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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 March 2023 (16.03.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/036395 A1

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/EP2021/074534

(22) International Filing Date:
07 September 2021 (07.09.2021)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building Bantian Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventor; and
(71) Applicant *(for MN only)*: **FRESSANCOURT, Antoine** [FR/DE]; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(72) Inventors: **IANNONE, Luigi**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE). **LOU, Zhe**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(74) Agent: **KREUZ, Georg**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: DEVICES AND METHODS FOR LIGHTWEIGHT PRIVACY PRESERVING EXCHANGE OF A KEY REFERENCE

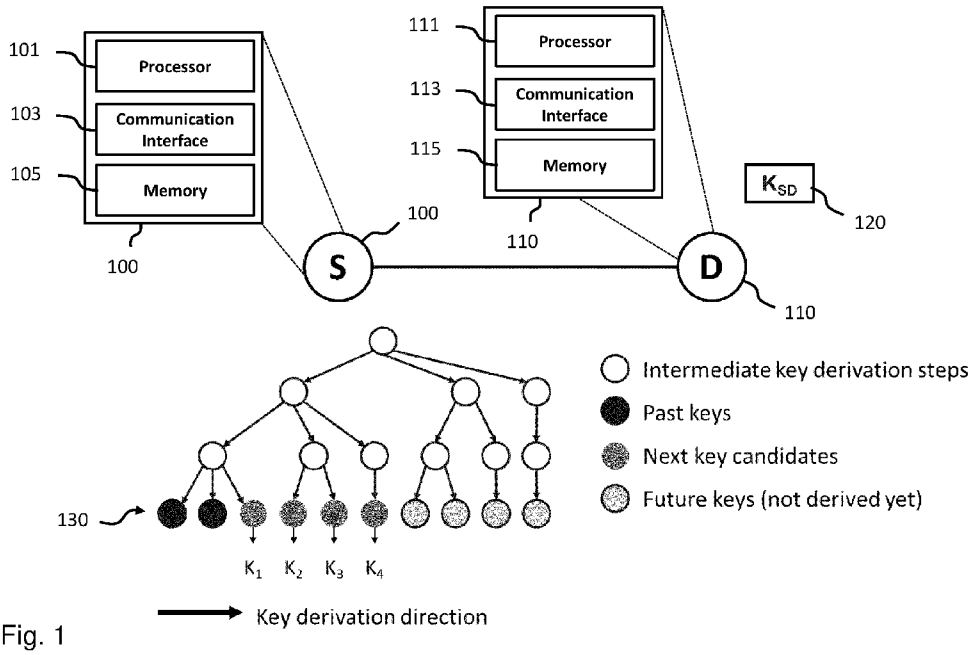

Fig. 1

(57) Abstract: Devices and methods for exchanging a lightweight anonymous key reference between a source node (100) and a destination (110) node in a communication network are disclosed. The source node (100) comprises a processing circuitry (101) configured to encrypt a bit pattern agreed between the source node (100) and the destination node (110) using a selected encryption key of a plurality of candidate encryption keys agreed between the transmitter node and the receiver node based on a key derivation mechanism. The source node (100) further comprises a communication interface (103) configured to transmit the encrypted bit pattern to the destination node (110).

[Continued on next page]

WO 2023/036395 A1

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))*

DEVICES AND METHODS FOR LIGHTWEIGHT PRIVACY PRESERVING EXCHANGE OF A KEY REFERENCE

TECHNICAL FIELD

The present disclosure relates to communication networks in general. More specifically, the present disclosure relates to devices and methods for exchanging a lightweight anonymous key reference between a source node and a destination node in a communication network.

BACKGROUND

For developing of network layer anonymity solutions in a communication network with a plurality of communication nodes privacy-preserving network protocols have been developed using two main approaches. In a first approach a trusted third party is employed to break the relationship between the sender and receiver. In a second approach a source routing system is used in which the privacy of the path determined by the source node and taken by a packet in the communication network is protected using cryptographic mechanisms.

More specifically, in the second approach, a source node determines a path to be taken by the packet it sends to the destination node, and includes a description of this path in the packets it will send to the destination node. In order to protect the privacy, i.e. identity of the source node and the destination node, it should be impossible for an intermediate routing node along the path to be able to determine what the full path taken by the packets in the network is. In other words, an intermediate routing node along the path should only be able to determine where the packet comes from (i.e. the previous upstream hop node along the path), and where it should send the packet (i.e. the next downstream hop node along the path). To allow the communication between the source node and the destination node to be perfectly private, those intermediate routing nodes further should not be able to determine the path's length, nor to use any information carried by the packet to correlate packets belonging to the same network flow together.

To further protect the privacy of a sender and a receiver of packets in a source-routed communication network, the path defined in a packet header should be protected and changed after each intermediate node. This can be done either using public key cryptography, which involves very heavy computations at each node, or using symmetric

key cryptography, which can support operating encryption/decryption at the line's rate, but requires that the node involved in the communication use either a secret key or a shared secret key.

When a secret key is used, to allow the source node to determine the source routed path, each intermediate routing node sends the source node an encrypted routing segment containing the information needed to route the packet. As this segment does not change with each packet, it can be used to correlate two packets following the same path, which raises a privacy issue.

When a shared secret key is used, the source node must give a pointer or an indication to each intermediate route node about which shared key they should use. If this reference is not changed in each packet belonging to the same flow, then this reference constitutes metadata that can be used to associate packets following the same path together, which raises the exact same privacy issue as in the previous scenario using a secret key.

In light of the above, there is a need for improved devices and methods for exchanging a lightweight anonymous key reference between a source node and a destination node in a communication network.

SUMMARY

It is an objective of the present disclosure to provide improved devices and methods for exchanging a lightweight anonymous key reference between a source node and a destination node in a communication network.

The foregoing and other objectives are achieved by the subject matter of the independent claims. Further implementation forms are apparent from the dependent claims, the description and the figures.

Generally, embodiments disclosed herein allow a source node and a destination node to exchange an anonymous key reference based on one or more of the following elements. A predictable and configurable key derivation scheme, which may loosely be synchronized between the source node and the destination node, for deriving a set of identical potential key candidates at the source node and the destination node. A fixed or dynamic common bit pattern that will be encrypted by both the source node and the

destination using one or more of the potential key candidates. A look-up table used by the destination node for matching the common bit pattern encrypted by the source node using one of the potential key candidates with the respective common bit pattern encrypted by the destination node using each of the potential key candidates. The destination node may decrypt further encrypted data provided by the source node based on the key candidate identified based on the common bit pattern encrypted by the source node and the look-up table. To indicate the candidate key to be used by the destination node, the source node may include the common pattern encrypted by the source node in a message to the destination node.

