(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 028 487 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Claims EN 7

(48) Corrigendum issued on:
31.03.2021 Bulletin 2021/13

(45) Date of publication and mention of the grant of the patent:
23.09.2020 Bulletin 2020/39

(21) Application number: **13890600.3**

(22) Date of filing: **01.08.2013**

(51) Int Cl.:
H04W 36/00 *(2009.01)* *H04W 74/08* *(2009.01)*
H04W 12/04 *(2021.01)* *H04L 9/08* *(2006.01)*

(86) International application number:
PCT/CN2013/080655

(87) International publication number:
WO 2015/013964 (05.02.2015 Gazette 2015/05)

(54) **METHODS, APPARATUSES AND COMPUTER PROGRAM PRODUCTS FOR FAST HANDOVER**

VERFAHREN, VORRICHTUNGEN UND COMPUTERPROGRAMMPRODUKTE FÜR SCHNELLES HANDOVER

PROCÉDÉS, APPAREILS ET PRODUITS-PROGRAMMES INFORMATIQUES DE TRANSFERT RAPIDE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
08.06.2016 Bulletin 2016/23

(73) Proprietor: **Nokia Technologies Oy**
02610 Espoo (FI)

(72) Inventors:
- **LIU, Yang**
  Beijing 100191 (CN)
- **ZHANG, Dajiang**
  Beijing 100102 (CN)
- **LI, Haitao**
  Beijing 100052 (CN)
- **ROSA, Claudio**
  DK-8920 Randers (DK)

(74) Representative: **Ruuskanen, Juha-Pekka et al**
Page White & Farrer
Bedford House
John Street
London WC1N 2BF (GB)

(56) References cited:
WO-A2-2006/102565 **CN-A- 101 335 985**
CN-A- 102 215 485

- **"3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 11)", 3GPP STANDARD; 3GPP TS 36.300, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. RAN WG2, no. V11.6.0, 7 July 2013 (2013-07-07), pages 1-209, XP050712084, [retrieved on 2013-07-07]**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 12)", 3GPP STANDARD; 3GPP TS 33.401, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. V12.8.1, 3 July 2013 (2013-07-03), pages 1-121, XP050712018, [retrieved on 2013-07-03]
- 3RD GENERATION PARTNERSHIP PROJECT.: 'Security architecture' 3GPP TS 33.401 V10.4.0 31 March 2013, XP055291292

Description

FIELD OF THE INVENTION

[0001] Embodiments of the present invention generally relate to wireless communication techniques including the 3GPP (the 3rd Generation Partnership Project) LTE technique. More particularly, embodiments of the present invention relate to methods, apparatuses, and computer program products for a fast handover.

BACKGROUND OF THE INVENTION

[0002] Various abbreviations that appear in the specification and/or in the drawing figures are defined as below:

BS	Base Station
CN	Core Network
C-RNTI	Cell Radio Network Temporary Identity
LTE	Long Term Evolution
NB	Node B
NCC	Next Hop Chaining Counter
NH	Next Hop Chain
eNB	evolved Node B
Identity	ID
HO	Handover
KDF	Key Derivation Function
PCI	Physical Cell Identifier
PRACH	Physical Random Access Channel
RRC	Radio Resource Control
RF	Radio Frequency
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
UE	User Equipment

[0003] The Rel-12 Study Item named as Small Cell Enhancement for higher layers in RAN2 has been discussed in 3GPP. In this Study Item, it is proposed to investigate solutions in regard to improving the mobility robustness, reducing signaling overhead towards the core network, and bettering inter-node UE context transfer procedure. In addition to these, small cell related mobility procedures will also be studied in this Study Item. In one of the mobility topics, a method called fast X2 HO is proposed.

[0004] The principle behind the fast X2 HO is that a target BS or eNB reserves a certain amount of resources for the fast X2 HO and indicates a predefined PRACH and associated C-RNTI to a source eNB. When a UE sends a measurement report to the source eNB and the source eNB ascertains there is a reserved channel for the fast X2 HO, it may indicate the predefined PRACH and associated C-RNTI to the UE via an RRC message, such as an RRCConnectionReconfiguration message. After that, the UE can set up an RRC connection with the target eNB directly using the predefined PRACH and the associated C-RNTI without a network HO preparation procedure. Therefore, the legacy HO signaling is omitted between the source eNB and the target eNB.

[0005] In the legacy X2 HO, the source eNB will derive the key KeNB* and send the pair (KeNB*, NCC) to the target eNB during the HO preparation. The target eNB will include the NCC into the HO command and send it to the UE, which is transparent to the source eNB. The UE will derive the same key KeNB*. In this manner, security communication can be established between the UE and the target eNB. More information regarding key derivations during HO can be found in section 7.2.8.4 of the 3GPP TS 33.401 V12.5.0 (2012-09).

[0006] However, in the fast X2 HO, the target eNB and the UE will not have the correct cryptography keys for security communication since the X2 interface signaling during the HO preparation is omitted. Due to this, the fast X2 HO is not applicable at least from the perspective of security communications.

"3rd Generation Partnership Project; Technical; Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 12)", 3GPP TS 33.401, V 12.8.1 specifies the security architecture, i.e. the security features and the security mechanisms for the Evolved Packet System and the Evolved Packet Core, and the security procedures performed within the evolved Packet System including the Evolved Packet Core and the Evolved UTRAN.

[0007] A general description of the handover procedure in LTE is disclosed by the 3GPP Technical Specification 36.300, V.11.6.0.

[0008] CN 101355985 A discloses a method for fast handover, which includes establishing a security alliance between a mobile node and a new access router of a target network before the fast handover; and during the fast handover of the mobile node, using the security association to ensure that the mobile node securely accesses the new access router.

SUMMARY OF THE INVENTION

[0009] Therefore, there is a need in the art to provide an efficient mechanism for establishing security communication between the UE and the target base station after the fast handover.

[0010] These and other problems are generally solved or circumvented, and technical advantages are generally achieved, by embodiments of the present invention, which include methods, apparatuses, and computer program products for a fast handover. The invention is defined by the present claims.

[0011] According to one aspect of the present invention, a method is provided, which comprises generating, at a source base station serving a user equipment, a first message and a second message including security information for security communication between a target base station and the user equipment after a fast handover. The method also comprises transmitting simultaneously, from the source base station, the first and second messages respectively to the target base station and the

user equipment.

[0012] In one embodiment, the method further comprises receiving from the target base station cryptography algorithm information including an identifier of at least one cryptography algorithm and generating the first and second messages based on the cryptography algorithm information.

[0013] In another embodiment, the first message includes at least an identifier of a cryptography algorithm selected from the at least one cryptography algorithm based on security capability of the user equipment, and a derived key.

[0014] In an additional embodiment, the second message includes at least physical random access channel information and a cell radio network temporary identity predefined to be used by the user equipment for the fast handover, and the identifier of the selected cryptography algorithm.

[0015] In a further embodiment, the derived key is K_{eNB^*} derived through a key derivation function using, as inputs, a key K_{eNB}, the predefined physical random access channel information and the cell radio network temporary identity.

[0016] According to another aspect of the present invention, a method is provided, which comprises signaling cryptography algorithm information to a source base station serving a user equipment for security communication between a target base station and the user equipment after a fast handover, wherein the cryptography algorithm information includes an identifier of at least one cryptography algorithm. The method also comprises receiving, from the source base station, a message including a derived key and an identifier of a cryptography algorithm selected from the at least one cryptography algorithm for the security communication.

[0017] In one embodiment, the derived key is K_{eNB^*} derived through a key derivation function using, as inputs, a key K_{eNB}, physical random access channel information and a cell radio network temporary identity predefined to be used by the user equipment for the fast handover.

[0018] In another embodiment, the method further comprises establishing security communication with the user equipment based on the derived key and the identifier of the cryptography algorithm.

[0019] According to an additional aspect of the present invention, a method is provided, which comprises receiving, from a source base station serving a user equipment, a message including security information for security communication between a target base station and the user equipment after a fast handover, wherein the security information includes at least an identifier of a cryptography algorithm. The method also comprises deriving, at the user equipment, a key for security communication with the target base station based on the identifier of the cryptography algorithm. The method further comprises using the derived key for the security communication with the target base station after the fast handover.

[0020] In one embodiment, the method further comprises receiving, from the source base station, physical random access channel information and a cell radio network temporary identity predefined by the target base station to be used by the user equipment for the fast handover.

[0021] In another embodiment, the derived key is K_{eNB^*} derived through a key derivation function using, as inputs, a key K_{eNB}, the physical random access channel information and the cell radio network temporary identity.

