algorithm and varies dynamically in different QKD processes initiated towards the receiver.

[0068] In order to avoid initiating a QKD process between non-legitimate quantum communication devices, quantum communication devices of the transmitter and the receiver need to verify the identity of the peer device through a pre-determined channel (such as classical channel) before the transmitter initiates a QKD process. According to one or more embodiments, any subsequent QKD process can be initiated only when both devices are authenticated.

[0069] In this technical solution, the transmitter generate transmitter authentication information with a first pre-provisioned algorithm, and the transmitter authentication information varies dynamically for different QKD processes. In order to accomplish this functionality, in this embodiment, the transmitter and the receiver may each maintain a

synchronously changing parameter n (relevant description can be found from relevant text in the subsequent step 101-1) according to a preset policy, and the transmitter and the receiver may use the parameter n to achieve the foregoing pre-determined channel-based authentication process.

[0070] For example, the requestor of a QKD process, i.e., the transmitter in the present application, may first transmit a quantum key negotiation request, where the request contains a hash value $\text{hash}(\text{userid_A}, n)$ calculated based on identification information userid_A (a description of the identification information can be found from relevant text in the subsequent step 101-1) of the transmitter and the parameter n . The peer device participating in the QKD process, i.e., the receiver in the present application, then calculates a hash value of locally preset userid_A and the locally maintained parameter n after receiving the foregoing request information, and returns response information containing a hash value $\text{hash}(\text{userid_B}, n)$ to the transmitter if the calculated value is consistent with the received value,; or ends the QKD process otherwise. Similarly, the transmitter may also verify the identity of the receiver in the same way, and if the receiver is authenticated, the QKD process may be initiated; the QKD process is not initiated otherwise.

[0071] In the implementation described above, a manner for pre-provisioning both the transmitter and the receiver with identification information of the other party is adopted. In other implementations, the transmitter and the receiver is not pre-provisioned with identification information of the other party; instead, a manner of carrying identification information in the request interaction of the QKD process is adopted. For example, information sent by the transmitter comprises $\text{hash}(\text{userid_A}, n)$ and userid_A , and information returned by the receiver comprises $\text{hash}(\text{userid_B}, n)$ and userid_B , and the transmitter and the receiver can also acquire identification information of the other party in this manner.

[0072] If both the transmitter and the receiver are authenticated in the above process, the subsequent QKD process is initiated, and the transmitter transmits quantum states containing at least authentication information and key information to the receiver. The process comprises steps 101-1 to 101-3, and is further described below with reference to FIG. 2.

[0073] Step 101-1: Generate transmitter authentication information with a first pre-provisioned algorithm.

[0074] In this technical solution, the transmitter and the receiver are pre-provisioned with the

same algorithm, i.e., the first pre-provisioned algorithm in the present application, for calculating transmitter authentication information, and the transmitter authentication information generated with the algorithm varies dynamically for different QKD processes initiated towards the receiver. In other words, authentication information of each requestor that is received by the receiver varies dynamically for the receiver, the receiver may perform authentication on the requestor according to the first pre-provisioned algorithm, and it is difficult for attackers to mimic the dynamically-varying authentication information, thus the receiver can effectively defend against spoofing attacks, man-in-the-middle attacks or DDoS attacks.

[0075] In one or more implementations, the required first pre-provisioned algorithm may be designed according to requirements as long as the dynamic-varying requirement is met. The following first pre-provisioned algorithm is used in this embodiment to calculate the transmitter authentication information according to the transmitter identification information `userid_A` and the synchronously changing parameter n according to a preset policy by the transmitter and receiver.

[0076] The transmitter identification information `userid_A` generally refers to identification information that can differentiate the transmitter from other quantum communication devices. For example, the transmitter identification information `userid_A` may be a device identifier as shipped from the factory or a fixed IP address of the transmitter (the same identification manner may also be adopted for receiver identification information `userid_B` involved in the following text).

[0077] The parameter n may be a synchronously changing numerical value according to the same preset policy by the transmitter and the receiver, i.e., a variable that can be inferred by the transmitter and the receiver. For example, the transmitter and the receiver may be pre-provisioned with the same initial numerical value and then synchronously change the respectively maintained numerical value according to a preset period, or a synchronous change may be triggered each time before a QKD process is initiated. The synchronous change may be implemented by means of a basic operation such as addition, subtraction, multiplication or division or a preset function. Because n is set locally at the transmitter and the receiver requiring no negotiation between the two parties, and n is a dynamically changing value, the probability that n is leaked or speculated is low, thereby ensuring security of authentication information.

[0078] In this embodiment, the transmitter authentication information Y may be calculated according to the following first pre-provisioned algorithm: $Y=f(\text{userid_A}, n)$, where the transmitter and the receiver use the same function f , for example, a hash function. The transmitter may acquire its identification information userid_A by calling a local function interface, while information of userid_A on the receiver side may be pre-provisioned or sent to the receiver by the transmitter through a pre-determined channel. For example, the information is sent at the negotiation request stage before the QKD process is initiated (information of userid_B on the transmitter side may also be acquired in the same manner).

[0079] It can be seen that userid_A is known by the transmitter and the receiver, and the parameter n of the transmitter and the receiver is also inferable in the foregoing first pre-provisioned algorithm. Therefore, transmitter authentication information calculated with the first pre-provisioned algorithm in a certain QKD process is definite for the transmitter and the receiver, the transmitter encloses the information in quantum states, and the receiver may verify the identity of the transmitter with the information. Due to the uniqueness of the identification information and the dynamic variation of the value of n , the receiver can effectively defend against spoofing attacks, man-in-the-middle attacks or DDoS attacks.

[0080] Based on the first pre-provisioned algorithm provided above, this embodiment further provides an exemplary implementation in which the number of times the transmitter and the receiver perform the QKD process may be used as the value of the parameter n . For example, the transmitter and the receiver set the initial value of the parameter n to 0, the two parties set the respectively maintained value of n to 1 when the transmitter and the receiver initiate the QKD process for the first time, and set the value of n to 2 when they initiate the QKD process for the second time, and so on, so as to realize a synchronous variation of the value of n for both the transmitter and the receiver. In one or more implementations, when the value of n accumulates to a preset upper limit, the transmitter and the receiver can synchronously clear n to 0 and restart the accumulation.

[0081] In the foregoing implementation, identification information of different QKD requestors, i.e., transmitters in the present application, is definitely different for the same receiver, so transmitter authentication information provided by each requestor in the QKD process is different. For the same QKD requestor, the value of n varies according to the number of times the QKD

process is performed, so transmitter authentication information provided by the same requestor in different QKD processes is also different. In this case, the receiver can verify identity information of a requestor more securely and therefore can resist spoofing attacks, man-in-the-middle attacks or DDoS attacks more effectively.

[0082] In one or more implementations, in addition to the first pre-provisioned algorithm based on the identification information and the parameter n as provided in this embodiment, first pre-provisioned algorithms in other forms may also be used. For example, this technical solution of the present application may also be implemented by pre-provisioning the same random number between a transmitter and a receiver, pre-provisioning different random numbers for different transmitters and receivers, and using the random number to replace the identification information.

[0083] Step 101-2: Select a preparation basis of the transmitter authentication information according to a basis selection rule agreed upon with a receiver.

[0084] Because the transmitter and the receiver calculate transmitter authentication information with the same first pre-provisioned algorithm, the transmitter transmits the information in quantum states, and the receiver verifies the identity of the transmitter with the same information, the transmitter and the receiver can select a corresponding basis of preparation or measurement basis according to an agreed basis selection rule after the transmitter and the receiver obtain the transmitter authentication information by calculation.

[0085] The agreed basis selection rule may be preset by the transmitter and the receiver or negotiated and determined through a pre-determined channel before the QKD process is initiated. For example, the transmitter uses preparation bases of horizontal polarization and vertical polarization, and the receiver uses a linear polarization measurement basis for measurement; or, the transmitter uses preparation bases of left-hand polarization and right-hand polarization, and the receiver uses a circular polarization measurement basis for measurement. Specifically for instance, for a bit 0, the transmitter uses a basis of preparation of horizontal polarization, and the receiver uses a linear polarization measurement basis, and for a bit 1, the transmitter uses a basis of preparation of left-hand polarization, and the receiver uses a circular polarization measurement basis.

[0086] The transmitter selects, according to the agreed basis selection rule, a corresponding basis of

preparation for a bit string corresponding to the transmitter authentication information generated in step 101-1.

[0087] Step 101-3: Transmit (in a preset manner) quantum states containing at least key information and the transmitter authentication information.

[0088] The preset manner may be pre-determined by the transmitter and the receiver, by which the transmitter transmits quantum states following the preset manner, and the receiver differentiates quantum states of various information following the same manner. For example, the transmitter may transmit quantum states of the transmitter authentication information and randomly generated key information with different wavelengths, and the receiver differentiates the quantum states with the different wavelengths accordingly.

[0089] Preferably, in order to provide further security assurance and prevent attackers from making targeted monitoring, the quantum states of the transmitter authentication information and the key information (which may be collectively called quantum states of data information) may be sent using the same wavelength, and control information may be introduced as prefixes of the transmitter authentication information and the key information to facilitate the differentiation of the quantum states by the receiver. Based on this consideration, in this embodiment, the transmitter transmits quantum states of the control information and the data information (including the key information and the transmitter authentication information) using different wavelengths in a preset information format, and the receiver differentiates the received quantum states of various information according to wavelength characteristics and the information format. The different wavelengths may be preset by the transmitter and the receiver or negotiated and determined through a pre-determined channel before the QKD process is initiated.

[0090] The information format may be defined in many manners as long as the receiver can correctly differentiate the quantum states. Several specific examples of which are given below.

[0091] Example 1: The transmitter authentication information and the key information have respective control information as prefixes (i.e., authentication control information and key control information in short, respectively), and wavelengths carrying quantum states of the two types of control information are different, referring to the schematic diagram of an information format shown in FIG 3. A wavelength carrying the quantum states of the data information

(including the transmitter authentication information and the key information) is λ_1 , a wavelength carrying quantum states of the authentication control information is λ_2 , a wavelength carrying quantum states of the key control information is λ_3 , and λ_1 , λ_2 and λ_3 are different from each other. λ_2 and λ_3 may be preset by the transmitter and the receiver or negotiated and determined before the quantum key negotiation process is initiated. In this manner, the transmitter can randomly select quantum states of the two types of control information, and the receiver can directly distinguish the authentication control information from the key control information according to the wavelengths.

[0092] Example 2: The transmitter authentication information and the key information have respective control information as prefixes, and the two types of control information have different codes, referring to the schematic diagram of an information format shown in FIG 4. A wavelength carrying the quantum states of the data information (including the transmitter authentication information and the key information) is λ_1 , a wavelength carrying quantum states of the authentication control information and a wavelength carrying quantum states of the key control information are both λ_2 (different from λ_1), but the two types of control information have different codes. For example, 00000 is the code of the authentication control information, and 11111 is the code of the key control information. The different codes are preset by the transmitter and the receiver or negotiated and determined through a pre-determined channel before the QKD process is initiated; and a basis for preparing or measuring quantum states of the two types of control information may also be preset by the transmitter and the receiver or negotiated and determined through the pre-determined channel before the QKD process is initiated.