More specifically, according to a first aspect a source node configured to securely exchange a key reference with a destination node in a communication network is provided. The source node comprises a processing circuitry configured to encrypt a bit pattern agreed between the source node and the destination node based on a selected encryption key of a plurality of candidate encryption keys. Moreover, the source node comprises a communication interface configured to transmit the encrypted bit pattern to the destination node.

In a further possible implementation form, the processing circuitry is further configured to encrypt a payload based on the selected encryption key and wherein the communication interface is configured to transmit the encrypted bit pattern and the encrypted payload to the destination node.

In a further possible implementation form, the processing circuitry is configured to encrypt a concatenation of the bit pattern and the payload using the selected encryption key or a key stream based on the selected encryption key.

In a further possible implementation form, the processing circuitry is configured to encrypt the concatenation of the bit pattern and the payload using an XOR operation with the selected encryption key or with the key stream based on the selected encryption key.

In a further possible implementation form, the processing circuitry is configured to generate the plurality of candidate encryption keys using a shared master key and a key derivation scheme agreed between the source node and the destination node.

In a further possible implementation form, the key derivation scheme is based on the Derive Unique Key Per Transaction, DUKPT, scheme defined in ANSI X9.24, in particular a O-DUKPT scheme.

According to a second aspect a method of generating a key reference at a source node in a communication network is provided. The method comprises a step of encrypting a bit pattern agreed between the source node and a destination node using a selected encryption key of a plurality of candidate encryption keys. Moreover, the method comprises a step of transmitting the encrypted bit pattern to the destination node.

The method according to the second aspect can be performed by the source node according to the first aspect. Thus, further features of the method according to the second aspect result directly from the functionality of the source node according to the first aspect as well as its different implementation forms and embodiments described above and below.

According to a third aspect a destination node configured to securely exchange a key reference with a source node 100 in a communication network is provided. The destination node comprises a communication interface configured to receive an encrypted bit pattern from the source node. Moreover, the destination node comprises a processing circuitry configured to select based on the encrypted bit pattern an encryption key of a plurality of candidate encryption keys.

In a further possible implementation form, the communication interface is further configured to receive an encrypted payload from the source node and the processing circuitry is further configured to decrypt the encrypted payload based on the selected encryption key.

In a further possible implementation form, the processing circuitry is configured to decrypt a concatenation of the encrypted bit pattern and the payload using the selected encryption key or a key stream based on the selected encryption key.

In a further possible implementation form, the processing circuitry is configured to decrypt the concatenation of the encrypted bit pattern and the payload using an XOR operation with the selected encryption key or with the key stream based on the selected encryption key.

In a further possible implementation form, the processing circuitry is configured to generate the plurality of candidate encryption keys using a shared master key and a key derivation scheme agreed between the source node and the destination node.

In a further possible implementation form, the key derivation scheme is based on the Derive Unique Key Per Transaction, DUKPT, scheme defined in ANSI X9.24, in particular a O-DUKPT scheme.

In a further possible implementation form, the destination node further comprises a memory configured to store a look-up table, wherein the look-up table stores for each of the plurality of candidate encryption keys the corresponding encrypted bit pattern.

According to a fourth aspect a method of processing a key reference at a destination node in a communication network is provided. The method comprises a step of receiving an encrypted bit pattern from a source node of the communication network. Moreover, the method comprises a step of selecting based on the encrypted bit pattern an encryption key of a plurality of candidate encryption keys.

The method according to the fourth aspect can be performed by the destination node according to the third aspect. Thus, further features of the method according to the fourth aspect result directly from the functionality of the destination node according to the third aspect as well as its different implementation forms and embodiments described above and below.

According to a fifth aspect a computer program product is provided, comprising a computer-readable storage medium for storing program code which causes a computer or a processor to perform the method according to the second aspect or the method according to the fourth aspect, when the program code is executed by the computer or the processor.

Details of one or more embodiments are set forth in the accompanying drawings and the description below. Other features, objects, and advantages will be apparent from the description, drawings, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, embodiments of the present disclosure are described in more detail with reference to the attached figures and drawings, in which:

Fig. 1 is a schematic diagram illustrating a communication network with a source node according to an embodiment for exchanging a key reference with a destination node according to an embodiment;

Fig. 2 is a schematic diagram illustrating a key derivation scheme used by a source node according to an embodiment and a destination node according to an embodiment as well as a look-up table used by the destination node according to an embodiment;

Figs. 3 and 4 are schematic diagrams illustrating processing steps implemented by a source node according to an embodiment and a destination node according to an embodiment for exchanging a key reference;

Fig. 5 is a flow diagram illustrating a method for generating a key reference at a source node according to an embodiment; and

Fig. 6 is a flow diagram illustrating a method for processing a key reference at a destination node according to an embodiment.

In the following, identical reference signs refer to identical or at least functionally equivalent features.

DETAILED DESCRIPTION OF THE EMBODIMENTS

In the following description, reference is made to the accompanying figures, which form part of the disclosure, and which show, by way of illustration, specific aspects of embodiments of the present disclosure or specific aspects in which embodiments of the present disclosure may be used. It is understood that embodiments of the present disclosure may be used in other aspects and comprise structural or logical changes not depicted in the figures. The following detailed description, therefore, is not to be taken in a limiting sense, and the scope of the present disclosure is defined by the appended claims.

For instance, it is to be understood that a disclosure in connection with a described method may also hold true for a corresponding device or system configured to perform the method and vice versa. For example, if one or a plurality of specific method steps are described, a corresponding device may include one or a plurality of units, e.g. functional units, to perform the described one or plurality of method steps (e.g. one unit performing the one or plurality of steps, or a plurality of units each performing one or more of the plurality of steps), even if such one or more units are not explicitly described or illustrated in the figures. On the other hand, for example, if a specific apparatus is described based on one or a plurality of units, e.g. functional units, a corresponding method may include one step to perform the functionality of the one or plurality of units (e.g. one step performing the functionality of the one or plurality of units, or a plurality of steps each performing the functionality of one or more of the plurality of units), even if such one or plurality of steps are not explicitly described or illustrated in the figures. Further, it is understood that the features of the various exemplary embodiments and/or aspects described herein may be combined with each other, unless specifically noted otherwise.

Figure 1 illustrates a source or first node 100 according to an embodiment and a destination or second node 110 of a communication network. In an embodiment, the source node 100 and the destination node 110 may be a communication node in an IP-based communication network, such as a server, an intermediate router or a client.