[0022] According to another aspect of the present invention, an apparatus is provided, which comprises at least one processor and at least one memory including computer program code. The memory and the computer program code are configured to, working with the processor, cause the apparatus at least to generate, at a source base station serving a user equipment, a first message and a second message including security information for security communication between a target base station and the user equipment after a fast handover. The memory and the computer program code are also configured to, working with the processor, cause the apparatus at least to transmit simultaneously, from the source base station, the first and second messages respectively to the target base station and the user equipment.

[0023] According to another aspect of the present invention, an apparatus is provided, which comprises at least one processor and at least one memory including computer program code. The memory and the computer program code are configured to, working with the processor, cause the apparatus at least to signal cryptography algorithm information to a source base station serving a user equipment for security communication between a target base station and the user equipment after a fast handover, wherein the cryptography algorithm information includes an identifier of at least one cryptography algorithm. The memory and the computer program code are also configured to, working with the processor, cause the apparatus at least to receive, from the source base station, a message including a derived key and an identifier of a cryptography algorithm selected from the at least one cryptography algorithm for the security communication.

[0024] According to another aspect of the present invention, an apparatus is provided, which comprises at least one processor and at least one memory including computer program code. The memory and the computer program code are configured to, working with the processor, cause the apparatus at least to receive, from a source base station serving a user equipment, a message including security information for security communication between a target base station and the user equipment after a fast handover, wherein the security information includes at least an identifier of a cryptography algorithm. The memory and the computer program code are also configured to, working with the processor, cause the apparatus at least to derive, at the user equipment, a key for security communication with the target

base station based on the identifier of the cryptography algorithm. The memory and the computer program code are also configured to, working with the processor, cause the apparatus at least to use the derived key for the security communication with the target base station after the fast handover.

[0025] According to another aspect of the present invention, an apparatus is provided, which comprises means for generating, at a source base station serving a user equipment, a first message and a second message including security information for security communication between a target base station and the user equipment after a fast handover. The apparatus also comprises means for transmitting simultaneously, from the source base station, the first and second messages respectively to the target base station and the user equipment.

[0026] According to another aspect of the present invention, an apparatus is provided, which comprises means for signaling cryptography algorithm information to a source base station serving a user equipment for security communication between a target base station and the user equipment after a fast handover, wherein the cryptography algorithm information includes an identifier of at least one cryptography algorithm. The apparatus also comprises means for receiving, from the source base station, a message including a derived key and an identifier of a cryptography algorithm selected from the at least one cryptography algorithm for the security communication.

[0027] According to another aspect of the present invention, an apparatus is provided, which comprises means for receiving, from a source base station serving a user equipment, a message including security information for security communication between a target base station and the user equipment after a fast handover, wherein the security information includes at least an identifier of a cryptography algorithm. The apparatus also comprises means for deriving, at the user equipment, a key for security communication with the target base station based on the identifier of the cryptography algorithm. The apparatus further comprises means for using the derived key for the security communication with the target base station after the fast handover.

[0028] According to another aspect of the present invention, a computer program product is provided, which, comprises a non-transitory computer readable medium having code portions stored thereon, the program code portions being a computer readable medium and configured when said computer program product is run on a computer or network device, to generate, at a source base station serving a user equipment, a first message and a second message including security information for security communication between a target base station and the user equipment after a fast handover. The program code portions are configured when said computer program product is run on a computer or network device to transmit simultaneously, from the source base station, the first and second messages respectively to the target base station and the user equipment.

[0029] According to another aspect of the present invention, a computer program product is provided, which, comprises a non-transitory computer readable medium having code portions stored thereon, the program code portions being a computer readable medium and configured when said computer program product is run on a computer or network device, to signal cryptography algorithm information to a source base station serving a user equipment for security communication between a target base station and the user equipment after a fast handover, wherein the cryptography algorithm information includes an identifier of at least one cryptography algorithm. The program code portions are configured when said computer program product is run on a computer or network device to receive, from the source base station, a message including a derived key and an identifier of a cryptography algorithm selected from the at least one cryptography algorithm for the security communication.

[0030] According to another aspect of the present invention, a computer program product is provided, which, comprises a non-transitory computer readable medium having code portions stored thereon, the program code portions being a computer readable medium and configured when said computer program product is run on a computer or network device, to receive, from a source base station serving a user equipment, a message including security information for security communication between a target base station and the user equipment after a fast handover, wherein the security information includes at least an identifier of a cryptography algorithm. The program code portions are configured when said computer program product is run on a computer or network device to derive, at the user equipment, a key for security communication with the target base station based on the identifier of the cryptography algorithm. The program code portions are configured when said computer program product is run on a computer or network device to use the derived key for the security communication with the target base station after the fast handover.

[0031] According to certain embodiments of the present invention, a fast X2 handover procedure is complemented and becomes more feasible with proposed security handlings, making it possible to decrease the service interruption during the fast X2 HO for users and hence improve the user experiences. During a key derivation processing according to the embodiments of the present invention, some parameter, such as NCC, does not need to be sent to the UE but a temporary security key can be generated according to a new KDF. Thereby, a potential security risk due to the UE autonomous access behavior can be avoided.

[0032] Other features and advantages of the embodiments of the present invention will also be understood from the following description of specific embodiments when read in conjunction with the accompanying drawings, which illustrate, by way of example, the principles

of embodiments of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] The embodiments of the invention that are presented in the sense of examples and their advantages are explained in greater detail below with reference to the accompanying drawings, in which:

Fig. 1 is a schematic communication architecture under which various embodiments of the present invention may be practiced;
Fig. 2 is a flow chart schematically illustrating a method for a fast handover from a source BS perspective according to an embodiment of the present invention;
Fig. 3 is a flow chart schematically illustrating a method for a fast handover from a target BS perspective according to another embodiment of the present invention;
Fig. 4 is a flow chart schematically illustrating a method for a fast handover from a UE perspective according to another embodiment of the present invention;
Fig. 5 is a schematic signaling diagram illustrating signaling interactions between a UE, a source BS and a target BS according to an embodiment of the present invention;
Fig. 6 illustrates a schematic block diagram of a UE that is suitable for use in practicing the exemplary embodiments of the present invention; and
Fig. 7 illustrates a schematic block diagram of a BS that is suitable for use in practicing the exemplary embodiments of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0034] Embodiments of the present invention propose an efficient mechanism of performing a fast HO from a source BS to a target BS in wireless communication systems (e.g., LTE system) such that service continuity for a served UE could be achieved. During such a fast HO, the source BS plays an intermediary role in conveying the security information to both the UE and the target BS such that security communication can be established between the UE and the target BS without further signaling via the X2 interface, thereby implementing the faster HO relative to the legacy HO.

[0035] Before detailed description of various embodiments of the present invention, it should be noted that the acronyms BS, NB, and eNB may refer generally to equipments providing wireless network interfaces in a cellular wireless system such as the LTE system, and thus will be used interchangeably throughout the specification and claims.

[0036] Embodiments of the present invention will be described in detail as below.

[0037] Fig. 1 is a schematic communication architecture under which various embodiments of the present invention may be practiced. As illustrated in Fig. 1, a UE is connected with a source BS via a wireless link and accepts the wireless service provided by the source BS. As the UE moves in a direction indicated by an arrow, it becomes increasingly closer to a target BS and far away from the source BS. During the movement, the UE may keep transmitting to the source BS measurement reports based on which the source BS may decide whether to direct the UE to make a HO to the target BS. It can be understood by those skilled in the art that there would be a certain number of potential target BSs around the source BS and the source BS may choose a proper one of them via an X2 interface as the final target BS based on several criteria, such as signal strength or quality (e.g., RSRP or RSRQ value) or sequence of responding to a HO request as initiated by the source BS. For a simplicity purpose, only one BS which is assumed to be the target BS is shown.

[0038] As mentioned before, during the existing fast X2 HO, the security communication cannot be implemented since the X2 signaling is omitted during the HO preparation and thus the target BS and the UE will not have the correct cryptography keys. To this end, the certain aspects of the present invention and embodiments thereof propose methods, apparatuses and computer program products to achieve security communication between the UE and the target BS, as will be discussed in detail hereinafter in connection with Figs. 2-7.