[0093] Example 3: The transmitter authentication information and the key information use common control information as a prefix, referring to the schematic diagram of an information format shown in FIG 5. A wavelength carrying the quantum states of the data information (including the transmitter authentication information and the key information) is λ_1 , the transmitter authentication information and the key information share the same control information prefix, a wavelength carrying quantum states of the control information is λ_2 , which is different from λ_1 . In this manner, because the receiver can distinguish the control information from the data information according to the wavelengths, the transmitter can randomly select the quantum states of the control information, but a length of the transmitter

authentication information located between the control information and the key information should be agreed upon by the transmitter and the receiver so as to enable the receiver to correctly distinguish the transmitter authentication information from the key information in the data information. In one or more implementations, the length of the transmitter authentication information may be preset by the transmitter and the receiver or negotiated and determined through a pre-determined channel before the QKD process is initiated.

[0094] It should be noted that the examples given above and the corresponding diagrams provide just part of the information format, and in one or more implementations, each information format may be repeated many times and concatenated. For example, the information format provided in Example 3 may be extended as (for example, but not limited to): control information|transmitter authentication information|key information|control information|transmitter authentication information|key information.

[0095] In the foregoing implementation provided in this embodiment, the transmitter transmits quantum states of control information, transmitter authentication information and key information, according to wavelength characteristics and in an information format that are agreed upon with the receiver. For ease of understanding, description is made below using the information format in Example 3 as an example.

[0096] For example, the transmitter transmits quantum states of a binary bit string with a length of n at time points $t_1, t_2 \dots t_n$, and the binary bit string is shown below:

$$x_1, x_2 \dots x_i, x_{i+1} \dots x_{i+m+1} \dots x_n$$

[0097] The binary bit string comprises three parts: the first part is a control information bit string, the second part is an authentication information bit string, and the third part is a key information bit string. The control information bit string is a randomly selected binary bit string and has a length of i ; the authentication information bit string is a transmitter authentication information bit string generated with the first pre-provisioned algorithm in step 101-1, and the length m thereof may be negotiated and determined by the transmitter and the receiver through a pre-determined channel; and the key information bit string is a randomly

generated binary bit string and has a length of $n-m-i$.

[0098] The transmitter transmits a coded quantum states

$\left(\left| \varphi_{j_1}^{x_1} \right\rangle, \left| \varphi_{j_2}^{x_2} \right\rangle \dots \left| \varphi_{j_i}^{x_i} \right\rangle, \left| \varphi_{j_{i+1}}^{x_{i+1}} \right\rangle \dots \left| \varphi_{j_{i+m}}^{x_{i+m}} \right\rangle, \left| \varphi_{j_{i+m+1}}^{x_{i+m+1}} \right\rangle \dots \left| \varphi_{j_n}^{x_n} \right\rangle \right)$ of the binary bit string to the receiver at the time

points $t_1, t_2, \dots, t_n$, where $j_1, j_2, \dots, j_i, j_{i+1}, \dots, j_{i+m}, j_{i+m+1}, \dots, j_n$ is a basis of preparation sequence used by the transmitter, $j_1, j_2, \dots, j_i$ is a random quantum states basis of preparation corresponding to the control information bit string and has a wavelength of λ_2 , $j_{i+1}, \dots, j_{i+m}$ is a quantum states basis of preparation of the authentication information bit string that is selected according to the basis selection rule agreed upon by the transmitter and the receiver, $j_{i+m+1}, \dots, j_n$ is a random quantum states basis of preparation corresponding to the key information bit string, wavelengths of the preparation bases of the authentication information bit string and the key information bit string are both λ_1 , which is different from λ_2 .

[0099] Correspondingly, the receiver can distinguish the control information from the data information according to the wavelengths, distinguish the transmitter authentication information from the key information in the data information according to the length m , and use a measurement basis sequence $k_{i+1}, \dots, k_{i+m}, k_{i+m+1}, \dots, k_n$ to measure the received quantum states of the data information, where $k_{i+1}, \dots, k_{i+m}$ is a measurement basis for the quantum states of the transmitter authentication information, the measurement basis is selected according to the basis selection rule agreed upon with the transmitter, and $k_{i+m+1}, \dots, k_n$ is a random quantum states measurement basis corresponding to the quantum states of the key information.

[0100] At this point, the transmitter has completed the quantum states transmitting operation through steps 101-1 to 101-3. In this process, the transmitter generates transmitter authentication information with a first pre-provisioned algorithm, and the transmitter authentication information is not fixed but varies dynamically in different QKD processes initiated towards the receiver, so as to provide a guarantee for the receiver to defend against various possible spoofing attacks, man-in-the-middle attacks or DDoS attacks.

[0101] Step 102: The receiver uses a preset manner to differentiate the received quantum states of various information, and the receiver measures received quantum states of the transmitter authentication information according to the basis selection rule, and if a measurement result is consistent with transmitter authentication information calculated with

the first pre-provisioned algorithm, transmits receiver authentication information generated with a second pre-provisioned algorithm; or determines that the transmitter is not authenticated and ends the QKD process otherwise.

[0102] In one or more implementations of this technical solution, the receiver verifies the identity of the transmitter by measuring the received quantum states of the transmitter authentication information, and if the transmitter is not authenticated, ends the QKD process; otherwise, the receiver may perform subsequent operations of measuring quantum states of the key information and the like.

[0103] Preferably, based on the above one-way authentication, the receiver may further provide its identity information to the transmitter for verification, and the transmitter can avoid "phishing attacks" and other possible attacks following this manner, so as to achieve a more secure two-way authentication. The specific process of the implementation comprises steps 102-1 to 102-5 and is further described below with reference to FIG. 6.

[0104] Step 102-1: Differentiate received quantum states of various information in the preset manner.

[0105] In this step, the receiver differentiates quantum states of information such as transmitter authentication information and key information in a preset manner agreed upon with the transmitter for quantum states of various information received from a quantum channel. In one or more implementations, different processing manners may be adopted according to different preset manners. Using the implementation provided in step 101-3 that the transmitter transmits quantum states of the control information and the data information with different wavelengths as an example, the quantum states of the control information and the data information may be differentiated first according to different wavelengths, and the quantum states of authentication information and key information may be differentiated further according to a preset information format.

[0106] For example, if the transmitter and the receiver agree upon the wavelength characteristics and the information format as demonstrated in Example 1 of step 101-3, in this step, if the receiver receives quantum states having a wavelength of λ_2 , it can be known that the quantum states is the quantum states of the authentication control information, that subsequently received quantum states having a wavelength of λ_1 is the quantum states of the transmitter

authentication information, and a measurement basis should be selected according to a basis selection rule agreed upon by the two parties for measurement. Instead, if quantum states having a wavelength of λ_3 are received, it can be known that a subsequently received quantum states having a wavelength of λ_1 is the quantum states of the key information, and a randomly selected measurement basis may be used for measurement.

[0107] For another example, if the transmitter and the receiver agree upon the wavelength characteristics and the information format as demonstrated in Example 2 of step 101-3 (e.g., if the receiver receives quantum states having a wavelength of λ_2), it can be known that the quantum states are the quantum states of the control information, and a measurement basis agreed upon (preset or negotiated and determined) with the transmitter is used for measurement. A measurement result is compared with an agreed-upon coded value to acquire the type of the received control information: authentication control information or key control information, and if quantum states having a wavelength of λ_1 is received subsequently, a measurement basis corresponding to the type may be used for measurement.

[0108] For the wavelength characteristics and the information format as demonstrated in Example 3 of step 101 and other wavelength characteristics and information formats that may be used by the transmitter, the receiver may also differentiate or filter the quantum states of various information in a similar manner, which will not be described herein again.

[0109] Step 102-2: Calculate transmitter authentication information with the first pre-provisioned algorithm.

[0110] According to this embodiment, the transmitter and the receiver are preset with the same algorithm for calculating transmitter authentication information, i.e., the first pre-provisioned algorithm in the present application. Reference can be made to the description of step 101-1 for details of the algorithm, which will not be described herein again.

[0111] Because the receiver is pre-provisioned with the same algorithm, authentication information that should be provided by the transmitter can be expected, and in this step, the receiver calculates transmitter authentication information with the first pre-provisioned algorithm to serve as an expected value of authentication information provided by the transmitter.

[0112] Step 102-3: Select a measurement basis according to the basis selection rule, and measure received quantum states of transmitter authentication information.

[0113] According to this embodiment, the transmitter and the receiver agree upon a basis selection rule. Reference can be made to the description of step 101-2 for description of the basis selection rule, which will not be described herein again.

[0114] If a fixed measurement basis (e.g., a linear polarization measurement basis) is set for the receiver in the basis selection rule, the received quantum states of the transmitter authentication information is measured by using the fixed measurement basis. If different measurement bases are set for different bit values in the basis selection rule, in this step, a corresponding measurement basis is selected according to the value of each bit of the transmitter authentication information calculated in step 102-2, and a corresponding bit in the received quantum states of the transmitter authentication information is measured.

[0115] Step 102-4: Determine whether a measurement result is consistent with the calculated transmitter authentication information, and if so, perform step 102-5; and end the QKD process otherwise.

[0116] A corresponding measurement result, namely, the transmitter authentication information carried in the quantum states, is obtained through the measurement in step 102-3. In this step, the measured transmitter authentication information is compared with the transmitter authentication information calculated in step 102-2, so as to complete authentication on the transmitter.

[0117] In this embodiment, the transmitter generates transmitter authentication information with a first pre-provisioned algorithm $Y=f(\text{userid_A}, n)$. The receiver also uses the same algorithm to calculate an expected value of the information, and compares measured transmitter authentication information with the expected value. If the measured transmitter authentication information is consistent with the expected value, it indicates that the transmitter uses the correct identification information userid_A , variable n , and function f when generating its authentication information, and only a quantum communication device having legal identity can acquire the foregoing information. Thus, it can be determined that the transmitter is authenticated, and therefore a subsequent step 102-5 can be performed accordingly. If, on the contrary, it can be determined that the transmitter is not authenticated, the QKD process is ended.

[0118] In a quantum channel transmission process, a few photons may fail to be detected or the

measurement result may not be completely consistent with the expectation due to factors such as attenuation and noise interference. In this case, it may lead to a meaningless reduction in the distribution amount of quantum keys if the transmitter is considered to fail the authentication and the QKD process is ended. Based on this consideration as well as the requirement for defense against spoofing attacks, man-in-the-middle attacks or DDoS attacks, a manner of setting a threshold may be adopted. That is, if the difference between transmitter authentication information measured by the receiver and an expected value is less than a preset threshold, for example, the number of bits of the measured transmitter authentication information inconsistent with the expected value is less than a preset upper limit value, the receiver may consider that the transmitter is authenticated.

[0119] Step 102-5: Randomly select a measurement basis to measure received quantum states of key information, disclose the measurement basis, and transmit receiver authentication information generated with a second pre-provisioned algorithm.

[0120] Upon reaching this step, the transmitter has been authenticated by the receiver, and therefore, the QKD process can be continued, and the receiver may randomly select a measurement basis to measure received quantum states of key information, and to disclose the measurement basis through a pre-determined channel according to a QKD protocol. In this embodiment, the disclosed measurement basis may be encrypted with a variable n maintained by the receiver and then transmitted, and the transmitter also uses a variable n maintained by the transmitter to decrypt the measurement basis after receiving it.

[0121] In order to provide further security assurance and to achieve two-way authentication, the transmitter and the receiver may be pre-provisioned with the same algorithm for calculating receiver authentication information, i.e., the second pre-provisioned algorithm in the present application. According to these embodiments, the receiver generates its authentication information with the algorithm and provides it to the transmitter, and the transmitter verifies the identity of the receiver with the same algorithm.