As illustrated in figure 1, the source node 100 comprises a processing circuitry 101 and a communication interface 103. The processing circuitry 101 of the source node 100 may be implemented in hardware and/or software. The hardware may comprise digital circuitry, or both analog and digital circuitry. Digital circuitry may comprise components such as application-specific integrated circuits (ASICs), field-programmable arrays (FPGAs), digital signal processors (DSPs), or general-purpose processors. The communication interface 103 may be a wired and/or wireless communication interface configured to exchange data packets, e.g. IP data packets with other nodes of the communication network. As illustrated in figure 1, the source node 100 may further comprise a non-transitory memory 105 configured to store data and executable program code which, when executed by the processing circuitry 101 causes the source node 100 to perform the functions, operations and methods described herein.

Likewise, the destination node 110 comprises a processing circuitry 111 and a communication interface 113. The processing circuitry 111 of the destination node 110

may be implemented in hardware and/or software. The hardware may comprise digital circuitry, or both analog and digital circuitry. Digital circuitry may comprise components such as application-specific integrated circuits (ASICs), field-programmable arrays (FPGAs), digital signal processors (DSPs), or general-purpose processors. The communication interface 113 may be a wired and/or wireless communication interface configured to exchange data packets, e.g. IP data packets with other nodes of the communication network. As illustrated in figure 1, the destination node 110 may further comprise a non-transitory memory 115 configured to store data and executable program code which, when executed by the processing circuitry 111 causes the destination node 110 to perform the functions, operations and methods described herein.

As illustrated in figure 1, the source node 100 and the destination node 110 may have previously negotiated a shared secret master key k_{SD} 120, for instance, by means of public and private keys. Moreover, the source node 100 and the destination node 110 may have agreed on one or more parameters to personalize a key derivation scheme. In an embodiment, the key derivation scheme may be the Derive Unique Key Per Transaction (DUKPT) scheme defined in ANSI X9.24. In a further embodiment, the key derivation scheme is the Optimal-DUKPT scheme (O-DUKPT) described in detail in Brier, Eric, and Thomas Peyrin, "A forward-secure symmetric-key derivation protocol", International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, 2010.

In the embodiment illustrated in figure 1, the source node 100 and the destination node 110 are both configured to use the key derivation scheme in a predictive manner in that starting from the first key, they compute the keys in the order defined by the O-DUKPT scheme disclosed in Brier, Eric, and Thomas Peyrin, "A forward-secure symmetric-key derivation protocol", International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, 2010.

In an embodiment, the source node 100 and the destination node 110 know about a last key that has been used to secure a content exchanged between the source node 100 and the destination node 110.

As illustrated in figure 2, the source node 100 and the destination node 110 moreover have negotiated a common bit pattern 140, by way of example the common bit pattern 10101010. As will be described in more detail in the following, the common bit pattern 140

allows the source node 100 and the destination node 110 to exchange an anonymous key reference. In an embodiment, the common bit pattern 140 may be a fixed bit pattern or a dynamic string of bits (changing according to a rule both known to the source node 100 and the destination node 110) that both the source node 100 and the destination node 110 will be able to recognize.

The processing circuitry 111 of the destination node 110 is configured to compute a couple of key candidates, i.e. candidate encryption keys k_1, k_2, k_3 and k_4 130 using the shared master key k_{SD} 120 and the parameterized key derivation scheme, in particular the O-DUKPT scheme. In an embodiment, those key candidates are the *n* next keys that will be used by the source node 100 and the destination node 110 to exchange encrypted information. The destination node 110 knows what the next *n* keys to be derived are because of the predictability of the key derivation scheme. In an embodiment, the processing circuitry 111 of the destination node 110 is configured to encrypt the mutually agreed bit pattern 140, e.g. the exemplary bit pattern 10101010, with each of the *n* key candidates, and to store the respective results, i.e. the bit pattern 140 encrypted with the respective key candidate in a matching look-up table 150 in the memory 115 of the destination node 110. In the embodiment illustrated in figure 2 the matching look-up table 150 has 2 columns, including a first column containing the encrypted bit patterns 140 and a second column containing the corresponding key candidate used for encrypting the bit pattern 140.

Figure 3 illustrates in more detail how the source node 100 may send a payload that may comprise security sensitive content 160 in encrypted form to the destination node 110. More specifically, as illustrated in figure 3, the processing circuitry 101 of the source node 100 is configured to concatenate the mutually agreed bit pattern 140, e.g. the exemplary bit pattern 10101010, with the security sensitive content 160 and to encrypt the resulting concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 using a selected key of the plurality of key candidates derived by the key derivation scheme. In an embodiment, the processing circuitry 101 of the source node 100 is configured to concatenate the mutually agreed bit pattern 140, e.g. the exemplary bit pattern 10101010, with the security sensitive content 160 by prepending the mutually agreed bit pattern 140, e.g. the exemplary bit pattern 10101010, to the security sensitive content 160. In an embodiment, the processing circuitry 101 of the source node 100 is configured to encrypt the resulting concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 based on a symmetric key encryption scheme. In

an embodiment, the processing circuitry 101 of the source node 100 is configured to encrypt the resulting concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 using an XOR operation with the selected key of the plurality of key candidates or a key stream based on the selected key. The encrypted concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 is transmitted via the communication interface 103 of the source node 100 to the destination node 110.

As illustrated in figure 4, once the communication interface 113 of the destination node 110 has received the encrypted concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 from the source node 100, the processing circuitry 111 of the destination node 110 may extract the encrypted bit pattern 140, for instance, from the beginning of the encrypted concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 and to determine based on the matching look-up table 150 the key candidate that has been used for arriving at the extracted encrypted bit pattern 140. Based on the such determined key candidate the processing circuitry 111 of the destination node 110 may decrypt the whole encrypted concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 and thereby retrieve the security sensitive content 160 in the clear. In an embodiment, the processing circuitry 111 of the destination node 110 is configured to decrypt the concatenation of the mutually agreed bit pattern 140 and the security sensitive content 160 using an XOR operation with the determined key of the plurality of key candidates or a key stream based on the determined key.

In an embodiment, the processing circuitry 111 of the destination node 110 may be configured to adjust the number of candidate keys to provide for some additional robustness. This is because, if an encrypted message sent from the source node 100 to the destination node 110 is lost, the destination node 110 may still determine the key candidate that has been used by the source node 100 for encrypting the next message. As will be appreciated, such a retrieval is straightforward, as long as the number of messages lost is smaller than the parameter *n*. If the number of messages lost is larger than the parameter *n*, the processing circuitry 111 of the destination node 110 may derive further key candidates using the mutually agreed key derivation scheme until a match is found, which may require a somewhat longer processing time at the destination node 110.