[0039] Fig. 2 is a flow chart schematically illustrating a method 200 for a fast HO from a source BS perspective according to an embodiment of the present invention. As illustrated in Fig. 2, at step S201, the method 200 generates, at a source BS serving a UE, a first message and a second message including security information for security communication between a target BS and the UE after a fast HO. In an embodiment, the first message includes at least an ID of a cryptography algorithm selected from the at least one cryptography algorithm based on security capability of the UE, and a derived key. In another embodiment, the second message includes at least PRACH information and a C-RNTI predefined to be used by the UE for the fast HO, and the ID of the selected cryptography algorithm. In one embodiment, the second message may additionally include the NCC and take a form of a dedicated RRC message, such as the existing RRCConnectionReconfiguration message.

[0040] In these embodiments, the derived key is K_{eNB^*} derived through a KDF using, as inputs, a key K_{eNB}, the predefined PRACH information and the C-RNTI. In the embodiments above, the first message including the derived key K_{eNB^*} and the ID of the selected cryptography algorithm may be sent to the target BS in a form of a newly standardized X2 message similar to the HO request message in the legacy HO procedure.

[0041] Although not illustrated in Fig. 2, in one embodiment, prior to generating the first and second messages, the method 200 receives from the target BS cryptography algorithm information including the ID of the at least one

cryptography algorithm and, after that, generates the first and second messages based on the cryptography algorithm information. In addition to the ID information, when there are a number of cryptography algorithms, the source BS may also be informed by the target BS of various priorities configured for each cryptography algorithm through a newly standardized X2 message similar to the HO response message in the legacy HO procedure.

[0042] As a part of the existing fast X2 HO, the source BS may also negotiate with the target BS regarding the PRACH and the associated C-RNTI predefined to be used by the UE when the fast X2 HO to the target BS is triggered.

[0043] Subsequent to the generation of the first and second messages, the method 200 transmits simultaneously, at step S202, from the source BS, the first and second messages respectively to the target BS and the UE. Simultaneous transmission of the first and second messages enables the UE and the target BS to implement the subsequent HO procedure and security operations in a timely and synchronous manner. For example, upon receipt of the second message, the UE may generate a same key as the derived key and have access to the target BS using the allocated PRACH and C-RNTI. On the other hand, upon receipt of the first message, the target BS may know the specific PRACH and C-RNTI which would be used by the
UE for the HO and get well prepared for HO by the UE.

[0044] From the above descriptions made with reference to Fig. 2, it is apparent to those skilled in the art that the source BS configured by the embodiments of the present invention transmits the security information to the target BS and the UE such that target BS and the UE are able to proceed with the security communication even if the HO is a fast X2 HO.

[0045] Fig. 3 is a flow chart schematically illustrating a method 300 for a fast HO from a target BS perspective according to another embodiment of the present invention. As illustrated in Fig. 3, at step S301, the method 300 signals cryptography algorithm information to a source BS serving a UE for security communication between a target BS and the UE after a fast HO, wherein the cryptography algorithm information includes an identifier of at least one cryptography algorithm. In one embodiment, the signaling of the cryptography algorithm information to the source BS can be implemented using a newly standardized X2 message similar to the HO response message in the legacy handover procedure, as previously discussed with reference to the method 200. The cryptography algorithm information herein may further include corresponding priorities for the corresponding cryptography algorithms.

[0046] At step S302, the method 300 receives, from the source BS, a message including a derived key and an identifier of a cryptography algorithm selected from the at least one cryptography algorithm for the security communication. As noted before, the derived key is K_{eNB}^* derived through a KDF using, as inputs, a key K_{eNB}, PRACH information and a C-RNTI predefined to be used by the UE for the fast HO. The PRACH information and the C-RNTI can be predefined by the target BS and sent to the source BS when the fast X2 HO is triggered.

[0047] Although not shown in Fig. 3, the method 300 further establishes security information with the UE based on the derived key and the identifier of the cryptography algorithm. In an embodiment, the derived key is K_{eNB}^* which is the same as the one derived at the UE.

[0048] Fig. 4 is a flow chart schematically illustrating a method 400 for a fast HO from a UE perspective according to another embodiment of the present invention. As illustrated in Fig. 4, at step S401, the method 400 receives, from a source BS serving a UE, a message including security information for security communication between a target BS and the UE after a fast handover, wherein the security information includes at least an identifier of a cryptography algorithm. In order for successful access to the target BS, the UE also receives from the source BS PRACH information and C-RNTI predefined by the target BS for the fast X2 HO. In this manner, a likelihood of the UE's successful fast HO to the target BS is markedly improved. In an embodiment, the security information may include the NCC.

[0049] Upon receiving the message (i.e., the second message in the method 200) from the source BS, the method 400, at step S402, derives a key for security communication with the target BS based on the ID of the cryptography algorithm. As mentioned previously, since there may be a plurality of cryptography algorithms applied by the target BS, the source BS will select a proper cryptography algorithm based on the UE's capability. In this way, the UE has the possibility and capability of deriving the same key as the one transmitted from the source BS to the target BS based on the algorithm ID. In an embodiment, the derived key is K_{eNB*} derived through a KDF using, as inputs, a key K_{eNB}, the PRACH information and the C-RNTI. As an alternative, the derivation of the K_{ENB*} could also be based on legacy parameters as known to those skilled in the art.

[0050] After that, the method proceeds to step S403 at which the method 400 uses the derived key for the security communication with the target base station after the fast HO.

[0051] Fig. 5 is a schematic signaling diagram 500 illustrating signaling interactions between a UE, a source BS and a target BS according to an embodiment of the present invention. As illustrated in Fig. 5, at S501, the target BS reserves certain resources for a fast X2 HO and indicates predefined PRACH information and associated C-RNTI to the source BS. In an example, the supported algorithm ID(s) and related configured priority (priorities) could also be sent to the source BS. At S502, the UE, which may be handed over to the target BS later on, sends one or more measurement reports to the source eNB. At S503, the source BS decides, based on the measurement report, to initiate a fast HO and consequently generate a key K_{eNB*}.

[0052] At S504, the source BS sends to the target BS a security key indication (i.e., a specific form of the first message as discussed before) which indicates the generated K_{eNB^*} and the algorithm ID of the cryptography algorithm selected based on the security capability of the UE and supported by the target BS, together with the PRACH or C-RNTI predefined by the target BS and used by the UE, to assist the target BS in mapping the key K_{eNB^*} with the UE.

[0053] At S505, simultaneously, the source BS sends to the UE another security key indication (i.e., a specific form of the second message as discussed before) via e.g., a dedicated RRC message (e.g., an RRCConnectionReconfiguration message) including pre-defined PRACH information, the associated C-RNTI, an NCC (optional) and the algorithm ID to the UE. At S506, the UE would check if there is algorithm ID in the received RRC message (e.g., the RRCConnectionReconfiguration message). If this is the case, the UE would derive the K_{eNB^*} according to a new KDF using, as inputs, the K_{eNB}, the predefined PRACH information (e.g., preamble index), and the associated C-RNIT. In an example, instead of using the new KDF, the K_{eNB^*} can be derived from the K_{eNB} or NH as the legacy X2 HO, together with the PCI, downlink frequency of the target BS. Since the NH is used to derive the key, NCC is needed according to 3GPP TS 33.401.

[0054] At S507, upon receiving the security key indication, the target BS may get ready for accepting the UE's access in the indicated PRACH or C-RNTI. Then, at S508, the UE may utilize the PRACH and C-RNTI to access the target BS and conduct security operations based on the K_{eNB^*} and the algorithm ID, and the target BS may optionally trigger a key refresh procedure following this fast X2 handover.

[0055] Fig. 6 illustrates a simplified block diagram of a UE 601 that is suitable for use in practicing the exemplary embodiments of the present invention. In Fig. 6, the UE 601 includes a data processor (DP) 602, a memory (MEM) 603 coupled to the DP 602, and a suitable RF transmitter TX and receiver RX 604 (which need not to be implemented in a same component) coupled to the DP 602. The MEM 603 stores a program (PROG) 605. The TX/RX 604 is for bidirectional wireless communications with the BS (source or target BS). Note that the TX/RX 604 has at least one antenna to facilitate communication; multiple antennas may be employed for multiple-input multiple-output MIMO communications in which case the UE 601 may have multiple TXs and/or RXs.

[0056] The PROG 605 is assumed to include program instructions that, when executed by the associated DP 602, enable the UE 601 to operate in accordance with the exemplary embodiments of the present invention, as discussed herein with the method 400.