[0122] In one or more implementations, the required second pre-provisioned algorithm may be designed to meet requirements. In this embodiment, in order to generate dynamic receiver authentication information, the following second pre-provisioned algorithm is applied based on the first pre-provisioned algorithm: receiver authentication information is calculated according to

receiver identification information userid_B and a variant of a synchronously changing parameter n according to a preset policy by the transmitter and the receiver. Reference can be made to the relevant text in step 101-1 for description of the parameter n . The variant of the synchronously changing parameter n according to the preset policy may include: the parameter n itself; or a result obtained by processing the parameter using a preset mathematical transformation method, for example, $n+1$. A rule for generating the variant of the parameter n may be agreed upon by the transmitter and the receiver.

[0123] A specific example of the second pre-provisioned algorithm is given below: receiver authentication information $Y=\text{hash}(\text{userid_B}, n+1)$, that is, a hash value of a character string formed by joining receiver identification information and information of the variant of the parameter n is calculated, and the hash value is used as the receiver authentication information.

[0124] It can be seen from the above description that the receiver authentication information calculated with the second pre-provisioned algorithm also varies dynamically. For the transmitter in this embodiment, different receivers have different identification information, so they provide different receiver authentication information. For the same receiver, because the value of n varies dynamically, the receiver authentication information provided by the receiver also varies dynamically. Furthermore, if the number of times the transmitter and the receiver perform the QKD process is used as the parameter n , receiver authentication information provided by the same receiver in different QKD processes is also different. It is difficult for attackers to mimic the dynamic characteristic, thereby providing a strong guarantee for the transmitter to avoid attacks such as phishing by verifying the identity of the receiver.

[0125] Step 103: The transmitter calculates receiver authentication information with the second pre-provisioned algorithm, and when the received receiver authentication information is consistent with the calculation result, determines that the receiver is authenticated. If the received receiver authentication information is not consistent, then the receiver is determined not to be authenticated and the QKD process is ended.

[0126] After receiving the receiver authentication information, the transmitter calculates receiver authentication information with the second pre-provisioned algorithm, and compares the received receiver authentication information with the calculated one, so as to complete the authentication on the receiver.

[0127] Using the specific example given in step 102-5, the transmitter calculates receiver authentication information with the second pre-provisioned algorithm, that is, $Y = \text{hash}(\text{userid_B}, n+1)$, where userid_B may be pre-provisioned or sent in advance by the receiver to the transmitter through a pre-determined channel. If the received receiver authentication information is consistent with the calculation result, it indicates that the receiver uses the correct identification information userid_B , variable n , and hash function when generating its authentication information. If the transmitter also knows the variant generation rule agreed upon by the two parties, and only a quantum communication device having legal identity can acquire the foregoing information, it can then determine that the receiver is authenticated; otherwise, it determines that the receiver is not authenticated and the QKD process is ended.

[0128] If the transmitter determines that the receiver is authenticated, the transmitter may, according to the QKD protocol, compare a measurement basis disclosed by the receiver with a basis of preparation used by the transmitter to select a correct measurement basis, screen out an original key according to the correct measurement basis, and disclose the correct measurement basis to the receiver through the pre-determined channel.

[0129] Subsequently, the receiver screens an original key according to the correct measurement basis disclosed by the transmitter, the transmitter and the receiver further acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes, and the QKD process is ended. In this embodiment, at the bit error rate estimation, error correction and privacy amplification stages, information negotiated by the transmitter and the receiver through the pre-determined channel may be a variant of the parameter n (for example, $n+1$), for performing the corresponding encryption or decryption operation.

[0130] At this point, it can be seen from the foregoing step 101 to step 103 that this technical solution described in this embodiment improves the existing QKD protocol and provides a new idea for performing dynamic authentication in a QKD process. Because the transmitter transmits, through the quantum channel, authentication information that is generated with the first pre-provisioned algorithm and varies dynamically in different QKD processes initiated towards the receiver, and the receiver also uses the same pre-provisioned algorithm to verify the received authentication information, dynamic authentication is realized on a QKD requestor in a QKD

process, and an effective defense can be provided against spoofing attacks, man-in-the-middle attacks and DDoS attacks on the receiver. Furthermore, on the basis of the one-way authentication, the transmitter and the receiver use the second pre-provisioned algorithm to realize dynamic authentication on the receiver by the transmitter, thereby effectively resisting potential risks of phishing attacks on the transmitter.

[0131] In addition, in this solution, the transmitter authentication information is sent in the form of quantum states, so that security can be further improved, and a waste of quantum key resources can be avoided, as authentication information is dynamically generated with an algorithm.

[0132] In addition, the present application further provides another authentication method used in a QKD process. The method is implemented on a quantum communication transmitter device participating in a QKD process. FIG. 7 illustrates a flow diagram of an embodiment of another authentication method used in a QKD process in the present application. The same steps in this embodiment as the foregoing embodiment are not described again, and the following description focuses on the differences. The method comprises the following steps:

[0133] Step 701: Generate transmitter authentication information with a first pre-provisioned algorithm, where the transmitter authentication information generated with the first pre-provisioned algorithm varies dynamically in different QKD processes initiated to a receiver, and the receiver device refers to a peer device participating in the QKD process.

[0134] The first pre-provisioned algorithm comprises: calculating the transmitter authentication information according to identification information of a host device and a synchronously changing parameter with the peer device according to a preset policy. The calculation of the transmitter authentication information may employ a hash function.

[0135] Step 702: A preparation basis of the transmitter authentication information is selected according to a basis selection rule agreed upon with the peer device.

[0136] Step 703: Quantum states containing at least key information and the transmitter authentication information are transmitted to the peer device in a preset manner.

[0137] For example, quantum states of control information and data information may be sent

with different wavelengths in a preset information format, where the data information comprises the key information and the transmitter authentication information.

[0138] The preset information is formatted so that the authentication information and the key information have respective control information as prefixes; or the authentication information and the key information use common control information as a prefix, and a length of the authentication information between the control information and the key information is preset or negotiated and determined with the peer device through a pre-determined channel.

[0139] After the quantum states transmission operation in this step is completed, information returned by the peer device may be received, where the information comprises at least receiver authentication information. Additionally, receiver authentication information may be calculated with a second pre-provisioned algorithm; whether the received receiver authentication information is consistent with the calculation result is determined. If the received receiver authentication information is consistent with the calculation result, the receiver is determined to be authenticated; otherwise, that the receiver is determined not to be authenticated and the QKD process is ended.

[0140] The second pre-provisioned algorithm comprises calculating the receiver authentication information according to identification information of the peer device and a variant of a synchronously changing parameter with the peer device according to a preset policy. The synchronously changing parameter with the peer device according to the preset policy consists of the number of times the QKD process is performed with the peer device. The calculation of the receiver authentication information may employ a hash function.

[0141] The information returned by the peer device may include not only the receiver authentication information, but also a measurement basis for measuring quantum states of the key information. After the determining that the receiver is authenticated, the following operations may be performed: determining a correct measurement basis of the quantum states of the key information, screening an original key, disclosing the correct measurement basis of the quantum states of the key information through a pre-determined channel, and acquiring a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes, so as to complete the QKD process.

[0142] Another authentication method used in a QKD process is provided in the foregoing embodiment. Correspondingly, the present application further provides an authentication apparatus

used in a QKD process. The apparatus is deployed on a quantum communication transmitter device participating in a QKD process. FIG 8 illustrates a schematic diagram of an embodiment of an authentication apparatus used in a QKD process in the present application. The apparatus embodiment is basically similar to the method embodiment and therefore is described briefly. Reference can be made to the description of the method embodiment for relevant parts. The apparatus embodiment described below is merely exemplary.

[0143] An authentication apparatus used in a QKD process in this embodiment comprises: an transmitter identity information generating unit 801, configured to generate transmitter authentication information with a first pre-provisioned algorithm, where the transmitter authentication information varies dynamically in different QKD processes initiated to a receiver; a basis of preparation selection unit 802, configured to select a basis of preparation of the transmitter authentication information according to a basis selection rule agreed upon with a peer device participating in the QKD process; and quantum states transmitting unit 803, configured to transmit quantum states containing at least key information and the transmitter authentication information to the peer device in a preset manner.

[0144] In an embodiment, the apparatus further comprises:

a receiver identity information receiving unit, configured to, after the quantum states transmitting unit completes the quantum states transmitting operation, receive information returned by the peer device, where the information comprises at least receiver authentication information;

a receiver identity information calculation unit, configured to calculate receiver authentication information with a second pre-provisioned algorithm; and

a receiver authentication unit, configured to determine whether the received receiver authentication information is consistent with the calculation result, and if so, determine that a receiver is authenticated; and to determine that the receiver is not authenticated and end the QKD process otherwise.

[0145] In an embodiment, the information received by the receiver identity information receiving unit not only comprises the receiver authentication information but also comprises a measurement basis used by the peer device for measuring quantum states of the key information. In these embodiments, the apparatus may comprise:

an original key screening unit, configured to determine a correct measurement basis of the quantum states of the key information, and screen an original key after the receiver authentication unit determines that the receiver is authenticated;

a correct measurement basis disclosing unit, configured to disclose the correct measurement basis of the quantum states of the key information through a pre-determined channel; and

a shared quantum key generating unit, configured to acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0146] In an embodiment, the first pre-provisioned algorithm used by the transmitter identity information generating unit comprises calculating the transmitter authentication information according to identification information of a host device and a synchronously changing parameter with the peer device according to a preset policy.

[0147] In an embodiment, the second pre-provisioned algorithm used by the receiver identity information calculation unit comprises calculating the receiver authentication information according to identification information of the peer device and a variant of a synchronously changing parameter with the peer device according to a preset policy.

[0148] In an embodiment, the synchronously changing parameter used for calculation within the transmitter identity information generating unit and the receiver identity information calculation unit according to the preset policy comprises the number of times the QKD process is performed with the peer device.

[0149] In an embodiment, the transmitter identity information generating unit or the receiver identity information calculation unit is specifically configured to calculate the corresponding authentication information with a hash function.

[0150] In an embodiment, the quantum states transmitting unit is specifically configured to transmit quantum states of control information and data information by respectively using different wavelengths in a preset information format, and the data information comprises the key information and the transmitter authentication information.

[0151] In an embodiment, the preset information format used by the quantum states transmitting unit includes the authentication information and the key information using respective control information as prefixes.

[0152] In an embodiment, the preset information format used by the quantum states transmitting unit includes the authentication information and the key information using common control information as a prefix, and a length of the authentication information between the control information and the key information is preset or negotiated and determined with the peer device through a pre-determined channel.

[0153] In addition, the present application further provides a third authentication method used in a QKD process. The method is implemented on a quantum communication receiver device participating in a QKD process. FIG 9 illustrates a flow diagram of an embodiment of a third authentication method used in a QKD process in the present application. The same steps in this embodiment as the foregoing embodiment are not described again, and the following focuses on differences. The method comprises the following steps:

[0154] Step 901: Receive quantum states sent by a peer device participating in a QKD process, and differentiate the received quantum states of various information in the same preset manner as that of the peer device.

[0155] Step 902: Calculate transmitter authentication information with the same first pre-provisioned algorithm as that of the peer device.

[0156] Step 903: Select a measurement basis according to the same basis selection rule as that of the peer device, and measure received quantum states of transmitter authentication information.

[0157] Step 904: Determine whether a measurement result is consistent with the calculated transmitter authentication information, and if so, determine that a transmitter is authenticated; otherwise, determine that the transmitter is not authenticated and end the QKD process.

[0158] In one or more embodiments, the following operations may be performed after determining that the transmitter is authenticated: generating receiver authentication information with the same second pre-provisioned algorithm as that of the peer device, and transmitting the receiver authentication information to the peer device.