Figure 5 is a flow diagram illustrating a method 500 of generating a key reference at the source node 100. The method 500 comprises a step 501 of encrypting the bit pattern 140

agreed between the source node 100 and the destination node 110 using a selected encryption key of a plurality of candidate encryption keys 130. Moreover, the method 500 comprises a step 503 of transmitting the encrypted bit pattern to the destination node. The method 500 can be performed by the source node 100 according to an embodiment. Thus, further features of the method 500 result directly from the functionality of the source node 100 as well as its different embodiments described above and below.

Figure 6 is a flow diagram illustrating a method 600 of processing a key reference at the destination node 110. The method comprises a step 601 of receiving the encrypted bit pattern 140 from the source node 100. Moreover, the method 600 comprises a step 603 of selecting based on the encrypted bit pattern an encryption key of a plurality of candidate encryption keys. The method 600 can be performed by the destination node 110 according to an embodiment. Thus, further features of the method 600 result directly from the functionality of the destination node 110 as well as its different embodiments described above and below.

Embodiments disclose herein allow two parties to exchange a key reference pointing to a symmetric key used to secure confidential information without exchanging an explicit pointer to the key. Thus, embodiments disclosed herein allow reducing the amount of metadata sent with an encrypted message, which results in an improved privacy. Besides, if a very dynamic key derivation scheme is used, then each message may be sent using a different symmetric key, which strongly enhances message forward secrecy. Moreover, the use of a predictable, loosely synchronized key derivation mechanism in embodiments disclosed herein allows the communication system to survive packet losses without compromising its security and the performance and/or speed at which messages can be decrypted. As will be appreciated, the encrypted bit pattern 140 employed by embodiments disclosed herein plays the same role as a non-interactive key exchange after an initial setup phase for a fraction of the computational cost, allowing the embodiments disclosed herein to be used in low power and/or low latency use cases, such as IoT, line rate packet relay, and the like. The symmetric key exchange combined with a robust symmetric encryption scheme, as used by embodiments disclosed herein, makes the sequence of encrypted patterns indistinguishable from a sequence of random bit strings.

The person skilled in the art will understand that the "blocks" ("units") of the various figures (method and apparatus) represent or describe functionalities of embodiments of

the present disclosure (rather than necessarily individual "units" in hardware or software) and thus describe equally functions or features of apparatus embodiments as well as method embodiments (unit = step).

In the several embodiments provided in the present application, it should be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described embodiment of an apparatus is merely exemplary. For example, the unit division is merely logical function division and may be another division in an actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections may be implemented by using some interfaces. The indirect couplings or communication connections between the apparatuses or units may be implemented in electronic, mechanical, or other forms.

The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a plurality of network units. Some or all of the units may be selected according to actual needs to achieve the objectives of the solutions of the embodiments.

In addition, functional units in the embodiments disclosed herein may be integrated into one processing unit, or each of the units may exist alone physically, or two or more units are integrated into one unit.

CLAIMS

1. A source node (100) configured to exchange a key reference with a destination node (110) in a communication network, wherein the source node (100) comprises:

a processing circuitry (101) configured to encrypt a bit pattern (140) agreed between the source node (100) and the destination node (110) based on a selected encryption key of a plurality of candidate encryption keys (130); and

a communication interface (103) configured to transmit the encrypted bit pattern (150) to the destination node (110).

2. The source node (100) of claim 1, wherein the processing circuitry (101) is further configured to encrypt a payload (160) based on the selected encryption key and wherein the communication interface (103) is configured to transmit the encrypted bit pattern (150) and the encrypted payload (160) to the destination node (110).

3. The source node (100) of claim 2, wherein the processing circuitry (101) is configured to encrypt a concatenation of the bit pattern (140) and the payload (160) using the selected encryption key or a key stream based on the selected encryption key.

4. The source node (100) of claim 3, wherein the processing circuitry (101) is configured to encrypt the concatenation of the bit pattern (140) and the payload (160) using an XOR operation with the selected encryption key or with the key stream based on the selected encryption key.

5. The source node (100) of any one of the preceding claims, wherein the processing circuitry (101) is configured to generate the plurality of candidate encryption keys (130) using a shared master key (120) and a key derivation scheme agreed between the source node (100) and the destination node (110).

6. The source node (100) of claim 5, wherein the key derivation scheme is based on the Derive Unique Key Per Transaction, DUKPT, scheme defined in ANSI X9.24.

7. A method (500) of generating a key reference at a source node (100) in a communication network, wherein the method (500) comprises:

encrypting (501) a bit pattern (140) agreed between the source node (100) and a destination node (110) using a selected encryption key of a plurality of candidate encryption keys (130); and

transmitting (503) the encrypted bit pattern (140) to the destination node (110).

8. A destination node (110) configured to exchange a key reference with a source node (100) in a communication network, wherein the destination node (110) comprises:

a communication interface (113) configured to receive an encrypted bit pattern (150) from the source node (100); and

a processing circuitry (111) configured to select based on the encrypted bit pattern (140) an encryption key of a plurality of candidate encryption keys (130).

9. The destination node (110) of claim 8, wherein the communication interface (113) is further configured to receive an encrypted payload (160) from the source node (100) and wherein the processing circuitry (111) is further configured to decrypt the encrypted payload (160) based on the selected encryption key.

10. The destination node (110) of claim 8, wherein the processing circuitry (111) is configured to decrypt a concatenation of the encrypted bit pattern (150) and the payload (160) using the selected encryption key or a key stream based on the selected encryption key.

11. The destination node (110) of claim 10, wherein the processing circuitry (111) is configured to decrypt the concatenation of the encrypted bit pattern (150) and the payload (160) using an XOR operation with the selected encryption key or with the key stream based on the selected encryption key.

12. The destination node (110) of any one of claims 8 to 11, wherein the processing circuitry (111) is configured to generate the plurality of candidate encryption keys (130)

using a shared master key (120) and a key derivation scheme agreed between the source node (100) and the destination node (110).

13. The destination node (110) of claim 12, wherein the key derivation scheme is based on the Derive Unique Key Per Transaction, DUKPT, scheme defined in ANSI X9.24.

14. The destination node (110) of any one of claims 8 to 13, wherein the destination node (110) further comprises a memory (115) configured to store a look-up table, wherein the look-up table stores for each of the plurality of candidate encryption keys (130) the corresponding encrypted bit pattern (140).

15. A method (600) of processing a key reference at a destination node (110) in a communication network, wherein the method (600) comprises:

receiving (601) an encrypted bit pattern (140) from a source node (100); and

selecting (603) based on the encrypted bit pattern (140) an encryption key of a plurality of candidate encryption keys (130).