[0057] In general, the various embodiments of the UE 601 can include, but are not limited to, cellular phones, personal digital assistants (PDAs) having wireless communication capabilities, portable computers having wireless communication capabilities, image capture devices such as digital cameras having wireless communication capabilities, gaming devices having wireless communication capabilities, music storage and playback appliances having wireless communication capabilities, Internet appliances permitting wireless Internet access and browsing, as well as portable units or terminals that incorporate combinations of such functions.

[0058] The MEM 603 may be of any type suitable to the local technical environment and may be implemented using any suitable data storage technology, such as semiconductor based memory devices, magnetic memory devices and systems, optical memory devices and systems, fixed memory and removable memory, as non-limiting examples. While only one MEM is shown in the UE 601, there may be several physically distinct memory units in the UE 601. The DP 602 may be of any type suitable to the local technical environment, and may include one or more of general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multicore processor architecture, as non-limiting examples. The UE 601 may have multiple processors, such as for example an application specific integrated circuit chip that is slaved in time to a clock which synchronizes the main processor.

[0059] Fig. 7 illustrates a simplified block diagram of a BS 701 (source or target BS in the HO procedure) that is suitable for use in practicing the exemplary embodiments of the present invention. In Fig.7, the BS 701 includes a data processor (DP) 702, a memory (MEM) 703 coupled to the DP 702, and a suitable RF transmitter TX and receiver RX 704 coupled to the DP 702. The MEM 703 stores a program (PROG) 705. The TX/RX 704 is for bidirectional wireless communications with the UE 601 as illustrated in Fig. 6. Note that the TX/RX 704 has at least one antenna to facilitate communication, though in practice a BS will typically have several. The BS 701 may be coupled via a data path to one or more external networks or systems, such as the Internet, for example.

[0060] The PROG 705 is assumed to include program instructions that, when executed by the associated DP 702, enable the BS 701 to operate in accordance with the exemplary embodiments of the present invention, as discussed herein with the methods 200 and 300.

[0061] The MEM 703 may be of any type suitable to the local technical environment and may be implemented using any suitable data storage technology, such as semiconductor based memory devices, magnetic memory devices and systems, optical memory devices and systems, fixed memory and removable memory, as non-limiting examples. While only one MEM is shown in the BS 701, there may be several physically distinct memory units in the BS 701. The DP 702 may be of any type suitable to the local technical environment, and may include one or more of general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multicore processor architecture, as non-limiting examples. The BS 701

may have multiple processors, such as for example an application specific integrated circuit chip that is slaved in time to a clock which synchronizes the main processor.

[0062] The embodiments of the present invention may be implemented by computer software executable by one or more of the DPs 602, 702 of the UE 601 and the BS 701, or by hardware, or by a combination of software and hardware.

[0063] Exemplary embodiments of the present invention have been described above with reference to block diagrams and flowchart illustrations of methods, apparatuses (i.e., systems). It will be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by various means including computer program instructions. These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks.

[0064] The foregoing computer program instructions can be, for example, sub-routines and/or functions. A computer program product in one embodiment of the invention comprises at least one computer readable storage medium, on which the foregoing computer program instructions are stored. The computer readable storage medium can be, for example, an optical compact disk or an electronic memory device like a RAM (random access memory) or a ROM (read only memory).

[0065] Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these embodiments of the invention pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the embodiments of the invention are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. A method performed by a base station (701) serving a user equipment (601), said method comprising:

   receiving (S501) information from a target base station, said information indicating physical random access channel information and a cell radio network temporary identity predefined to be used by said user equipment,
   the method being **characterized by**:

   deciding (S503) to initiate a fast handover of said user equipment to said target base station using the physical random access channel information and the cell radio network temporary identity;
   generating (S201) a first message and a second message, each including security information for security communication between the target base station (701) and the user equipment (601) after the fast handover, wherein the second message additionally includes said physical random access channel information and said cell radio network temporary identity for use by the user equipment to access the target base station during the fast handover; and
   transmitting (S202) simultaneously, from the source base station (701), the first message to the target base station (701) and the second message to the user equipment (601).

2. The method as recited in Claim 1, wherein the information received (S501) from the target base station additionally includes cryptography algorithm information including an identifier of at least one cryptography algorithm; and
   wherein the generating of the first and second messages is based on the cryptography algorithm information.

3. The method as recited in Claim 2, wherein the first message includes at least an identifier of a cryptography algorithm and a derived key, wherein the identifier of the cryptography algorithm is selected from the at least one received cryptography algorithm identifier based on security capability of the user equipment (601).

4. The method as recited in Claim 3, wherein the second message includes at least the physical random access channel information and the cell radio network temporary identity predefined to be used by the user equipment (601) for the fast handover, and the identifier of the selected cryptography algorithm.

5. The method as recited in Claim 3 or 4, wherein the derived key, K_{eNB^*}, is derived through a key derivation function using, as inputs, a key, K_{eNB}, the predefined physical random access channel information and the cell radio network temporary identity.

6. A method performed by a user equipment, the method comprising:

   receiving (S401), from a source base station (701) serving the user equipment (601), a message including physical random access channel

information and a cell radio network temporary identity predefined by a target base station to be used by the user equipment to access the target base station during a fast handover, the message additionally including security information for security communication between the target base station (701) and the user equipment (601) after the fast handover, wherein the security information includes at least an identifier of a cryptography algorithm,
the method being **characterized in** by:

deriving (S402) a key for security communication with the target base station (701) based on the physical random access channel information, the cell radio network temporary identity and the identifier of the cryptography algorithm; and
using (S403) the derived key for the security communication with the target base station (701) after the fast handover.

7. A base station (701), comprising:

means for receiving (S501) information from a target base station, said information indicating physical random access channel information and a cell radio network temporary identity predefined to be used by a user equipment;
the base station being **characterized by** comprising:

means for deciding (S503) to initiate a fast handover of the user equipment to the target base station using the physical random access channel information and the cell radio network temporary identity;
means for generating (S201), a first message and a second message, each including security information for security communication between the target base station (701) and the user equipment (601) after the fast handover, wherein the second message additionally includes the physical random access channel information and the cell radio network temporary identity for use by the user equipment to access the target base station during the fast handover; and
means for transmitting (S202) simultaneously the first message to the target base station (701) and the second message to the user equipment (601).

8. The base station (701) as recited in Claim 7, wherein the information from the target base station (701) additionally includes cryptography algorithm information including an identifier of at least one cryptography algorithm; and
wherein the means for generating the first and second messages is based on the cryptography algorithm information.

9. The base station (701) as recited in Claim 8, wherein the first message includes at least an identifier of a cryptography algorithm and a derived key, wherein the base station further comprises means for selecting the identifier from the at least one received cryptography algorithm identifier based on security capability of the user equipment (601).

10. The base station (701) as recited in Claim 9, wherein the second message includes at least the physical random access channel information and the cell radio network temporary identity predefined to be used by the user equipment (601) for the fast handover, and the identifier of the selected cryptography algorithm.

11. The base station (701) as recited in Claim 9 or 10, wherein the base station further comprises means for deriving the derived key, K_{eNB^*}, through a key derivation function using, as inputs, a key, K_{eNB}, the predefined physical random access channel information and the cell radio network temporary identity.

12. A user equipment (601), comprising:

means for receiving (S401), from a source base station (701) serving the user equipment (601), a message including physical random access channel information and a cell radio network temporary identity predefined by a target base station to be used by the user equipment to access the target base station during a fast handover, the message additionally including security information for security communication between the target base station (701) and the user equipment (601) after the fast handover, wherein the security information includes at least an identifier of a cryptography algorithm,
the user equipment being **characterized by** comprising:

means for deriving (S402) a key for security communication with the target base station (701) based on the physical random access channel information, the cell radio network temporary identity, and the identifier of the cryptography algorithm; and
means for using (S403) the derived key for the security communication with the target base station (701) after the fast handover.

13. The user equipment (601) as recited in Claim 12, wherein the means for deriving the key further comprise:

means for deriving the key, K_{eNB}*, through a key derivation function using, as inputs, a key, K_{eNB}, the physical random access channel information and the cell radio network temporary identity predefined by the target base station (701) to be used by the user equipment (601) for the fast handover.

14. A computer program comprising instructions which, when executed by a processor in a user equipment cause the user equipment to perform the method of claim 7.

15. A computer program comprising instructions which, when executed by a processor in a base station, cause the base station to perform a method according to at least one of claims 1-6.