[0159] In one or more other embodiments, the following operations may be performed after determining that the transmitter is authenticated: randomly selecting a measurement basis to measure received quantum states of the key information, and disclosing the measurement basis

through a pre-determined channel; receiving a correct measurement basis of the quantum states of the key information sent by the peer device through the pre-determined channel; and screening an original key, and acquiring a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0160] The third authentication method used in a QKD process is provided in the foregoing embodiment. Correspondingly, the present application further provides an authentication apparatus used in a QKD process. The apparatus is deployed on a quantum communication receiver device participating in a QKD process. Referring to FIG 10, FIG 10 is a schematic diagram of an embodiment of an authentication apparatus used in a QKD process in the present application. The apparatus embodiment is basically similar to the method embodiment and therefore is described briefly. Reference can be made to the description of the method embodiment for relevant parts. The apparatus embodiment described below is merely exemplary.

[0161] An authentication apparatus used in a QKD process in this embodiment comprises: a quantum states receiving and differentiating unit 1001, configured to receive quantum states sent by a peer device participating in the QKD process, and to differentiate the received quantum states of various information in the same preset manner as that of the peer device; a transmitter identity information calculation unit 1002, configured to calculate transmitter authentication information with the same first pre-provisioned algorithm as that of the peer device; an identity information quantum states measurement unit 1003, configured to select a measurement basis according to the same basis selection rule as that of the peer device, and to measure received quantum states of transmitter authentication information; and a transmitter authentication unit 1004, configured to determine whether a measurement result is consistent with the calculated transmitter authentication information, and if so, to determine that a transmitter is authenticated; and to determine that the transmitter is not authenticated and end the QKD process otherwise.

[0162] In an embodiment, the apparatus further comprises:

a receiver identity information generating unit, configured to generate receiver authentication information with the same second pre-provisioned algorithm as that of the peer device after the transmitter authentication unit determines that the transmitter is authenticated;; and

a receiver identity information transmitting unit, configured to transmit the receiver

authentication information to the peer device.

[0163] In an embodiment, the apparatus further comprises:

a key information quantum states measurement basis disclosing unit, configured to randomly select a measurement basis to measure received quantum states of key information after the transmitter authentication unit determines that the transmitter is authenticated, and disclose the measurement basis through a pre-determined channel;

a correct measurement basis receiving unit, configured to receive a correct measurement basis of the quantum states of the key information sent by the peer device through the pre-determined channel; and

a screening and shared quantum key generating unit, configured to screen an original key, and acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0164] In addition, an embodiment of the present application further provides an authentication system used in a QKD process. As shown in FIG. 11, the system comprises an authentication apparatus 1101 deployed on a quantum communication transmitter device and an authentication apparatus 1102 deployed on a quantum communication receiver device.

[0165] The authentication apparatuses respectively deployed on the quantum communication transmitter device and the quantum communication receiver device use an authentication method provided in the present application to realize dynamic authentication on a peer device in a QKD process. An interactive processing flow of the authentication system used in a QKD process is described briefly below with reference to FIG. 12. The authentication apparatus deployed on the quantum communication transmitter device is called A for short, the authentication apparatus deployed on the quantum communication receiver device is called B for short, the transmitter and the receiver are both preset with identification information `userid_A` and `userid_B` as well as a first pre-provisioned algorithm and a second pre-provisioned algorithm, and the transmitter and the receiver respectively maintain a synchronously changing parameter n according to a preset policy.

- 1) A transmits a key negotiation request to B, where the request carries `hash(userid_A, n)`.
- 2) B verifies the validity of the identity of A and transmits `hash(userid_B, n)` to A.

3) A verifies the validity of the identity of B; and selects, according to a basis selection rule agreed upon with B, a corresponding basis of preparation for transmitter authentication information generated with a first pre-provisioned algorithm $f(\text{userid_A}, n)$, and transmits quantum states containing at least key information and the transmitter authentication information in a preset manner.

4) B differentiates the received quantum states of various information in the preset manner, and measures received quantum states of the transmitter authentication information according to the basis selection rule. In addition, if a measurement result is consistent with transmitter authentication information calculated with the first pre-provisioned algorithm $f(\text{userid_A}, n)$, B also transmits receiver authentication information $\text{hash}(\text{userid_B}, n+1)$ generated with a second pre-provisioned algorithm, randomly selects a measurement basis to measure received quantum states of the key information, and then discloses the measurement basis. Otherwise, the transmitter is not authenticated and the QKD process is ended.

5) A calculates receiver authentication information with the second pre-provisioned algorithm, and when the received receiver authentication information is consistent with the calculation result, screens an original key, and discloses a correct measurement basis of the quantum states of the key information through a pre-determined channel; otherwise, determines that the receiver is not authenticated and ends the QKD process.

6) B screens an original key; and A and B acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

[0166] It should be noted that a possible interaction process of the system is shown above, and different ways of interaction may be adopted in other implementations. Relevant description is made in the method embodiments provided above and will not be repeated herein.

[0167] The present application has been disclosed above according to one or more embodiments, but is not intended to be limited thereto. Possible variations and modifications can be made by those skilled in the art without deviating from the spirit and scope of the present application. Therefore, the scope of the present application shall be defined by the claims of the present application.

[0168] In a typical configuration, a computing device includes one or more processors (CPUs), input-output interfaces, network interfaces and memories.

[0169] A memory may include a volatile memory in a computer-readable medium, a random access memory (RAM) and/or a non-volatile memory, such as a read-only memory (ROM) or a flash RAM. A memory is an example of a computer-readable medium.

[0170] A computer-readable medium includes a non-volatile medium, a volatile medium, a mobile medium or an immobile medium, which may implement information storage by means of any method or technology. Information may be a computer-readable instruction, a data structure, a module of a program, or other data. Examples of computer storage media include, but are not limited to a phase change random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other types of random access memories (RAMs), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technologies, a compact disc-read only memory (CD-ROM), a digital versatile disc (DVD) or other optical memories, a cartridge magnetic tape, a magnetic tape or magnetic disk memory or other magnetic storage devices or any other non-transmission media, which may be configured to store information that can be accessed by a computing device. As defined herein, computer-readable media do not include transitory media, for example, modulated data signals and carriers.

[0171] Those skilled in the art should understand that an embodiment of the present application may be provided as a method, a system or a computer program product. Therefore, the present application may be in the form of a full hardware embodiment, a full software embodiment, or an embodiment combining software and hardware. Furthermore, the present application may be in the form of computer program products implemented on one or more computer storage media (including, but not limited to a magnetic disk memory, a CD-ROM, an optical memory or the like), which include a computer program code.

CLAIMS

1. An authentication method used in a quantum key distribution (QKD) process, the process comprising:

selecting, by a transmitter participating in the QKD process, a preparation basis for authenticating transmitter identity information according to a basis selection rule;

transmitting a plurality of quantum states comprising key information and the transmitter authentication information, the transmitter authentication information being generated with a first pre-provisioned algorithm;

differentiating, by a receiver participating in the QKD process, the plurality of quantum states;

measuring the plurality of quantum states comprising the transmitter authentication information according to the basis selection rule;

calculating, by the transmitter, a transmitter authentication information using a first pre-provisioned algorithm;

comparing the the measured plurality of quantum states and the transmitter authentication information calculated using the first pre-provisioned algorithm;

determining that the transmitter is authenticated when the measured plurality of quantum states is consistent with the transmitter authentication information calculated using the first pre-provisioned algorithm;

determining that the transmitter is not authenticated when the measured plurality of quantum states is not consistent with the transmitter authentication information calculated using the first pre-provisioned algorithm; and

terminating the QKD process when the measured plurality of quantum states is not consistent with the transmitter authentication information calculated using the first pre-provisioned algorithm,

wherein the transmitter authentication information generated with the first pre-provisioned algorithm varies dynamically in different QKD processes initiated towards the receiver.

2. The authentication method of Claim 1, wherein the determining that the transmitter is authenticated further comprises:

generating, by the receiver, receiver authentication information with a second pre-provisioned algorithm;

transmitting the receiver authentication information to the transmitter;

calculating, by the transmitter, receiver authentication information with the second pre-provisioned algorithm;

comparing the receiver authentication information generated by the receiver with receiver authentication information calculated by the transmitter;

determining that the receiver is authenticated when the receiver authentication information generated by the receiver is consistent with receiver authentication information calculated by the transmitter;

determining that the receiver is not authenticated when the receiver authentication information generated by the receiver is not consistent with receiver authentication information calculated by the transmitter; and

terminating the QKD process when when the receiver authentication information generated by the receiver is not consistent with receiver authentication information calculated by the transmitter.

3. The authentication method of Claim 2, wherein determining that the transmitter is authenticated further comprises:

randomly selecting a measurement basis to measure the received quantum states of the key information;

disclosing the measurement basis through a pre-determined channel;

determining a correct measurement basis of the quantum states of the key information;

screening an original key;

disclosing the correct measurement basis of the quantum states of the key information through the pre-determined channel;

screening, by the receiver, an original key; and

acquiring, by the transmitter and the receiver, a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

4. The authentication method of Claim 2, wherein the first pre-provisioned algorithm is performed by calculating the transmitter authentication information according to transmitter identification information and a synchronously changing parameter according to a preset policy by both the transmitter and the receiver, wherein the transmitter identification information on the receiver side is pre-provisioned or sent to the receiver by the transmitter through a pre-determined channel.

5. The authentication method of Claim 4, wherein selecting a basis of preparation further comprises:

performing, by both the transmitter and the receiver, an authentication process for the peer device of the other party with the synchronously changing parameter according to the preset policy during a request initiating interaction carried out through the pre-determined channel; and

not initiating the QKD process if either device fails the authentication.

6. The authentication method of Claim 2, wherein the second pre-provisioned algorithm is performed by calculating the receiver authentication information according to receiver identification information and a variant of the synchronously changing parameter according to a preset policy by both the transmitter and the receiver, wherein the receiver identification information on the transmitter side is pre-provisioned or sent to the transmitter by the receiver through a pre-determined channel.

7. The authentication method of Claim 6, wherein the variant of the synchronously changing parameter according to the preset policy comprises at least one of the parameter itself, and a result obtained from processing the parameter with a preset mathematical transformation method.

8. The authentication method of Claim 4, wherein synchronously changing parameter according to the preset policy by both the transmitter and the receiver comprises a number of times the transmitter and the receiver perform the QKD processes.

9. The authentication method of Claim 4, wherein calculating the authentication information comprises calculating the corresponding authentication information with a hash function.

10. The authentication method of Claim 1, wherein transmitting of quantum states comprising key information and the transmitter authentication information comprises transmitting quantum states of control information and data information with respectively different wavelengths in a preset information format, wherein the data information comprises the key information and the transmitter authentication information.

11. The authentication method of Claim 10, wherein the preset information format comprises using control information as prefixes for the authentication information and the key information.

12. The authentication method of Claim 11, wherein a wavelength carrying quantum states of the control information used as the prefix of the authentication information is different from a wavelength carrying quantum states of the control information used as the prefix of the key information.

13. The authentication method of Claim 11, wherein the preset information format comprises the control information used as the prefix of the authentication information and the control information used as the prefix of the key information having different codes, and the different codes are preset by the transmitter and the receiver or determined via negotiation through a pre-determined channel,

wherein at least one of a basis for preparing and a basis of measuring quantum states of control information is preset by the transmitter and the receiver or determined via negotiation through the pre-determined channel.

14. The authentication method of Claim 10, wherein the preset information format comprises using common control information as a prefix of the authentication information and the key information, and the length of the authentication information between the control information and the key information is preset by the transmitter and the receiver or determined via negotiation through a pre-determined channel.