16. A computer program product comprising a computer-readable storage medium for storing program code which causes a computer or a processor to perform the method (500) of claim 7 or the method (600) of claim 15 when the program code is executed by the computer or the processor.

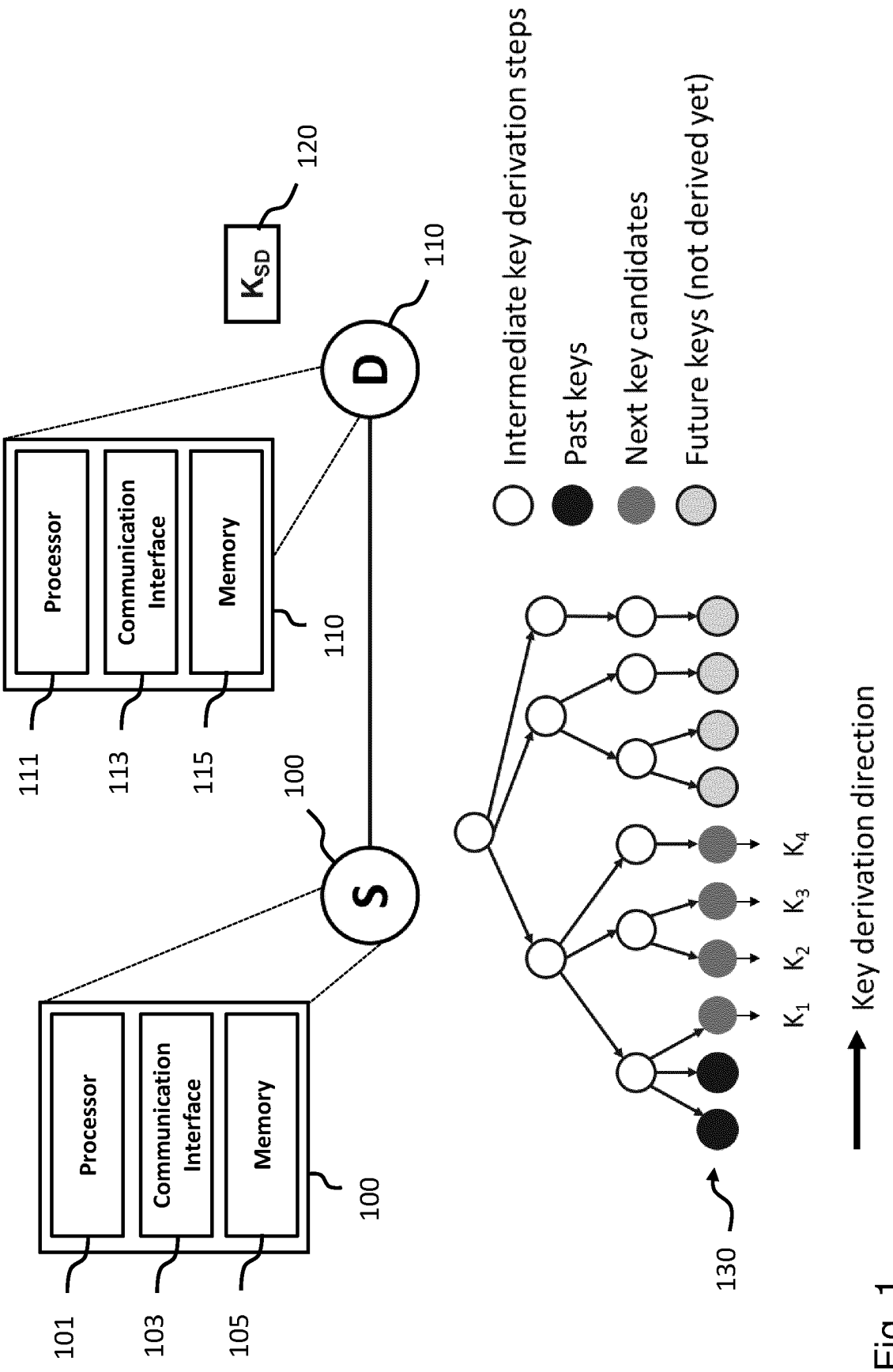
Processor
Communication Interface
Memory
101
103
105
100
S
100
Processor
Communication Interface
Memory
111
113
115
110
D
110
K_{SD}
120
Intermediate key derivation steps
Past keys
Next key candidates
Future keys (not derived yet)
130
K_1 K_2 K_3 K_4
Key derivation direction

Fig. 1

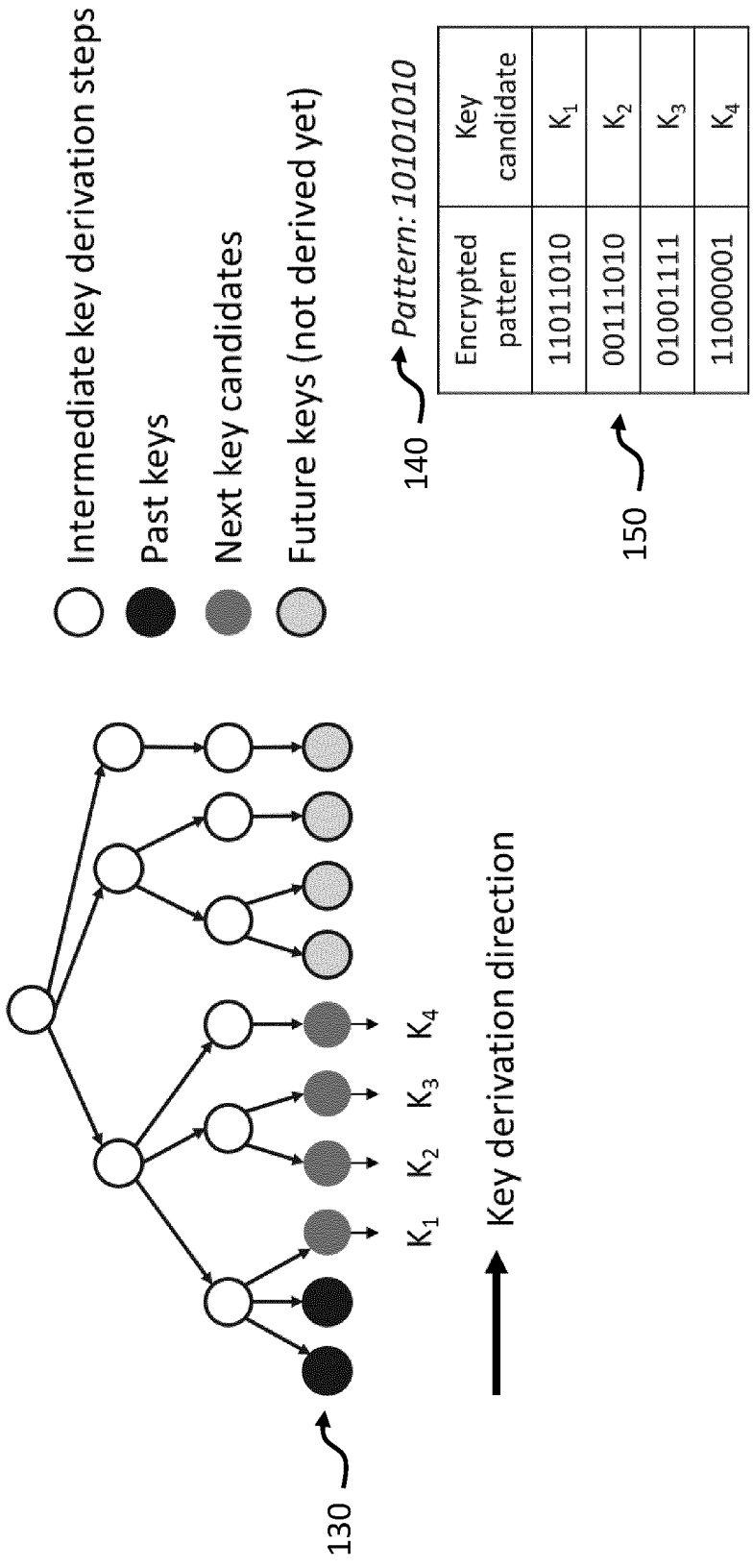
Intermediate key derivation steps
Past keys
Next key candidates
Future keys (not derived yet)
Pattern: 10101010
140
Encrypted pattern
Key candidate
11011010
K1
00111010
K2
01001111
K3
11000001
K4
150
130
K1 K2 K3 K4
Key derivation direction