Patentansprüche

1. Verfahren, das durch eine Basisstation (701) durchgeführt wird, die eine Benutzerausrüstung (601) bedient, wobei das Verfahren umfasst:

Empfangen (S501) von Informationen aus einer Zielbasisstation, wobei die Informationen Informationen über einen physischen Direktzugriffskanal und eine temporäre Zellenfunknetzidentität angeben, die zur Verwendung durch die Benutzerausrüstung vordefiniert sind,
wobei das Verfahren **gekennzeichnet ist durch**:

Entscheiden (S503), ein schnelles Handover der Benutzerausrüstung an die Zielbasisstation unter Verwendung der Informationen des physischen Direktzugriffskanals und der temporären Zellenfunknetzidentität einzuleiten;
Erzeugen (S201) einer ersten Nachricht und einer zweiten Nachricht, die jeweils Sicherheitsinformationen für die Sicherheitskommunikation zwischen der Zielbasisstation (701) und der Benutzerausrüstung (601) nach dem schnellen Handover enthalten, wobei die zweite Nachricht zusätzlich die Informationen des physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität zur Verwendung **durch** die Benutzerausrüstung zum Zugriff auf die Zielbasisstation während des schnellen Handovers enthält; und
gleichzeitiges Übertragen (S202) der ersten Nachricht aus der Quellenbasisstation (701) an die Zielbasisstation (701) und der zweiten Nachricht an die Benutzerausrüstung (601).

2. Verfahren nach Anspruch 1, wobei die aus der Zielbasisstation empfangenen Informationen (S501) zusätzlich Kryptografiealgorithmusinformationen einschließlich einer Kennung mindestens eines Kryptografiealgorithmus enthalten; und
wobei das Erzeugen der ersten und zweiten Nachricht auf den Kryptografiealgorithmusinformationen basiert.

3. Verfahren nach Anspruch 2, wobei die erste Nachricht mindestens eine Kennung eines Kryptografiealgorithmus und einen abgeleiteten Schlüssel enthält, wobei die Kennung des Kryptografiealgorithmus aus der mindestens einen empfangenen Kryptografiealgorithmuskennung basierend auf der Sicherheitskapazität der Benutzerausrüstung (601) ausgewählt wird.

4. Verfahren nach Anspruch 3, wobei die zweite Nachricht mindestens die Informationen des physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität, die zur Verwendung durch die Benutzerausrüstung (601) für das schnelle Handover vordefiniert sind, sowie die Kennung des ausgewählten Kryptografiealgorithmus enthält.

5. Verfahren nach Anspruch 3 oder 4, wobei der abgeleitete Schlüssel, K_{eNB*}, durch eine Schlüsselableitungsfunktion abgeleitet wird, die als Eingaben einen Schlüssel, K_{eNB}, die Informationen des vordefinierten physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität verwendet.

6. Verfahren, das durch eine Benutzerausrüstung durchgeführt wird, wobei das Verfahren umfasst:

Empfangen (S401) einer Nachricht aus einer Quellenbasisstation (701), die die Benutzerausrüstung (601) bedient, wobei die Nachricht Informationen über einen physischen Direktzugriffskanal und eine temporäre Zellenfunknetzidentität enthält, die durch eine Zielbasisstation zur Verwendung durch die Benutzerausrüstung vordefiniert sind, um während eines schnellen Handovers auf die Zielbasisstation zuzugreifen, wobei die Nachricht zusätzlich Sicherheitsinformationen für die Sicherheitskommunikation zwischen der Zielbasisstation (701) und der Benutzerausrüstung (601) nach dem schnellen Handover enthält, wobei die Sicherheitsinformationen mindestens eine Kennung eines Kryptografiealgorithmus enthalten,
wobei das Verfahren **gekennzeichnet ist durch**:

Ableiten (S402) eines Schlüssels für die Sicherheitskommunikation mit der Zielbasisstation (701) basierend auf den Informatio-

nen des physischen Direktzugriffskanals, der temporären Zellenfunknetzidentität und der Kennung des Kryptografiealgorithmus; und

Verwenden (S403) des abgeleiteten Schlüssels für die Sicherheitskommunikation mit der Zielbasisstation (701) nach dem schnellen Handover.

7. Basisstation (701), umfassend:

Mittel zum Empfangen (S501) von Informationen aus einer Zielbasisstation, wobei die Informationen Informationen über einen physischen Direktzugriffskanal und eine temporäre Zellenfunknetzidentität angeben, die zur Verwendung durch eine Benutzerausrüstung vordefiniert sind;

wobei die Basisstation **dadurch gekennzeichnet ist, dass** sie umfasst:

Mittel zum Entscheiden (S503), ein schnelles Handover der Benutzerausrüstung an die Zielbasisstation unter Verwendung der Informationen des physischen Direktzugriffskanals und der temporären Zellenfunknetzidentität einzuleiten;

Mittel zum Erzeugen (S201) einer ersten Nachricht und einer zweiten Nachricht, die jeweils Sicherheitsinformationen für die Sicherheitskommunikation zwischen der Zielbasisstation (701) und der Benutzerausrüstung (601) nach dem schnellen Handover enthalten, wobei die zweite Nachricht zusätzlich die Informationen des physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität zur Verwendung durch die Benutzerausrüstung zum Zugriff auf die Zielbasisstation während des schnellen Handovers enthält; und

Mittel zum gleichzeitigen Übertragen (S202) der ersten Nachricht an die Zielbasisstation (701) und der zweiten Nachricht an die Benutzerausrüstung (601).

8. Basisstation (701) nach Anspruch 7, wobei die Informationen aus der Zielbasisstation (701) zusätzlich Kryptografiealgorithmusinformationen einschließlich einer Kennung mindestens eines Kryptografiealgorithmus enthalten; und

wobei die Mittel zum Erzeugen der ersten und zweiten Nachricht auf den Kryptografiealgorithmusinformationen basieren.

9. Basisstation (701) nach Anspruch 8, wobei die erste Nachricht mindestens eine Kennung eines Kryptografiealgorithmus und einen abgeleiteten Schlüssel enthält, wobei die Basisstation ferner Mittel zum Auswählen der Kennung aus der mindestens einen empfangenen Kryptografiealgorithmuskennung basierend auf der Sicherheitskapazität der Benutzerausrüstung (601) umfasst.

10. Basisstation (701) nach Anspruch 9, wobei die zweite Nachricht mindestens die Informationen des physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität, die zur Verwendung durch die Benutzerausrüstung (601) für das schnelle Handover vordefiniert sind, sowie die Kennung des ausgewählten Kryptografiealgorithmus enthält.

11. Basisstation (701) nach Anspruch 9 oder 10, wobei die Basisstation ferner Mittel zum Ableiten des abgeleiteten Schlüssels, K_{eNB^*}, durch eine Schlüsselableitungsfunktion umfasst, die als Eingaben einen Schlüssel, K_{eNB}, die Informationen des vordefinierten physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität verwendet.

12. Benutzerausrüstung (601), umfassend:

Mittel zum Empfangen (S401) einer Nachricht aus einer Quellenbasisstation (701), die die Benutzerausrüstung (601) bedient, wobei die Nachricht Informationen über einen physischen Direktzugriffskanal und eine temporäre Zellenfunknetzidentität enthält, die durch eine Zielbasisstation zur Verwendung durch die Benutzerausrüstung vordefiniert sind, um während eines schnellen Handovers auf die Zielbasisstation zuzugreifen,

wobei die Nachricht zusätzlich Sicherheitsinformationen für die Sicherheitskommunikation zwischen der Zielbasisstation (701) und der Benutzerausrüstung (601) nach dem schnellen Handover enthält, wobei die Sicherheitsinformationen mindestens eine Kennung eines Kryptografiealgorithmus enthalten,

wobei die Benutzerausrüstung **dadurch gekennzeichnet ist, dass** sie umfasst:

Mittel zum Ableiten (S402) eines Schlüssels für die Sicherheitskommunikation mit der Zielbasisstation (701) basierend auf den Informationen des physischen Direktzugriffskanals, der temporären Zellenfunknetzidentität und der Kennung des Kryptografiealgorithmus; und

Mittel zum Verwenden (S403) des abgeleiteten Schlüssels für die Sicherheitskommunikation mit der Zielbasisstation (701) nach dem schnellen Handover.

13. Benutzerausrüstung (601) nach Anspruch 12, wobei die Mittel zum Ableiten des Schlüssels ferner umfassen:

Ableiten des Schlüssels, K_{eNB*}, durch eine Schlüsselableitungsfunktion, die als Eingaben einen Schlüssel K_{eNB}, die Informationen des physischen Direktzugriffskanals und die temporäre Zellenfunknetzidentität verwendet, die durch die Zielbasisstation (701) zur Verwendung durch die Benutzerausrüstung (601) für das schnelle Handover zu verwenden sind.