15. An authentication apparatus used in a QKD process, the apparatus comprising:

a transmitter identity information generating unit configured to generate transmitter authentication information with a first pre-provisioned algorithm, wherein the transmitter authentication information varies dynamically in different QKD processes initiated towards a receiver;

a basis of preparation selection unit configured to select a basis of preparation for the transmitter authentication information according to a basis selection rule agreed upon with a peer device participating in the QKD process; and

a quantum states transmitting unit configured to transmit quantum states containing at least key information and the transmitter authentication information to the peer device in a preset manner,

wherein the apparatus is deployed on a quantum communication transmitter device participating in a QKD process.

16. The authentication apparatus of Claim 16, wherein the apparatus further comprises:

a receiver identity information receiving unit configured to receive information returned by the peer device after the quantum states transmitting unit completes the quantum states transmitting operation, wherein the information comprises at least receiver authentication information;

a receiver identity information calculation unit configured to calculate receiver authentication information with a second pre-provisioned algorithm; and

a receiver authentication unit configured to determine that the receiver is authenticated when the receiver authentication the receiver authentication information received is consistent with the calculation result and further configured to determine that the receiver is not authenticated and end the QKD process otherwise.

17. The authentication apparatus of Claim 16, wherein the apparatus further comprises:

an original key screening unit configured to determine a correct measurement basis for the quantum states of the key information and to screen the original key after the receiver authentication unit determines that the receiver is authenticated;

a correct measurement basis disclosing unit configured to disclose the correct measurement basis for the quantum states of the key information through a pre-determined channel; and

a shared quantum key generating unit configured to acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes,

wherein the information received by the receiver identity information receiving unit further comprises a measurement basis used by the peer device for measuring quantum states of the key information.

18. An authentication apparatus used in a QKD process, the apparatus comprising:

a quantum states receiving and differentiating unit configured to receive quantum states sent by a peer device participating in the QKD process, and to differentiate the received quantum states of various information in the same preset manner as that of the peer device;

a transmitter identity information calculation unit configured to calculate transmitter authentication information with the a first pre-provisioned algorithm used by the peer device;

an identity information quantum states measurement unit configured to select a measurement basis according to the same basis selection rule as that of the peer device, and to measure a received plurality of quantum states of transmitter authentication information; and

a transmitter authentication unit configured to determine whether received plurality of quantum states is consistent with the calculated transmitter authentication information, to determine that a transmitter is authenticated when the measurement result is consistent, and to determine that the transmitter is not authenticated and end the QKD process otherwise,

wherein the apparatus is deployed on a quantum communication receiver device participating in a QKD process.

19. The authentication apparatus of Claim 18, wherein the apparatus further comprises:

a receiver identity information generating unit configured to generate receiver authentication information with the a second pre-provisioned algorithm used by the peer device after the transmitter authentication unit determines that the transmitter is authenticated; and

a receiver identity information transmitting unit configured to transmit the receiver authentication information to the peer device.

20. The authentication apparatus used in the QKD process of Claim 19, wherein the apparatus further comprises:

a key information quantum states measurement basis disclosing unit configured to randomly select a measurement basis to measure received quantum states of key information, and to disclose the measurement basis through a pre-determined channel after the transmitter authentication unit determines that the transmitter is authenticated;

a correct measurement basis receiving unit configured to receive a correct measurement basis of the quantum states of the key information sent by the peer device through the pre-determined channel; and

a screening and shared quantum key generating unit configured to screen an original key and acquire a final shared quantum key through bit error rate estimation, error correction and privacy amplification processes.

1/12

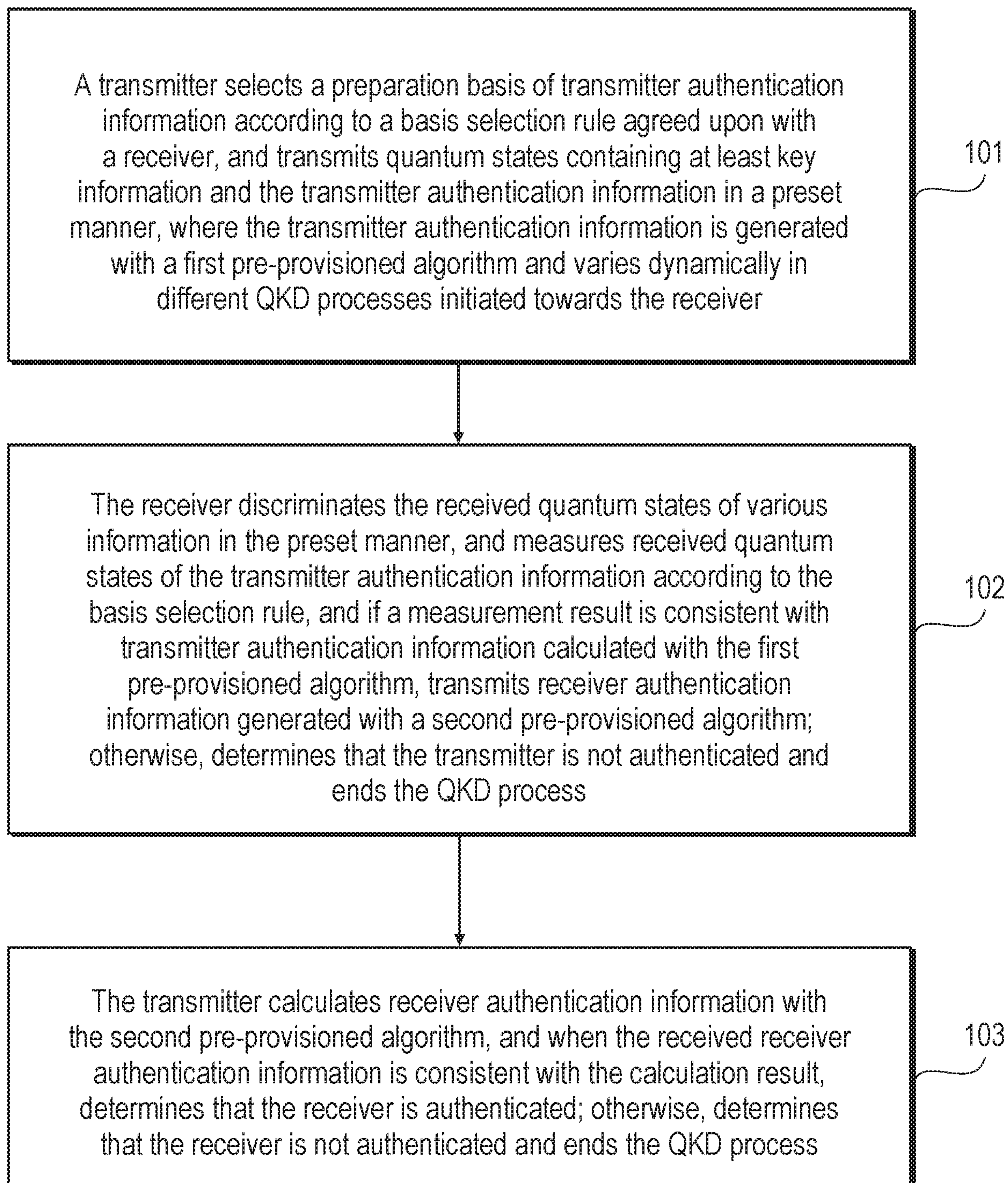


FIG. 1

2/12

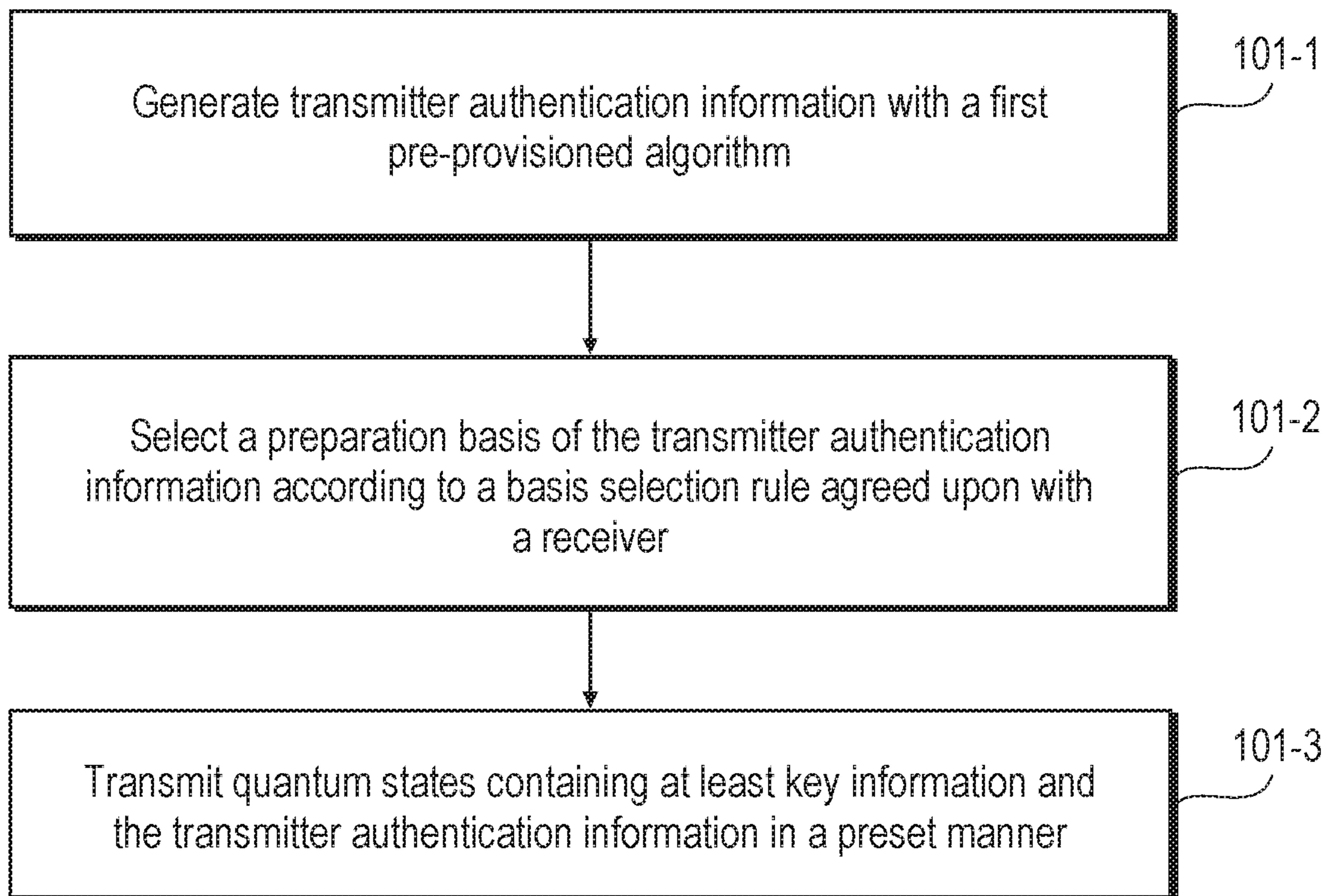


FIG. 2

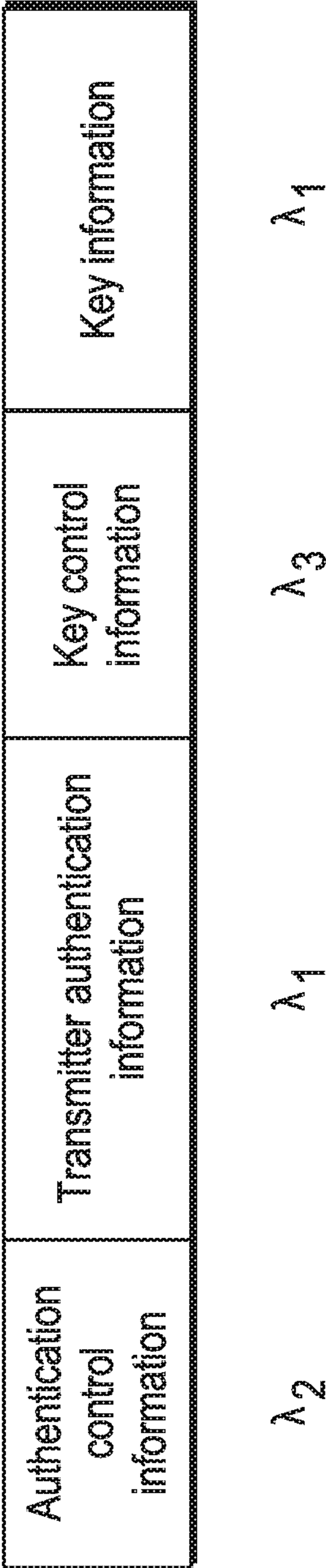


FIG. 3

Authentication control information 00000	Transmitter authentication information	Key control information 11111	Key information
---	---	-------------------------------------	-----------------