Fig. 2

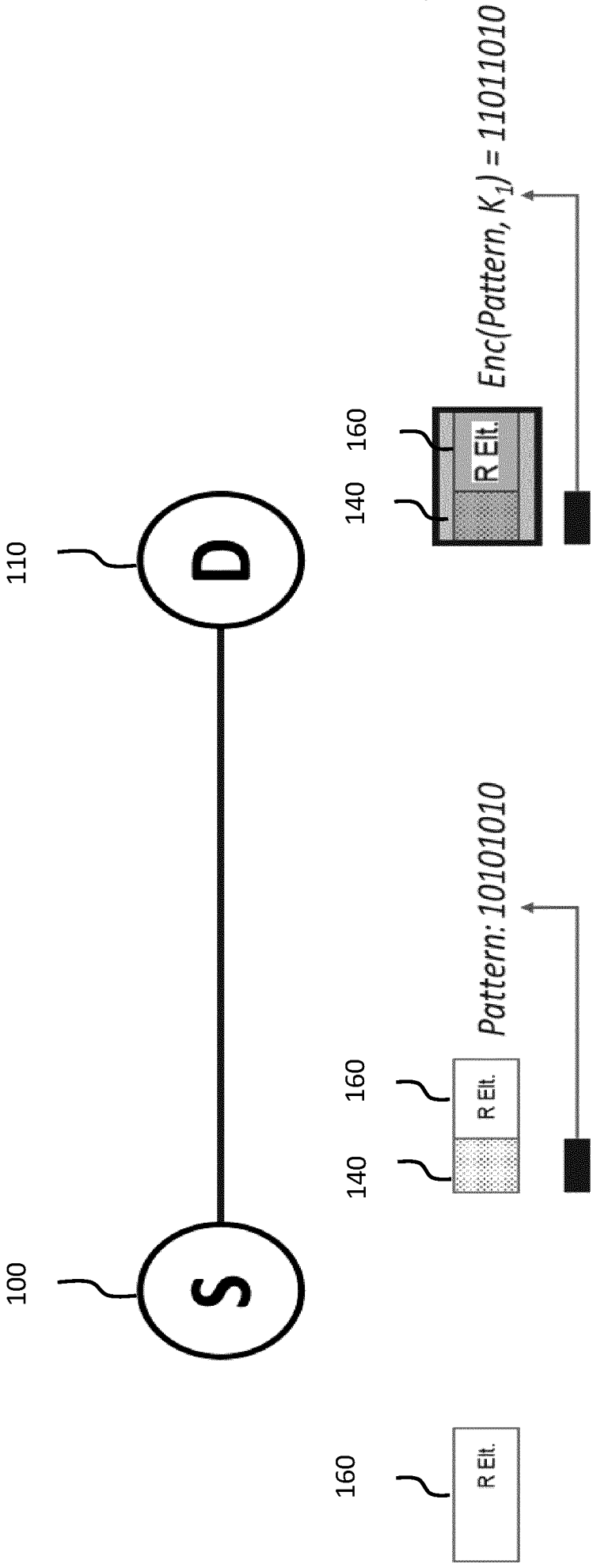
100
S
110
D
140
160
R Elt.
Pattern: 10101010
140
160
R Elt.
Enc(Pattern, K1) = 11011010
160
R Elt.