14. Computerprogramm, umfassend Anweisungen, die beim Ausführen durch einen Prozessor in einer Benutzerausrüstung die Benutzerausrüstung veranlassen, das Verfahren nach Anspruch 7 durchzuführen.

15. Computerprogramm, umfassend Anweisungen, die beim Ausführen durch einen Prozessor in einer Basisstation die Basisstation veranlassen, ein Verfahren nach mindestens einem der Ansprüche 1-6 durchzuführen.

Revendications

1. Procédé exécuté par une station de base (701) desservant un équipement d'utilisateur (601), ledit procédé comprenant :

la réception (S501) d'informations à partir d'une station de base cible, lesdites informations contenant des informations de canal d'accès aléatoire physique et une identité temporaire de réseau radio cellulaire prédéfinies pour être utilisées par ledit équipement d'utilisateur,
ledit procédé étant **caractérisé par** :

la décision (S503) d'initier un transfert rapide dudit UE vers ladite station de base cible en utilisant les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire ;
la génération (S201) d'un premier message et d'un second message, chacun comprenant des informations de sécurité pour une communication de sécurité entre la station de base cible (701) et l'équipement d'utilisateur (601) après ledit transfert rapide, dans lequel le second message comprend en outre lesdites informations de canal d'accès aléatoire physique et ladite identité temporaire de réseau radio cellulaire destinées à être utilisées par l'UE pour accéder à ladite station de base cible pendant ledit transfert rapide; et
la transmission (S202) simultanément, à partir de la station de base source (701), du premier message à la station de base cible (701) et du second message à l'équipement d'utilisateur (601).

2. Procédé selon la revendication 1, dans lequel les informations reçues (S501) à partir de la station de base cible comprennent en outre des informations d'algorithme de cryptographie comprenant un identificateur d'au moins un algorithme de cryptographie; et
dans lequel la génération des premier et second messages est basée sur les informations d'algorithme de cryptographie.

3. Procédé selon la revendication 2, dans lequel le premier message comprend au moins un identificateur d'un algorithme de cryptographie et une clé dérivée, dans lequel l'identificateur de l'algorithme de cryptographie est choisi parmi l'au moins un identificateur d'algorithme de cryptographie reçu sur la base de la capacité de sécurité de l'équipement d'utilisateur (601) .

4. Procédé selon la revendication 3, dans lequel le second message comprend au moins les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire prédéfinies pour être utilisées par l'équipement d'utilisateur (601) pour le transfert rapide, et l'identificateur de l'algorithme de cryptographie sélectionné.

5. Procédé selon la revendication 3 ou 4, dans lequel la clé dérivée, KeNB*, est dérivée par l'intermédiaire d'une fonction de dérivation de clé en utilisant, comme entrées, une clé KeNB, les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire prédéfinies.

6. Procédé exécuté par un équipement d'utilisateur, UE, ledit procédé comprenant :
la réception (S401), à partir d'une station de base source (701) desservant ledit équipement d'utilisateur (601), d'un message comprenant des informations de canal d'accès aléatoire physique et une identité temporaire de réseau radio cellulaire prédéfinies par une station de base cible pour être utilisées par l'UE pour accéder à ladite station de base cible pendant un transfert rapide, ledit message comprenant en outre des informations de sécurité pour une communication de sécurité entre la station de base cible (701) et l'équipement d'utilisateur (601) après ledit transfert rapide, dans lequel les informations de sécurité comprennent au moins un identificateur d'un algorithme de cryptographie, ledit procédé étant **caractérisé par** :

la dérivation (S402) d'une clé pour la communication de sécurité avec la station de base cible (701) sur la base des informations de canal d'accès aléatoire physique, de l'identité temporaire de réseau radio cellulaire, et de l'identificateur de l'algorithme de cryptographie; et

l'utilisation (S403) de la clé dérivée pour la communication de sécurité avec la station de base cible (701) après le transfert rapide.

7. Station de base (701), comprenant :

un moyen pour recevoir (S501) des informations à partir d'une station de base cible, lesdites informations contenant des informations de canal d'accès aléatoire physique et une identité temporaire de réseau radio cellulaire prédéfinies pour être utilisées par ledit UE,
ladite station de base étant **caractérisée par** ce qu'elle comprend :

un moyen pour décider (S503) d'initier un transfert rapide dudit UE vers ladite station de base cible en utilisant les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire ;
un moyen pour générer (S201) un premier message et un second message, chacun comprenant des informations de sécurité pour une communication de sécurité entre la station de base cible (701) et l'équipement d'utilisateur (601) après ledit transfert rapide, dans lequel le second message comprend en outre lesdites informations de canal d'accès aléatoire physique et ladite identité temporaire de réseau radio cellulaire destinées à être utilisées par l'UE pour accéder à ladite station de base cible pendant ledit transfert rapide; et
un moyen pour transmettre (S202) simultanément le premier message à la station de base cible (701) et le second message à l'équipement d'utilisateur (601).

8. Station de base (701) selon la revendication 7, dans laquelle les informations provenant de la station de base cible (701) comprennent en outre des informations d'algorithme de cryptographie comprenant un identificateur d'au moins un algorithme de cryptographie; et
dans laquelle le moyen de génération des premier et second messages est basé sur les informations d'algorithme de cryptographie.

9. Station de base (701) selon la revendication 8, dans laquelle le premier message comprend au moins un identificateur d'un algorithme de cryptographie et une clé dérivée, dans laquelle la station de base comprend en outre un moyen pour sélectionner ledit identificateur, parmi l'au moins un identificateur d'algorithme de cryptographie reçu, sur la base de la capacité de sécurité de l'équipement d'utilisateur (601).

10. Station de base (701) selon la revendication 9, dans laquelle le second message comprend au moins les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire prédéfinies destinées à être utilisées par l'équipement d'utilisateur (601) pour le transfert rapide, et l'identificateur de l'algorithme de cryptographie sélectionné.

11. Station de base (701) selon la revendication 9 ou 10, dans laquelle la station de base comprend en outre un moyen pour dériver la clé KeNB* dérivée par l'intermédiaire d'une fonction de dérivation de clé en utilisant, comme entrées, une clé KeNB, les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire prédéfinies.

12. Équipement d'utilisateur, UE (601), comprenant :
un moyen pour recevoir (S401), à partir d'une station de base source (701) desservant l'UE (601), un message comprenant des informations de canal d'accès aléatoire physique et une identité temporaire de réseau radio cellulaire prédéfinies par une station de base cible pour être utilisées par l'UE pour accéder à ladite station de base cible pendant un transfert rapide, ledit message comprenant en outre des informations de sécurité pour une communication de sécurité entre la station de base cible (701) et l'UE (601) après ledit transfert rapide, dans lequel les informations de sécurité comprennent au moins un identificateur d'un algorithme de cryptographie, ledit UE étant **caractérisé par** ce qu'il comprend :

un moyen pour dériver (S402) une clé pour la communication de sécurité avec la station de base cible (701) sur la base des informations de canal d'accès aléatoire physique, de l'identité temporaire de réseau radio cellulaire, et de l'identificateur de l'algorithme de cryptographie; et
un moyen pour utiliser (S403) la clé dérivée pour la communication de sécurité avec la station de base cible (701) après le transfert rapide.

13. UE (601) selon la revendication 12, le moyen pour dériver la clé comprenant en outre :
un moyen pour dériver la clé KeNB* par l'intermédiaire d'une fonction de dérivation de clé en utilisant, comme entrées, une clé KeNB, les informations de canal d'accès aléatoire physique et l'identité temporaire de réseau radio cellulaire prédéfinies par la station de base cible (701) pour être utilisées par l'UE (601) pour le transfert rapide.

14. Programme d'ordinateur comprenant des instructions qui, lorsqu'elles sont exécutées par un processeur dans un équipement d'utilisateur, amènent ledit

équipement d'utilisateur à exécuter le procédé de la revendication 7.

15. Programme d'ordinateur comprenant des instructions qui, lorsqu'elles sont exécutées par un processeur dans une station de base, amènent ladite station de base à exécuter le procédé selon au moins l'une des revendications 1 à 6.