λ_2 λ_1 λ_2 λ_1

FIG. 4

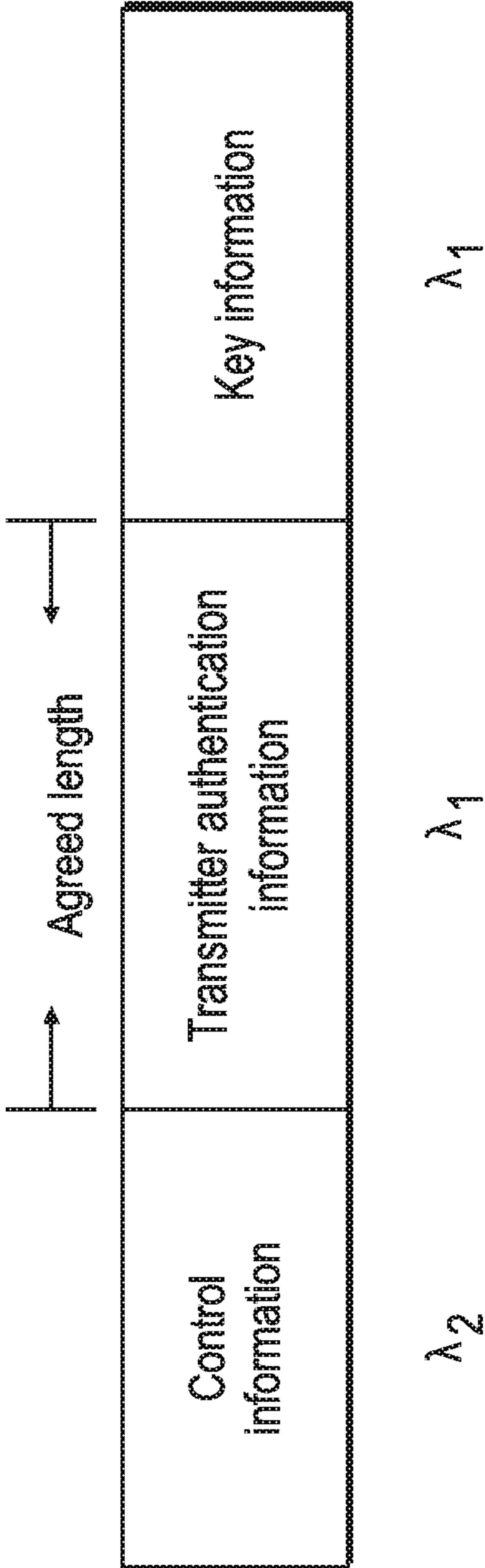


FIG. 5

6/12

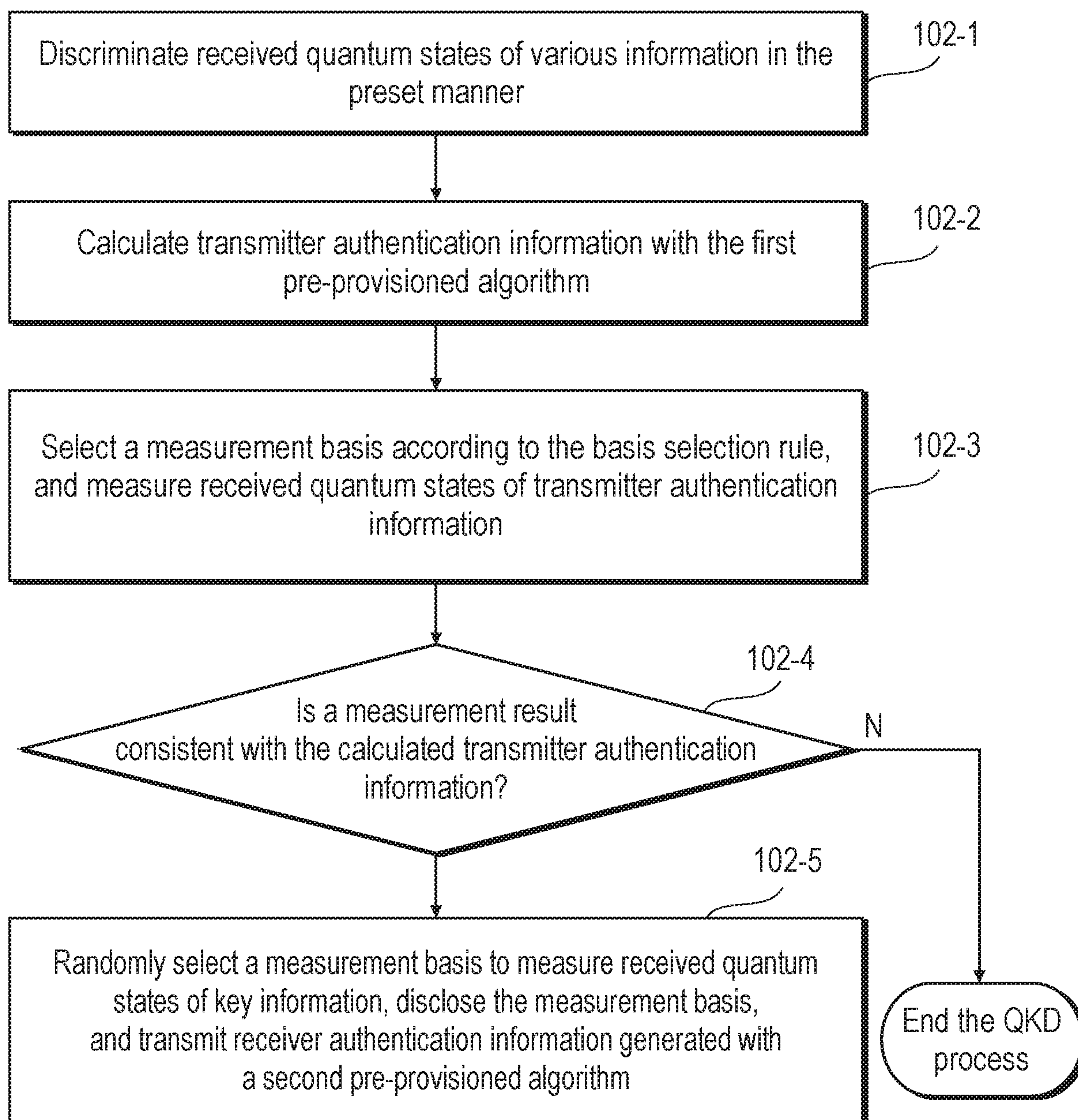


FIG. 6

7/12

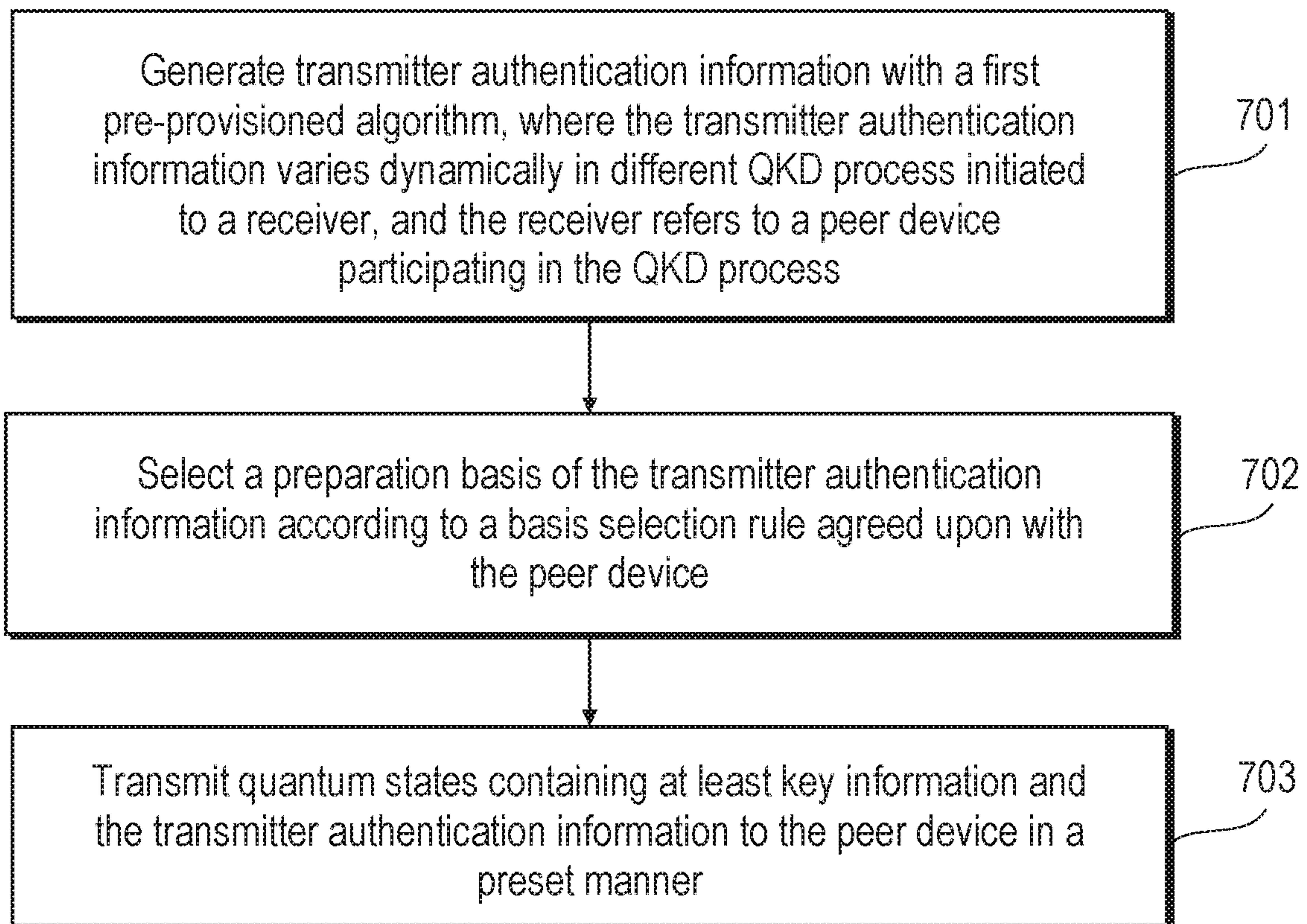