Fig. 3

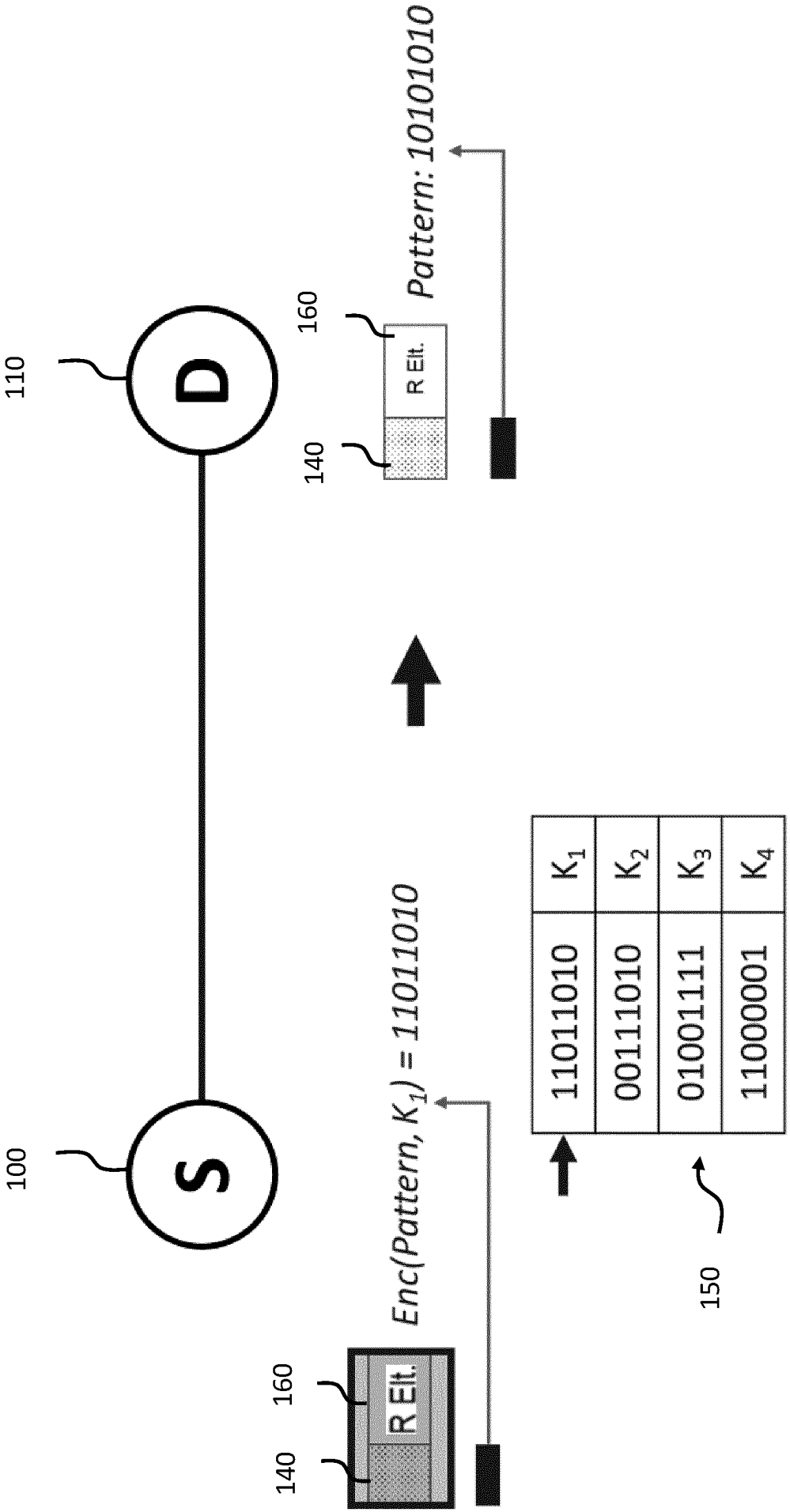
S
D
100
110
R Elt.
140
160
Enc(Pattern, K_1) = 11011010
Pattern: 10101010
K_1 11011010
K_2 00111010
K_3 01001111
K_4 11000001
150

Fig. 4

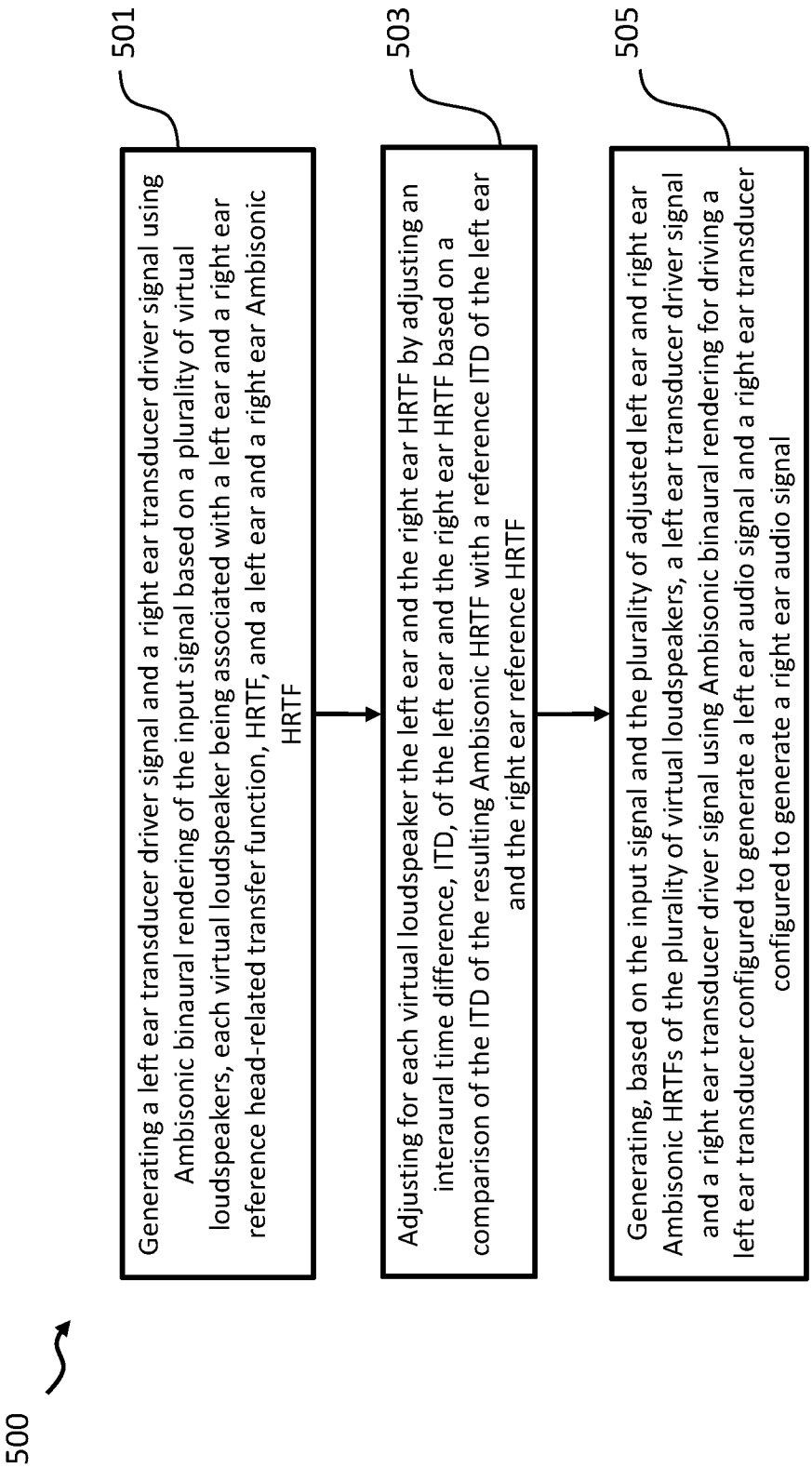
500
501
Generating a left ear transducer driver signal and a right ear transducer driver signal using Ambisonic binaural rendering of the input signal based on a plurality of virtual loudspeakers, each virtual loudspeaker being associated with a left ear and a right ear reference head-related transfer function, HRTF, and a left ear and a right ear Ambisonic HRTF
503
Adjusting for each virtual loudspeaker the left ear and the right ear HRTF by adjusting an interaural time difference, ITD, of the left ear and the right ear HRTF based on a comparison of the ITD of the resulting Ambisonic HRTF with a reference ITD of the left ear and the right ear reference HRTF
505
Generating, based on the input signal and the plurality of adjusted left ear and right ear Ambisonic HRTFs of the plurality of virtual loudspeakers, a left ear transducer driver signal and a right ear transducer driver signal using Ambisonic binaural rendering for driving a left ear transducer configured to generate a left ear audio signal and a right ear transducer configured to generate a right ear audio signal