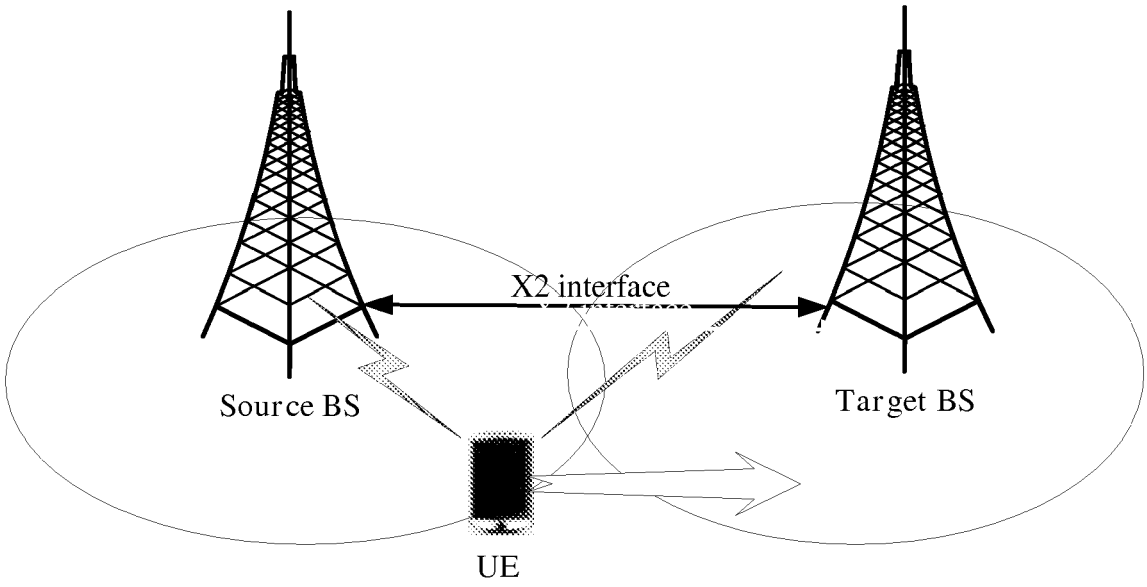
X2 interface
Source BS
Target BS
UE

Fig. 1

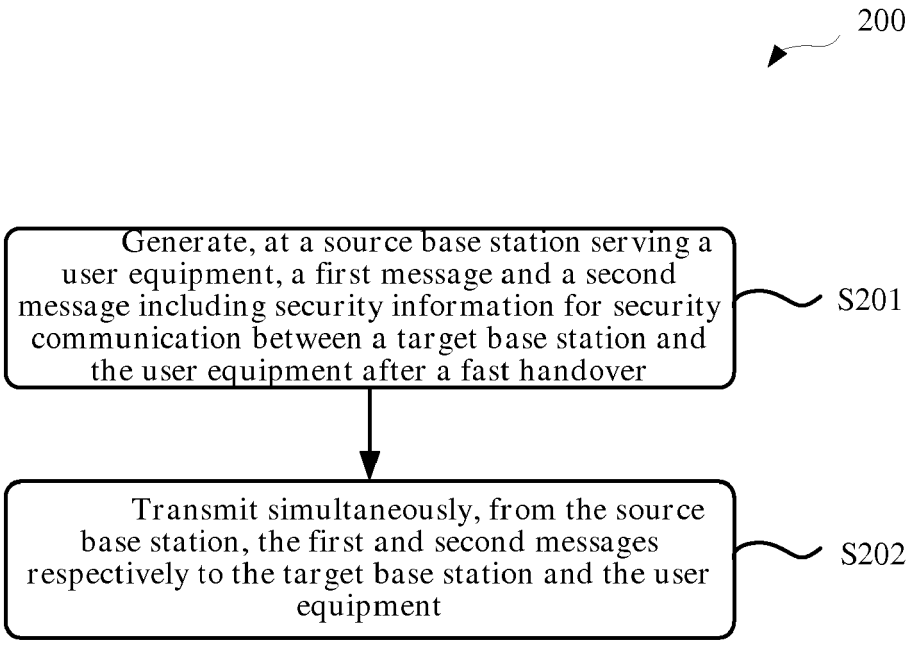
200
Generate, at a source base station serving a user equipment, a first message and a second message including security information for security communication between a target base station and the user equipment after a fast handover
S201
Transmit simultaneously, from the source base station, the first and second messages respectively to the target base station and the user equipment
S202

Fig. 2

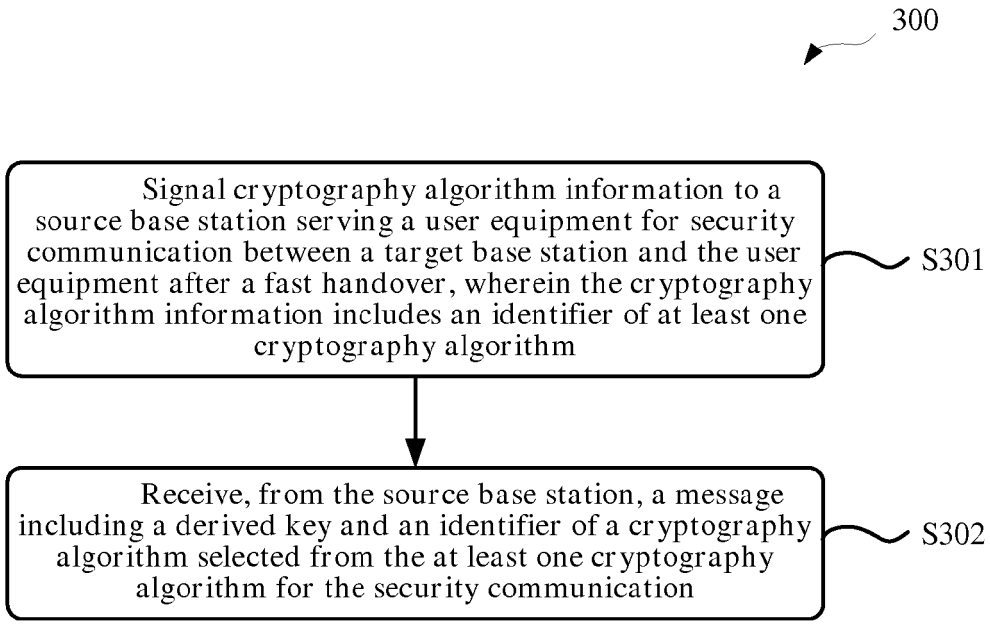
300
Signal cryptography algorithm information to a source base station serving a user equipment for security communication between a target base station and the user equipment after a fast handover, wherein the cryptography algorithm information includes an identifier of at least one cryptography algorithm
S301
Receive, from the source base station, a message including a derived key and an identifier of a cryptography algorithm selected from the at least one cryptography algorithm for the security communication
S302

Fig. 3

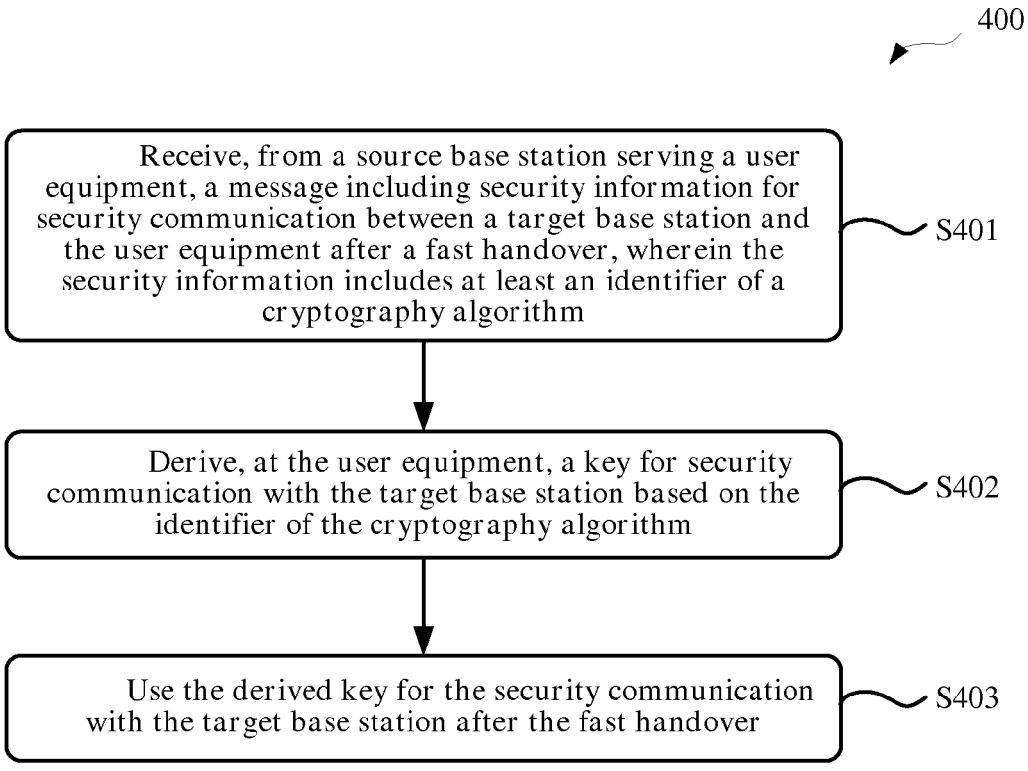
400
Receive, from a source base station serving a user equipment, a message including security information for security communication between a target base station and the user equipment after a fast handover, wherein the security information includes at least an identifier of a cryptography algorithm
S401
Derive, at the user equipment, a key for security communication with the target base station based on the identifier of the cryptography algorithm
S402
Use the derived key for the security communication with the target base station after the fast handover
S403