FIG. 7

8/12

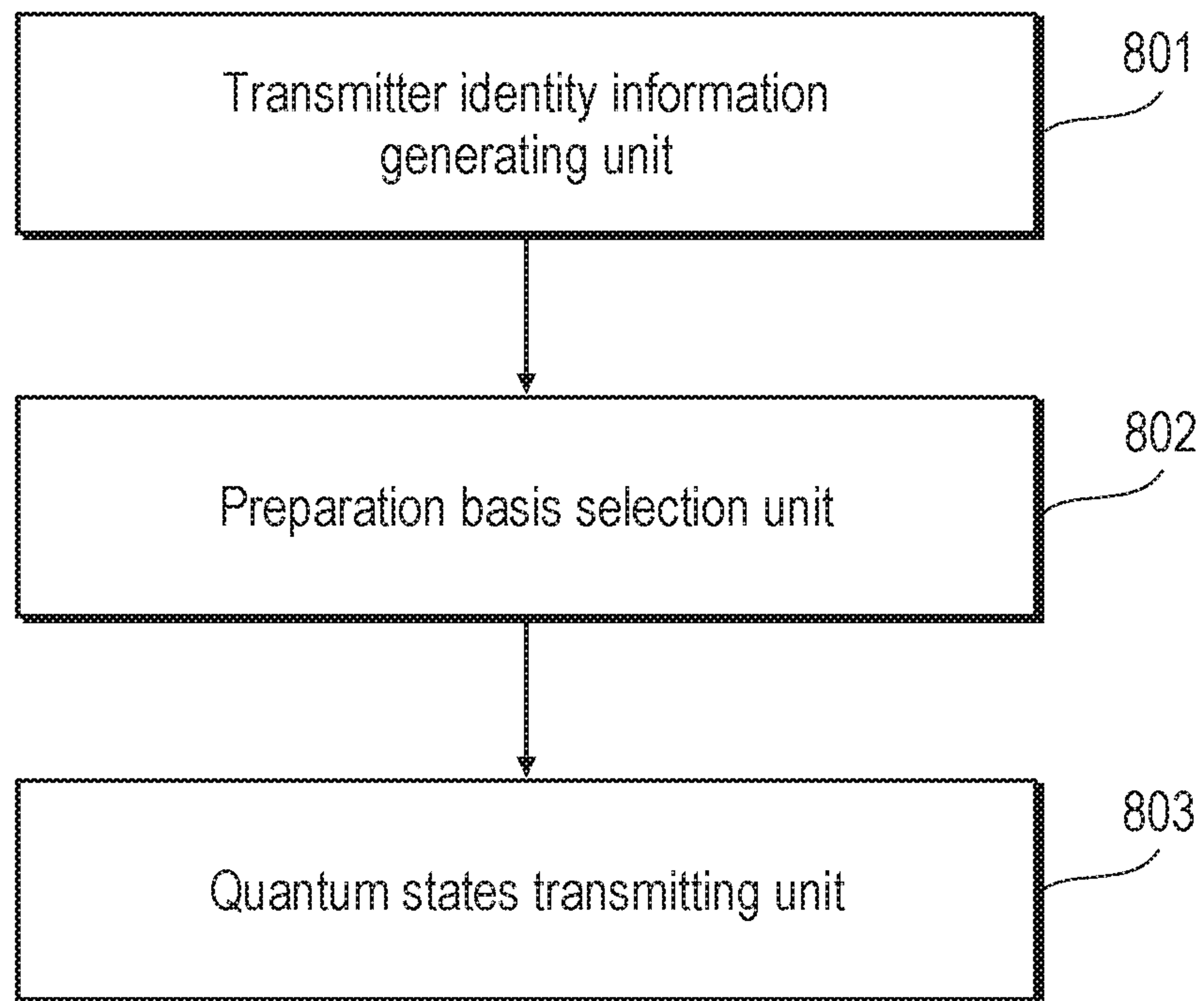


FIG. 8

9/12

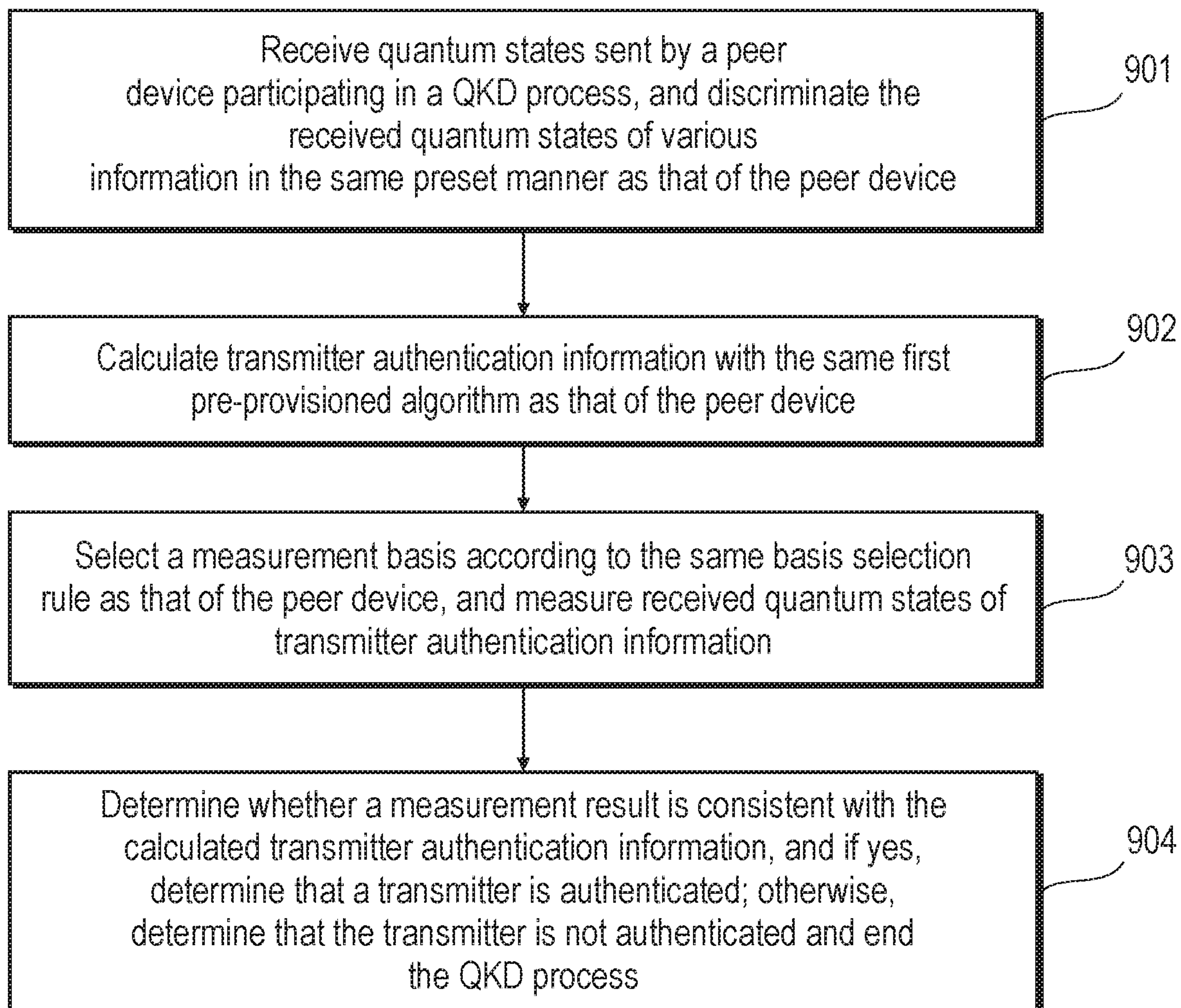


FIG. 9

10/12

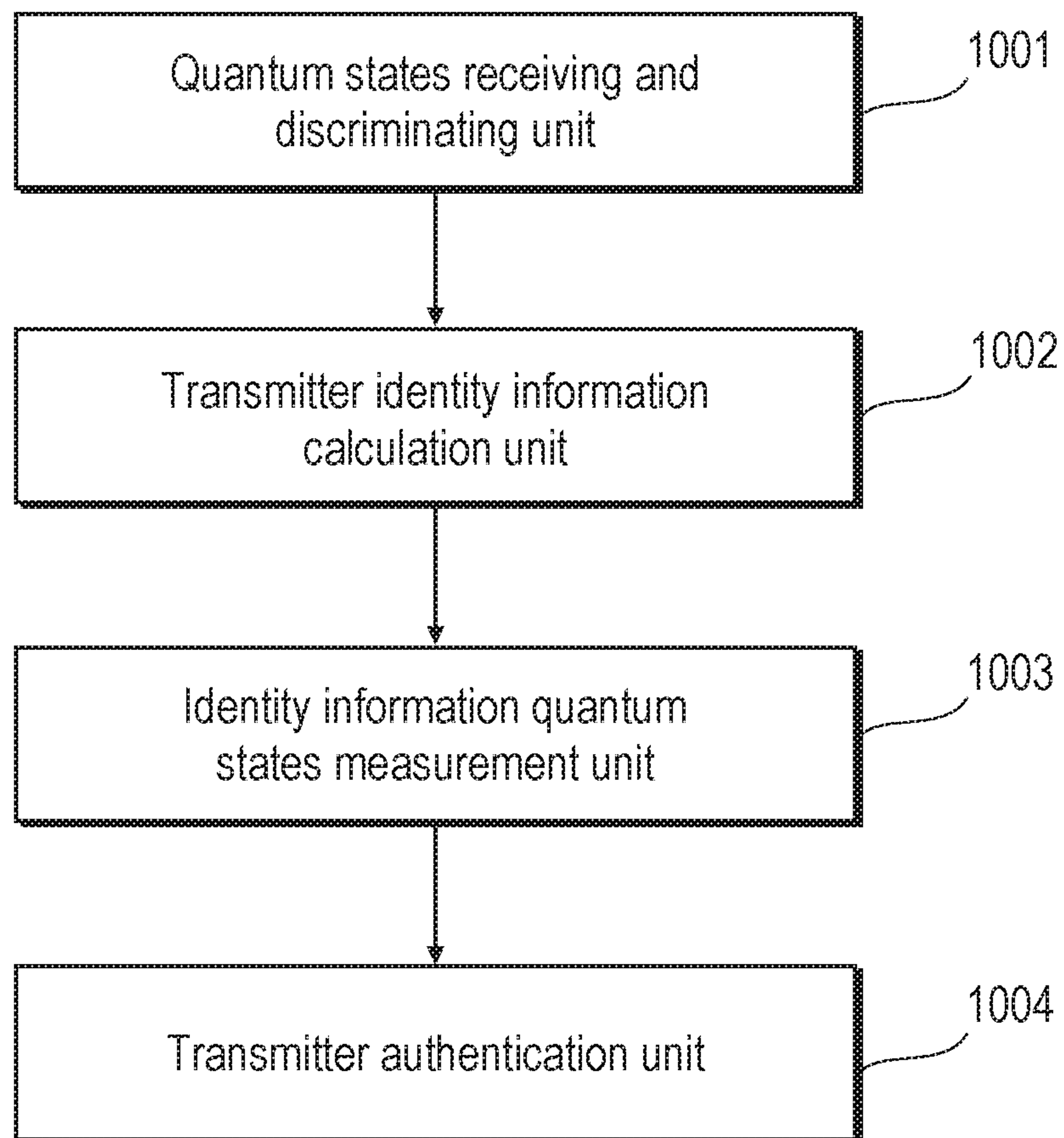