Fig. 5

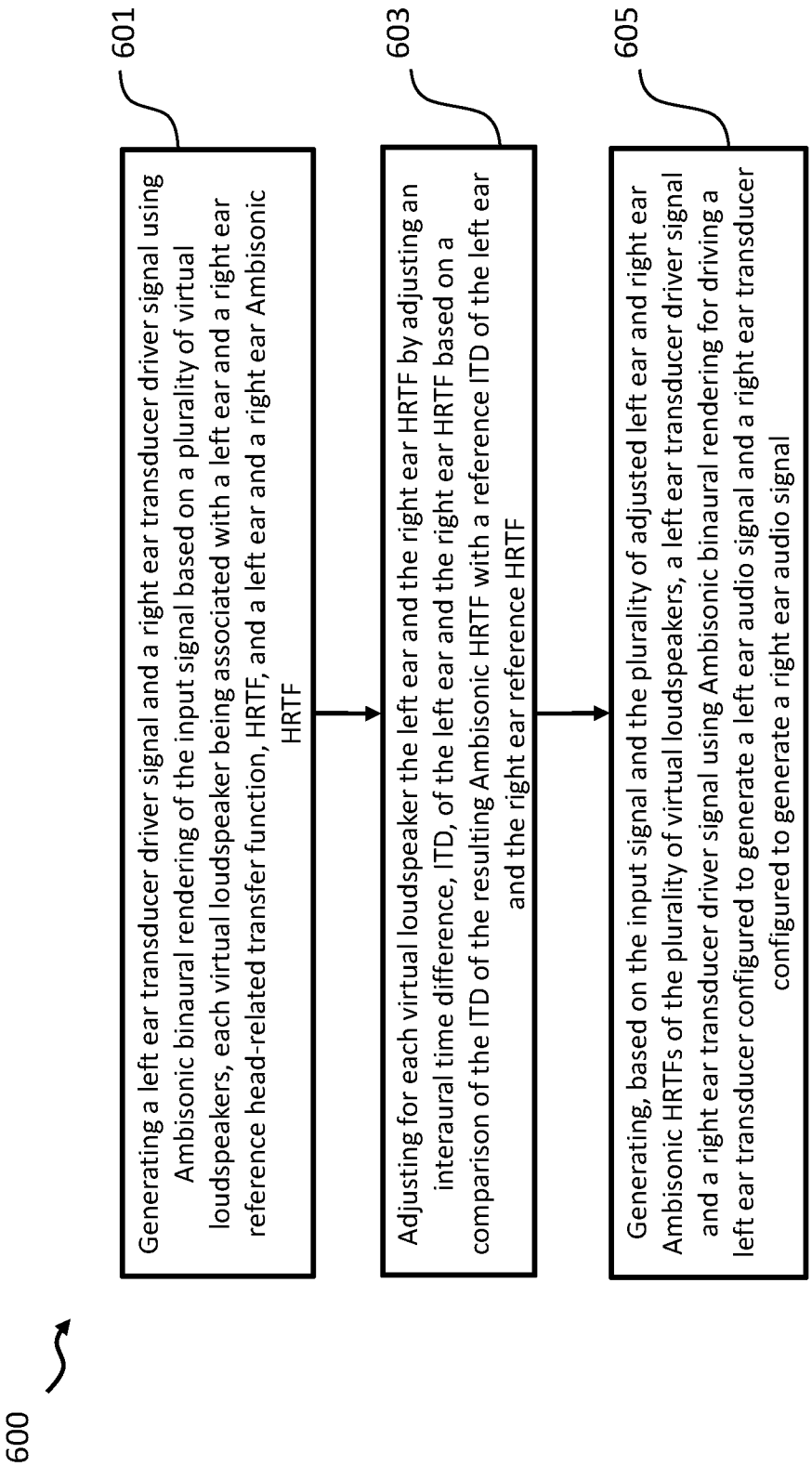
600
601
Generating a left ear transducer driver signal and a right ear transducer driver signal using Ambisonic binaural rendering of the input signal based on a plurality of virtual loudspeakers, each virtual loudspeaker being associated with a left ear and a right ear reference head-related transfer function, HRTF, and a left ear and a right ear Ambisonic HRTF
603
Adjusting for each virtual loudspeaker the left ear and the right ear HRTF by adjusting an interaural time difference, ITD, of the left ear and the right ear HRTF based on a comparison of the ITD of the resulting Ambisonic HRTF with a reference ITD of the left ear and the right ear reference HRTF
605
Generating, based on the input signal and the plurality of adjusted left ear and right ear Ambisonic HRTFs of the plurality of virtual loudspeakers, a left ear transducer driver signal and a right ear transducer driver signal using Ambisonic binaural rendering for driving a left ear transducer configured to generate a left ear audio signal and a right ear transducer configured to generate a right ear audio signal

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/074534

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD.

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	RENE MAYRHOFER ED - FRANK STAJANO ET AL: "The Candidate Key Protocol for Generating Secret Shared Keys from Similar Sensor Data Streams", 2 July 2008 (2008-07-02), SECURITY AND PRIVACY IN AD-HOC AND SENSOR NETWORKS; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 1 - 15, XP019095851, ISBN: 978-3-540-73274-7	1-16
Y	section 4; figure 3	1-16
Y	US 2017/155510 A1 (CLOOSTERMANS BOUKE [NL] ET AL) 1 June 2017 (2017-06-01) paragraph [0101]	1-16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2022	15/06/2022

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

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/074534

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 10 887 289 B2 (FUJITSU LTD [JP]) 5 January 2021 (2021-01-05) columns 14,16 _____	1-13,15, 16

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2021/074534

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017155510 A1	01-06-2017	CN 106464490 A	22-02-2017
		EP 3161993 A1	03-05-2017
		JP 2017519457 A	13-07-2017
		US 2017155510 A1	01-06-2017
		WO 2015197368 A1	30-12-2015
US 10887289 B2	05-01-2021	NONE	