Fig. 4

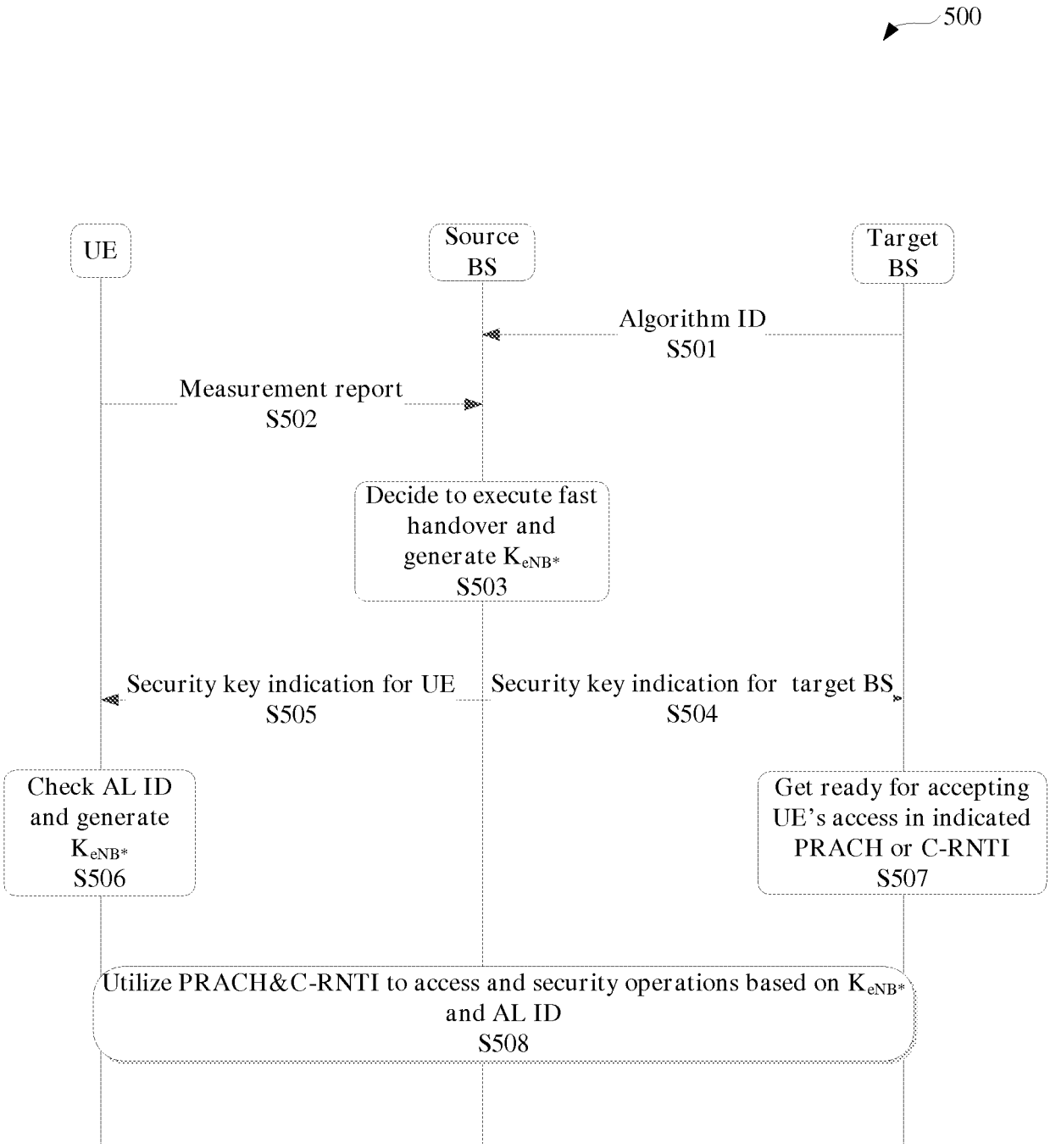
500
UE
Source BS
Target BS
Algorithm ID
S501
Measurement report
S502
Decide to execute fast handover and generate K_{eNB*}
S503
Security key indication for UE
S505
Security key indication for target BS
S504
Check AL ID and generate K_{eNB*}
S506
Get ready for accepting UE's access in indicated PRACH or C-RNTI
S507
Utilize PRACH&C-RNTI to access and security operations based on K_{eNB*} and AL ID
S508

Fig. 5

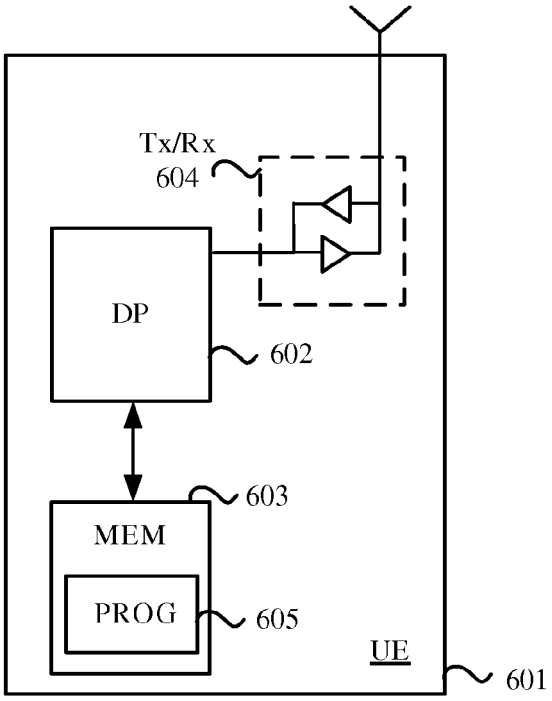
Tx/Rx
604
DP
602
603
MEM
PROG
605
UE
601

Fig. 6

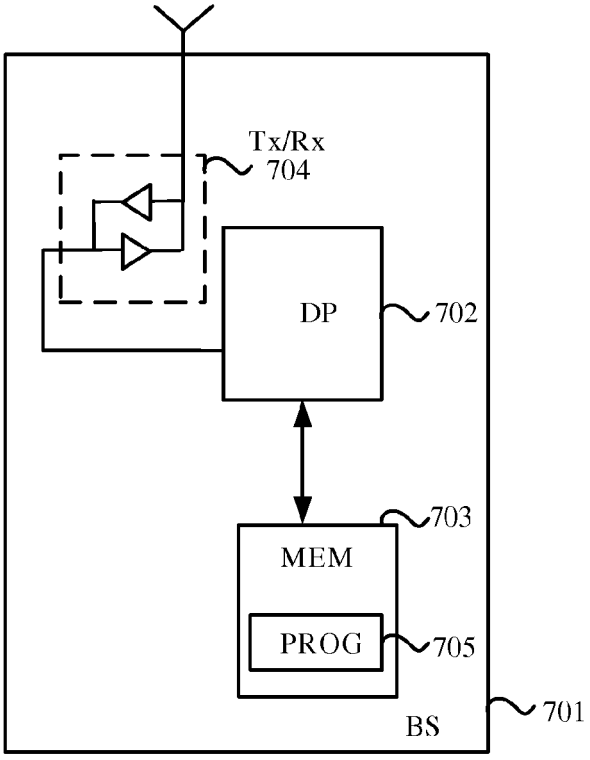
Tx/Rx
704
DP
702
703
MEM
PROG
705
BS
701

Fig. 7

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 101355985 A **[0008]**

Non-patent literature cited in the description

- *3GPP TS 33.401 V12.5.0,* September 2012 **[0005]**