FIG. 10

11/12

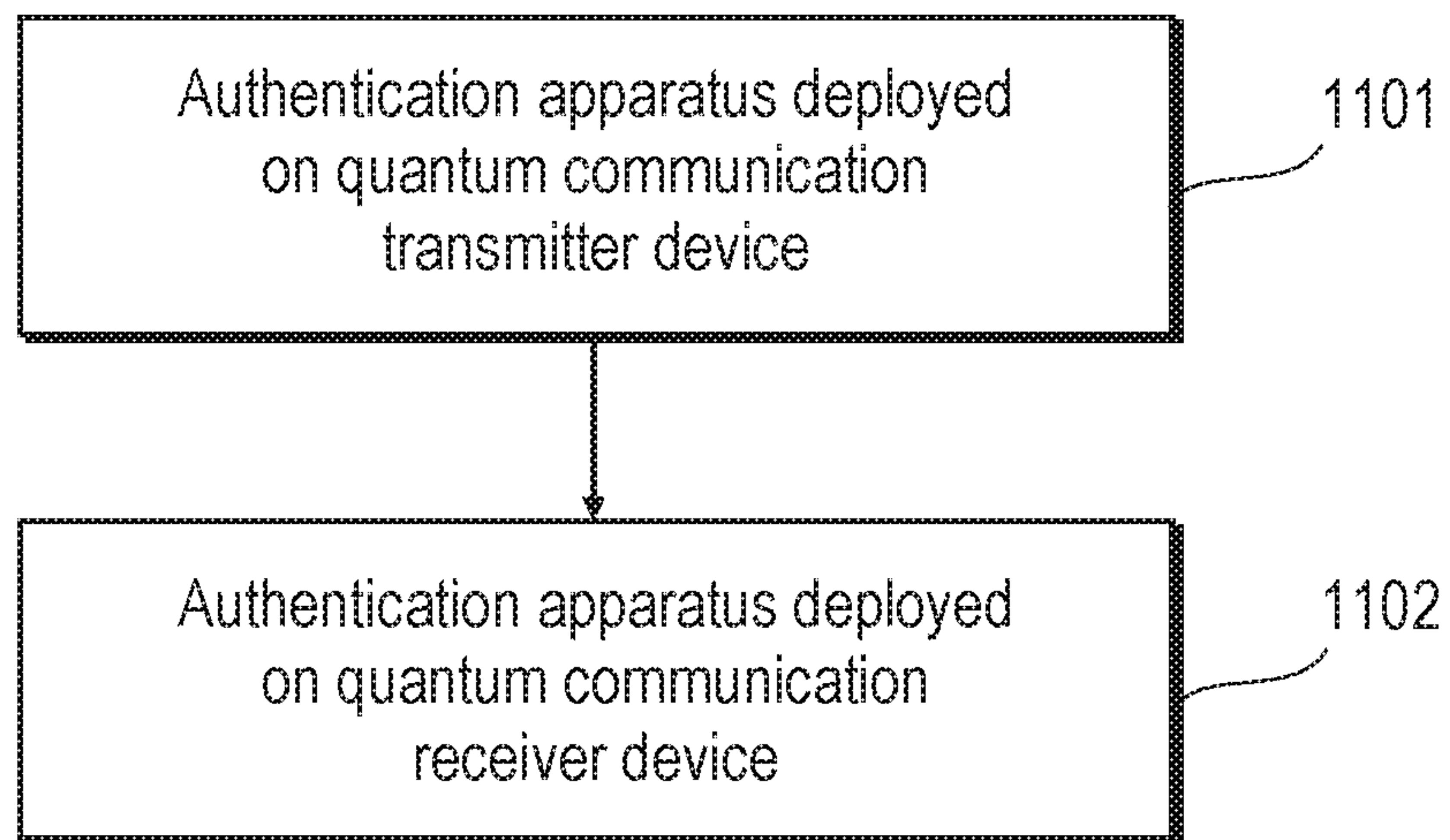
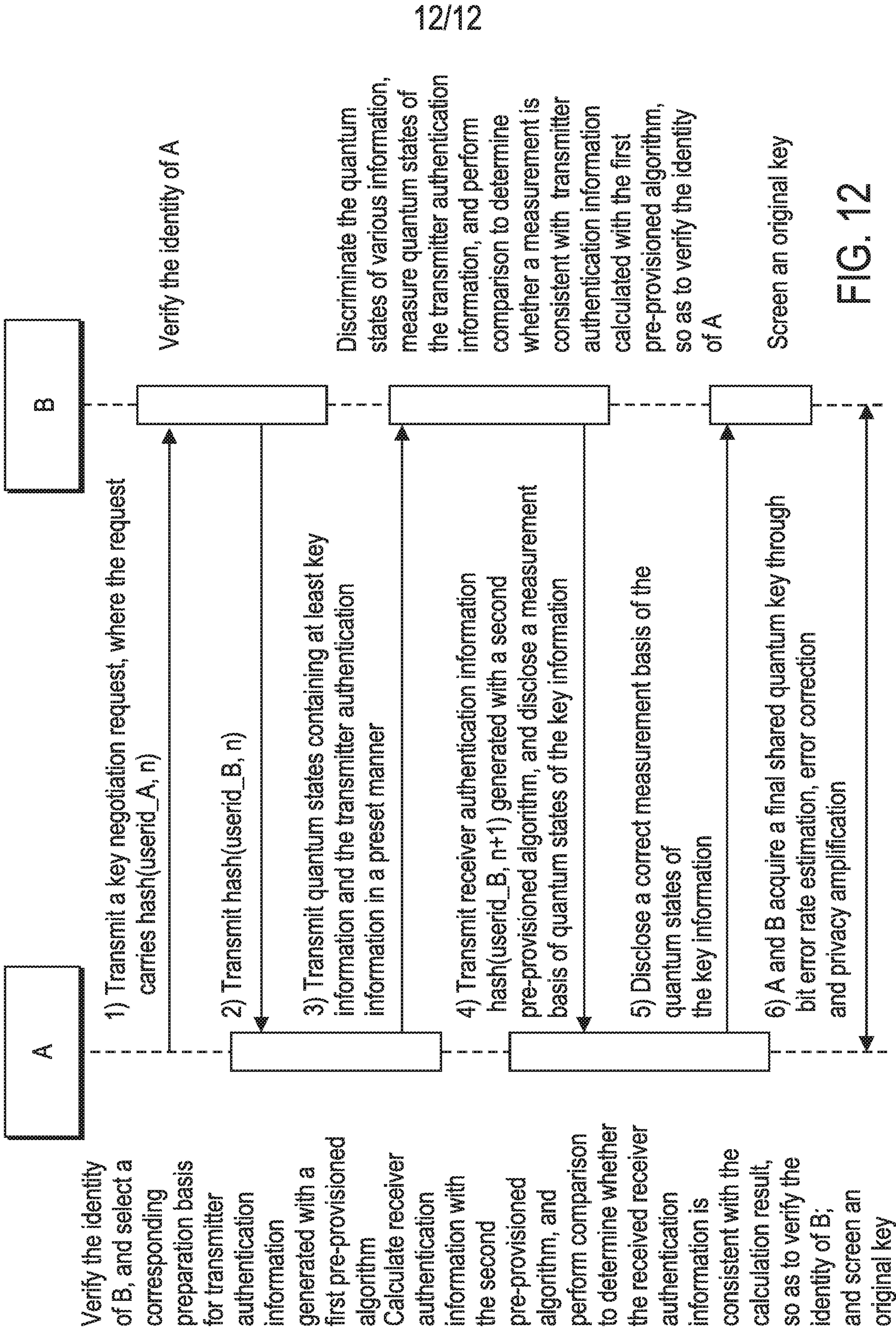


FIG. 11



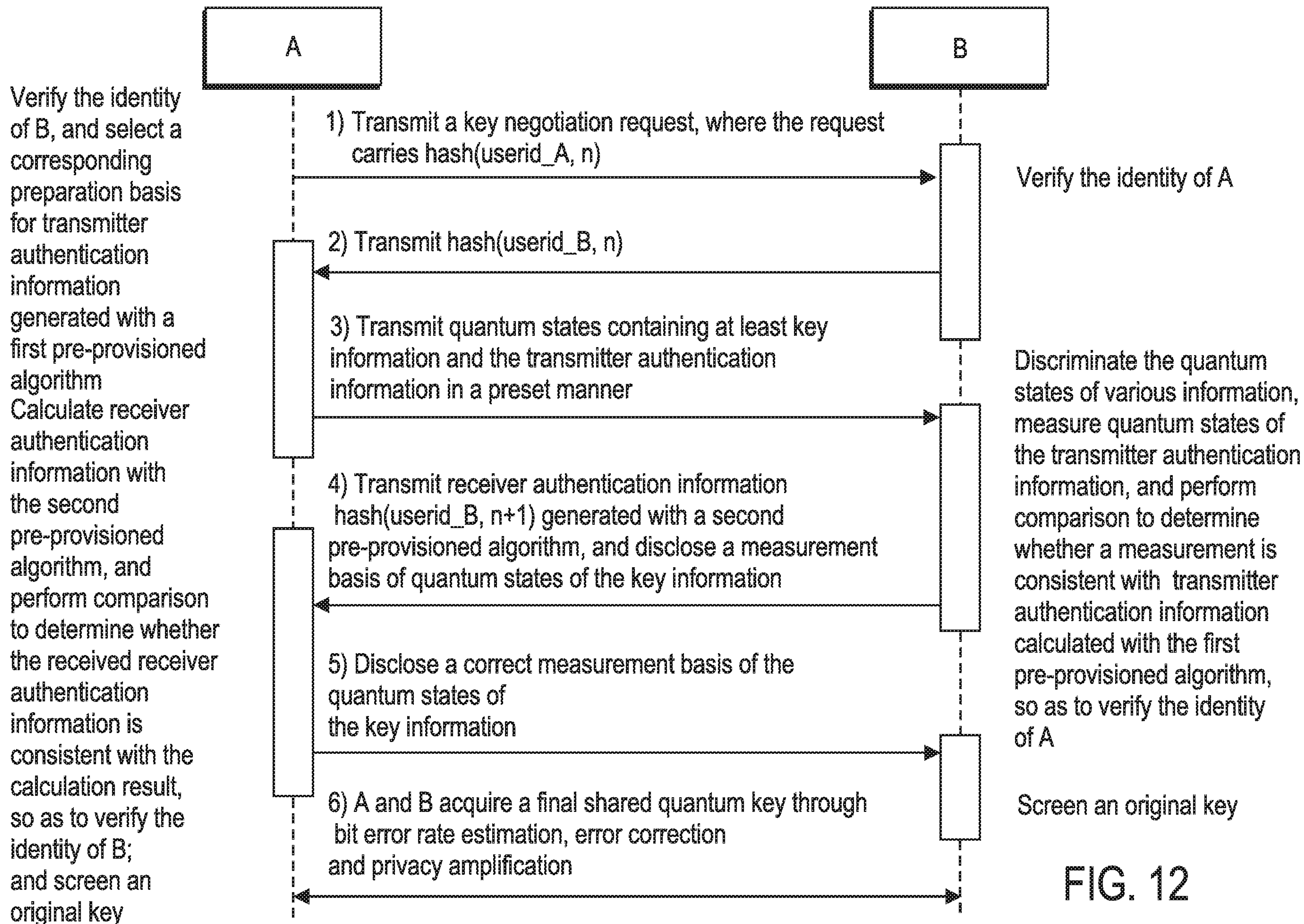


FIG. 12